Les spatialités de la vie privée à l'ère numérique - Usages et perceptions de la domotique et du logis connecté

Jean-François Perrat

Numéro National de Thèse : 2023ENSL0017

THESE

en vue de l'obtention du grade de Docteur, délivré par

l'ECOLE NORMALE SUPERIEURE DE LYON

Ecole Doctorale N° 483
Sciences sociales (Histoire, Géographie, Aménagement, Urbanisme, Architecture, Archéologie, Science politique, Sociologie, Anthropologie)

Discipline : géographie

Soutenue publiquement le 20/04/2023, par :

Jean-François PERRAT

Les spatialités de la vie privée à l'ère numérique

Usages et perceptions de la domotique et du logis connecté

Devant le jury composé de :

BOULLIER, Dominique Professeur des Universités Institut d'études politiques de Paris Rapporteur
EVENO, Emmanuel Professeur des Universités Université de Toulouse Jean-Jaurès Rapporteur
ALOMBERT, Anne Maîtresse de Conférences Université Paris 8 Examinatrice
BERNIER, Xavier Professeur des Universités Sorbonne Université Examinateur
JOLIVEAU, Thierry Professeur des Universités Université de Saint-Étienne Examinateur
REY, Bénédicte Maîtresse de Conférences Université de technologie de Belfort-Montbéliard Examinatrice
LUSSAULT, Michel Professeur des Universités École normale supérieure de Lyon Directeur de thèse
BEAUDE, Boris Professeur Associé Université de Lausanne Co-directeur de thèse

En mémoire de mon frère Pierre,

qui n'est pas pour rien dans toute cette histoire

SOMMAIRE

REMERCIEMENTS

Mes remerciements vont d'abord à Michel Lussault et à Boris Beaude, qui auront su encadrer cette thèse dans une atmosphère de grande liberté intellectuelle, de rigueur bienveillante et de suggestivité. Tous deux se gardent bien de dirigisme, mais ils ne m'en voudront pas de signaler ici la qualité de leur supervision sur les longs chemins suivis au cours de ce travail. Depuis longtemps déjà, le *Dictionnaire de la géographie et de l'espace des sociétés* avait été l'inépuisable tuteur aiguillonnant mes curiosités d'étudiant en géographie, et je suis toujours aussi honoré d'avoir pu entreprendre un travail doctoral avec l'un de ses éditeurs. Pour avoir découvert Boris Beaude et sa pensée plus tardivement, j'espère que ce travail rend aujourd'hui justice à l'illumination et à la complicité d'esprit immédiate ressentie à ma première lecture des *Fins d'Internet*, immédiatement suivie de celle d'*Internet : changer l'espace, changer la société*, et qui auront été pour moi un tournant intellectuel majeur.

Mes plus vifs remerciements vont ensuite aux membres du jury qui m'ont fait l'honneur de lire et d'évaluer ce travail, de surcroît dans un temps ramassé : Dominique Boullier et Emmanuel Eveno comme rapporteurs, et Anne Alombert, Xavier Bernier, Thierry Joliveau et Bénédicte Rey comme examinatrices et examinateurs.

Un grand merci collectif à mes enquêtés, qu'ils aient subi mes questions en entretien ou contribué de près ou de loin à la réflexion, avec une mention particulière à la Quadrature du Net pour leur action opiniâtre dans la défense des libertés civiles à l'ère numérique.

Un autre grand merci à mes collègues enseignants (et à mes enseignants devenus collègues !) de l'ENS de Lyon, de l'UPEC, de l'UPEM, et de Paris IV.

Un clin d'œil aux vieux briscards de mes années de formation, avec qui nous continuons de mûrir ensemble. Louis, Cécile, JB, Gilles... À Marie-Christine Doceul, qui m'aura définitivement éveillé à la géographie – sur un terrain bien préparé par Daniel Escobessa et Audrey Ferlut au lycée. À Myriam Houssay-Holzschuch pour avoir accompagné avec *maestria*

mes premiers pas dans la recherche, quoique je me sois depuis un peu éloigné de l'Afrique du Sud.

À mes camarades doctorants et stagiaires du couloir de géographie de l'ENS de Lyon, dont la soif d'échanges intellectuels et de traits d'humour n'a sans doute été dépassé que par leur appétit pour des nourritures beaucoup moins spirituelles, généralement exprimé dès 11h30. À ma bande sûre : Franck pour notre détention amicale à perpétuité, l'éblouissante Laetitia pour sa présence en béton, et mon inénarrable co-régional de l'étape Alex (qui, quoi qu'il en dise, est aussi Aindien que moi) ; les relectures de ce dernier ont été un soutien continu de ce travail. Désolé à Sophie et à Ninon de les avoir retardées d'environ une décennie dans leurs recherches comme co-bural trop bavard. L'expression de mes plus sincères salutations à Jean-Benoît, animateur passionné de Géoconfluences, une bête magnifique ! Le poil luisant ! Une merveille ! Une tête passée par la porte à Ludovic pour nos échanges sur l'architecture les soirs et les jours non-ouvrés où nous nous retrouvions à hanter les locaux. À tout le petit monde qui aura peuplé le couloir Sud au cours des années : Anne-Lise, Raphaëlle, Clément, Anaïs, Florence, Emmanuelle, François, Alexandra, Monique, Octavie… Puissions-nous toutes et tous longtemps nous RUtrouver autour d'une bonne tablée !

À mes amis qui m'attendent avec fidélité hors des murs du labo ou du repli domestique dans lequel une longue rédaction m'aura trop souvent soustrait au plaisir de les voir. Thomas, Maxime, Romain, Vincent, Beril, Dilara, Hugues, les Pierres, Mandement, Étienne, Cathy, Laura, Benoît, Louis/e, Antoine… j'arrive !

À ma famille, et d'abord à mes parents, Albert Perrat, et au docteur Angela Perrat-Mabilon, qui sera à jamais la première détentrice de ce titre. Tous deux auront su m'accompagner depuis toujours vers les joies de la découverte et de la science. À mes frères et sœurs, Arnaud, Aurélie, Christophe, et Marie : vous voyez, ce n'était pas SI long. Merci à vous ainsi qu'à Dominique pour la relecture orthographique plus que nécessaire de ce texte. Un petit « Alexa, hello » à la vieille enceinte Amazon Echo qui m'aura suivi pendant la thèse – et minuté bien des cuissons.

À Merve(m), enfin, qui m'est unique dans la catégorie si spéciale qui les rassemble toutes : tu es tout l'oxygène du Monde.

INTRODUCTION

Chapitre 1 - ITINERAIRE PERSONNEL DANS LE CHAMP DE LA GEOGRAPHIE DU NUMERIQUE

I - L'APPROCHE TERRITORIALE D'INTERNET

Comme bien des travaux de recherche, la présente thèse est née du sentiment d'un manque. Un sentiment qui s'est avéré trompeur, comme toujours, mais qui était peut-être moins infondé qu'à l'habitude dans le champ encore jeune de la géographie du numérique. C'est en 2014, en préparant les concours de l'enseignement secondaire, que la rédaction d'une fiche sur la représentation des réseaux m'a confronté pour la première fois à la littérature scientifique sur les questions numériques en géographie. J'avais déjà été sensibilisé aux travaux de Manuel Castells sur la « société en réseaux »[1] et aux *science and technology studies* (STS) de Bruno Latour et Michel Callon dans un cours de Manuel Appert à l'université Lyon 2. Mais la principale référence que j'avais alors trouvée à propos d'Internet, *Internet : géographie d'un réseau*, de Gabriel Dupuy[2], m'avait plus particulièrement interpellé. J'avais apprécié qu'il existe une géographie d'Internet, d'une part, et été frustré par son approche très topographique et aménagiste, d'autre part, qui me ramenait vers une géographie classique là où je pressentais la possibilité d'approches beaucoup plus originales.

La géographie du numérique et d'Internet prolonge en effet celle des technologies de l'information et de la communication, qui a longtemps en France fait la part belle à l'approche territoriale[3]. La thématique émerge dans la géographie française au cours des années 1970 et s'affermit dans les années 1980, notamment sous l'impulsion d'Henry Bakis[4]. S'il s'est d'abord agi d'aborder la question sous l'angle de la géographie industrielle, en étudiant par exemple l'inscription spatiale d'une firme comme IBM dans son réseau de sous-traitance[5], il a rapidement été question d'interroger plus fondamentalement quels pouvaient être les effets des TIC sur l'espace géographique et dans une moindre mesure sur les pratiques spatiales, dans la

[1] M. CASTELLS, *The rise of the network society*, 1999e éd., Oxford (Royaume-Uni), Blackwell, 1996
[2] G. DUPUY, *Internet : géographie d'un réseau*, Paris (France), Ellipses, 2002, 1 vol.
[3] Les paragraphes qui suivent sont en large partie tirés d'un article déjà publié : J.-F. PERRAT, « Un "deep/dark web" ? Les métaphores de la profondeur et de l'ombre sur le réseau Tor », *Netcom. Réseaux, communication et territoires*, vol. 32, no 1-2, 2018, § 12-14 (en ligne : https://journals.openedition.org/netcom/3134)
[4] H. BAKIS, « Éléments pour une géographie des télécommunications », *Annales de géographie*, vol. 89, no 496, 1980, p. 657-688 (en ligne : https://www.persee.fr/doc/geo_0003-4010_1980_num_89_496_19992 ; consulté le 2 octobre 2018)
[5] H. BAKIS, *I.B.M: une multinationale régionale*, Grenoble (France), Presses universitaires de Grenoble, 1977

mouvance de travaux comme ceux de Thorngren sur le développement régional en Suède[6], ou de Abler sur le téléphone et le système métropolitain aux États-Unis[7]. En matière de mobilités, la thématique de la substitution (ou non) des déplacements par la télécommunication, très active depuis les années 1960, est dépassée dans les années 1980 par la question du rapport entre les télécommunications et la forme même des villes[8], ou encore par la question de la structuration de l'espace industriel par les réseaux de télécommunication, et non plus seulement la localisation des matières premières ou des réseaux de transport[9].

Avec l'émergence du réseau mondial Internet et du World Wide Web dans les années 1990, beaucoup de chercheurs prennent le contrepied de cette approche territoriale. Une tendance consistant à penser que les TIC pourraient s'exonérer de l'espace matériel et des territoires au profit des télécommunications, à la fois quasi instantanées et peu coûteuses en énergie, est alors montée en puissance[10]. Nicholas Negroponte, l'un des pionniers de la réflexion sur l'émergence d'Internet au MIT avance que cette nouvelle technologie permettra d'« aplanir les organisations, mondialiser la société, décentraliser l'autorité et favoriser l'harmonie entre les êtres humains »[11]. Les possibilités concrètes offertes par le télétravail ou le commerce en ligne, ainsi que le succès des thématiques du « village global »[12] ou du « cyberespace »[13], y ont largement contribué. L'urbaniste et architecte William J. Mitchell va par exemple jusqu'à avancer que « le Net nie la géométrie »[14]. Nous serions alors entrés à l'ère d'un « espace de flux »[15]. Cette remise en cause de l'utilité de la coprésence physique aurait même dû pour certains précipiter la fin des villes. La « fin de la géographie » annoncée n'a évidemment pas eu lieu : la prégnance des facteurs de localisation, des économies d'échelle et

[6] B. THORNGREN, *Telecommunications and Regional Development in Sweden*, National Swedish Board for Technical Development, 1977
[7] R. ABLER, « The telephone and the evolution of the American metropolitan system », dans IDS Pool, *The social impact of the telephone*, Cambridge (États-Unis), MIT Press, 1977, p. 318-341
[8] T. SCHWANEN, « Information Technology and Mobility », dans *International Encyclopedia of Geography*, s. l., American Cancer Society, 2017
[9] H. BAKIS, « Télécommunication et organisation spatiale des entreprises », *Revue Géographique de l'Est*, vol. 25, nº 1, 1985, p. 33-46 (en ligne : https://www.persee.fr/doc/rgest_0035-3213_1985_num_25_1_1566 ; consulté le 28 septembre 2018)
[10] H. BAKIS, « Le « géocyberespace » revisité », *Netcom*, vol. 21, nº 3-4, 16 décembre 2007, p. 285-296 (en ligne : http://netcom.revues.org/2220 ; consulté le 15 novembre 2016)
[11] N. NEGROPONTE, *Being Digital*, New York (ÉUA), Knopf, 1995, p. 182 cité par F. TURNER, *Aux sources de l'utopie numérique: de la contre-culture à la cyberculture, Stewart Brand, un homme d'influence*, L. Vannini (trad.), 2e éd., Caen (France), C&F éditions, 2021, p. 35
[12] M. MCLUHAN et Q. FIORE, *The Medium is the Massage*, J. Agel (éd.), Londres (Royaume-Uni), The Penguin Press, 1967
[13] W. GIBSON, *Neuromancer*, New York (États-Unis), Ace Books, 1994
[14] W. J. MITCHELL, *City of bits: space, place, and the infobahn*, 6e éd., Cambridge (États-Unis), MIT Press, 1999, p. 8
[15] M. CASTELLS, *The rise of the network society*, *op. cit.*

des effets d'agrégation n'a pas été abolie par Internet en ce qui concerne les biens matériels[16]. Plus encore, Internet a en fait renforcé le besoin d'une approche territoriale du numérique et des TIC dans la mesure où la présence d'infrastructures de télécommunication et des capacités locales à en tirer parti contribuent à accentuer concurrences et hiérarchies territoriales[17]. Contre le mythe de l'aspatialité d'Internet, les aménageurs ont eux-mêmes théorisé le problème de la « fracture numérique » entre les territoires[18]. Cette « impasse » théorique de la fin de la géographie serait née d'une trop grande « préoccupation pour les usages » d'Internet, faisant fi de sa « matérialité »[19].

Entre la fin des années 1990 et les années 2000, un consensus largement partagé s'est établi autour de l'idée qu'il fallait aborder Internet dans une approche territoriale, spatialisée, en rupture avec les apories sus-citées comme avec les approches trop sectorielles des économistes[20]. Internet ne devait pas être conçu comme abolissant l'espace, mais comme « [augmentant] » les capacités d'interaction des territoires, de leurs habitants et de leurs institutions[21] dans des approches interrogeant l'interspatialité entre espace en ligne et espace territorial. Selon un terme forgé par Henry Bakis, l'espace géographique du XXIe siècle serait un « géocyberespace » hybridant le géoespace traditionnel au « cyberespace » informationnel[22] en un complexe où les délimitations seraient de plus en plus floues. Dans sa thèse, Marina Duféal a ainsi retrouvé la même structure dans les liens entre sites institutionnels des communes de l'arc méditerranéen que dans leur système urbain géospatial[23]. Elle suggère aussi qu'un phénomène territorial comme l'insularité corse se retrouve dans son « inscription spatiale » en ligne[24]. Thierry Joliveau développe quant à lui l'idée de « géoweb » pour décrire les services

[16] F. LASSERRE, « Internet : La fin de la géographie ? », *Cybergeo : European Journal of Geography*, 31 octobre 2000 (en ligne : https://cybergeo.revues.org/4467 ; consulté le 5 janvier 2017)
[17] H. BAKIS, « Le « géocyberespace » revisité », *op. cit.*
[18] G. DUPUY, *La fracture numérique*, Paris (France), Ellipses, 2007
[19] M. DUFEAL et L. GRASLAND, « La planification des réseaux à l'épreuve de la matérialité des TIC et de l'hétérogénéité des territoires », *Flux*, nº 54, 2003, § 1 (en ligne : http://www.cairn.info/article.php?ID_ARTICLE=FLUX_054_0049 ; consulté le 2 octobre 2018)
[20] M. DUFEAL, *Les sites web, marqueurs et vecteurs de dynamiques spatiales et économiques dans l'espace méditerranéen français*, thèse de doctorat en géographie, Avignon (France), université d'Avignon et des Pays du Vaucluse, 2004, chap. 1 & 2
[21] P. MUSSO, « Territoires numériques », *Médium*, nº 15, 2008, p. 33 (en ligne : http://www.cairn.info/revue-medium-2008-2-p-25.html ; consulté le 21 juin 2018)
[22] H. BAKIS, « Le « géocyberespace » revisité », *op. cit.* ; P. VIDAL et H. BAKIS, « De la négation du territoire au géocyberespace : vers une approche intégrée de la relation entre espace et TIC », dans C. Brossaud et B. Reber (éd.), *Humanités numériques 1 : nouvelles technologies cognitives et épistémologie*, Paris (France), Hermes - Lavoisier, 2007, vol. 1, p. 101-116
[23] M. DUFEAL, *Les sites web, marqueurs et vecteurs de dynamiques spatiales et économiques dans l'espace méditerranéen français*, *op. cit.*
[24] M. DUFEAL, « L'inscription spatiale de l'insularité: la Corse séparée de la France – sur le Web, Abstract », *Annales de géographie*, vol. 5, nº 645, 2005, p. 496-509 (en ligne : https://www.cairn.info/revue-annales-de-geographie-2005-5-page-496.html ; consulté le 29 juin 2018)

cartographiques en ligne tels que Google Maps[25], et plus largement de « géonumérisation » pour décrire le « processus de transcription au moyen d'outils informatiques des objets, êtres, phénomènes, activités, images, textes ... localisés sur la surface terrestre »[26], terme également repris par Henri Desbois[27]. Il s'agit là encore de lier Internet et territoire : les usages nouveaux permis par le numérique sont mis en avant, mais le référentiel reste géospatial.

C'est donc dans cette mouvance que s'inscrit le travail de Gabriel Dupuy au moment où je le consulte en 2014. Du reste, deux ans plus tard encore, en 2016, alors que je préparais cette fois mon mémoire de master 2, le catalogue de l'Institut de géographie de Paris, l'un des fonds les plus riches de la discipline, ne contenait que seize références incluant le mot « Internet » dans les titres et sous-titres d'ouvrages et d'articles imprimés[28]. Pour beaucoup, ces références s'inscrivaient là encore dans une approche très territoriale ou aménagiste. Cela étant dit sans vouloir négliger l'importance d'une telle approche : c'est pendant que je travaillais au CGET[29], dans un service issu de l'ex-DATAR, haut-lieu historique de l'aménagement du territoire français, que Michel Lussault et moi sommes entrés en contact pour poser les jalons du mémoire de master qui a préludé à cette thèse. Mon idée était alors de faire se croiser mon intérêt autodidacte pour les TIC et ma formation beaucoup plus académique en géographie. Ma prétention était d'aborder Internet sous un angle plus nettement orienté par les pratiques mêmes ayant lieu et s'appuyant sur le réseau qui, quoique plus intangibles que la fibre optique d'un *backbone* ou l'implantation d'antennes-relais, m'apparaissaient tout aussi spatiales.

II - INTERNET COMME ESPACE A PART ENTIERE

Bien évidemment, l'angle mort bibliographique que je pensais avoir repéré n'était en fait que l'ombre portée de ma méconnaissance de la littérature du domaine.

[25] T. JOLIVEAU, « Le géoweb, un nouveau défi pour les bases de données géographiques », *L'Espace géographique*, vol. 40, n° 2, 12 juillet 2011, p. 154-163 (en ligne : http://www.cairn.info/resume.php?ID_ARTICLE=EG_402_0154 ; consulté le 29 septembre 2016)
[26] T. JOLIVEAU, « Géomatique et géonumérisation », sur *Monde géonumérique*, 8 octobre 2007 (en ligne : https://mondegeonumerique.wordpress.com/geomatique-et-cie/geomatique-et-geonumerisation/ ; consulté le 8 octobre 2018)
[27] H. DESBOIS, « La carte et le territoire à l'ère numérique », *Socio. La nouvelle revue des sciences sociales*, n° 4, 25 avril 2015, p. 39-60 (en ligne : https://socio.revues.org/1262 ; consulté le 20 février 2017)
[28] J.-F. PERRAT, *Peler l'oignon. Étude géographique des services cachés du réseau Tor*, mémoire de M2, Lyon (France), École normale supérieure de Lyon, 2016, p. 8
[29] Commissariat général à l'égalité des territoires, qui a lui-même été fusionné au sein de la nouvelle Agence nationale pour la cohésion des territoires en 2019.

Début 2015, je découvris les travaux de Boris Beaude, d'abord *Les fins d'Internet*[30], puis *Internet : changer l'espace, changer la société*[31]. J'y ai trouvé cette même volonté de rompre avec une approche trop territoriale d'Internet. Les questions de l'implantation des infrastructures ou des enjeux géopolitiques liés à leur interconnexion sont bien sûr traitées[32]. Mais elles sont secondaires en regard de l'affirmation forte qu'Internet est aussi un espace à part entière, en ligne, de substance immatérielle, et de métrique topologique. Pour reprendre un distinguo habituel en informatique, Internet a une composante matérielle / réseau / *hardware* et une composante logique / servicielle / *software*. En langue française, d'autres auteurs en avaient bien sûr déjà repris l'idée, comme Henry Bakis qui avait proposé dès 1997 le triptyque géoespace / cyberespace / géocyberespace pour désigner respectivement l'espace matériel classique, l'espace des pratiques en lignes, et l' « [interfaçage] » du premier et du deuxième[33]. Mais, comme on l'a vu, les travaux qui ont suivi se sont concentrés sur l'approche géocyberspatiale, envisageant toujours les espaces en ligne comme une augmentation ou un reflet du géoespace.

L'apport majeur de Boris Beaude est d'avoir élaboré un cadre conceptuel permettant une lecture pleinement spatiale des espaces réticulaires et des interactions en ligne, sans avoir à les ramener à une augmentation du géoespace pour justifier de leur géographicité. Il propose le concept de synchôrisation, formé sur *chôra* (« espace habité » ou « place » en grec ancien) et sur le préfixe *syn-* (qui renvoie à l'idée de réunion dans l'espace ou le temps), la synchôrisation étant le pendant spatial de la synchronisation temporelle. Il s'agit du « processus qui consiste à se donner un espace commun pour être et pour agir »[34]. L'originalité du concept est d'adjoindre deux propriétés fondamentales d'Internet. D'une part, Internet est une technologie de gestion de la distance : il permet d'abolir l'écart entre deux réalités sociales par

[30] B. BEAUDE, *Les fins d'Internet*, Limoges (France), FYP (Limoges), 2014
[31] B. BEAUDE, *Internet: changer l'espace, changer la société - Les logiques contemporaines de synchorisation*, Limoges (France), Fyp éditions, 2012
[32] C'est d'ailleurs une des principales thématiques des *Fins d'Internet*, au nombre desquelles l'auteur compte la tentation de substituer à *Inter*net des *intra*nets nationaux plus faciles à contrôler, en particulier dans des régimes autoritaires comme la Chine, la Russie ou l'Iran.
[33] Plus précisément, il distingue :
« - l'espace de la distance, classiquement abordé comme l'espace physique avec ses lieux et sa « rugosité » (le géoespace);
- l'espace technologique des réseaux et des flux où l'on peut retrouver le contenu de la notion précédente de cyberespace ;
- les manifestations spatiales résultant de l'interface entre les deux premiers niveaux, en un « tout » définissant LA nouvelle réalité spatio-temporelle des sociétés de communication et d'information, dans une sorte de fusion entre l'espace physique, l'espace des réseaux et les nouvelles potentialités et usages sociaux en découlant. » (H. BAKIS, « Le « géocyberespace » revisité », *op. cit.*, p. 288)
[34] B. BEAUDE, *Internet: changer l'espace, changer la société*, *op. cit.*, chap. 2

la télécommunication. D'autre part, l'interaction sur Internet peut être pérenne : là où la plupart des technologies de télécommunication antérieures permettent une mise en relation point à point, mais temporaire, comme dans le cas d'un appel téléphonique, Internet crée des espaces qui subsistent aux interactions qui y ont lieu et en conservent les traces. Cette propriété a notamment fondé l'essor, dans les années 1990, de l'étude des « communautés en ligne » (*online communities*)[35], dont Andrew Feenberg a proposé une des premières analyses détaillées à partir de son expérience d'enseignement et de retours d'expérience partagés au Western Behavioral Sciences Institute (Californie) en 1982[36].

Le concept de synchôrisation généralise les observations de ce type, et les inscrit dans une conception relationnelle de l'espace où « l'espace procède de la spatialité »[37] - cela plus nettement en ligne que dans l'espace territorial, du fait de la plus grande inertie des agencements spatiaux matériels. C'est la raison pour laquelle Boris Beaude défend l'idée que les espaces en ligne, bien qu'immatériels ne sont pas, comme le laisse entendre un terme d'usage courant, « virtuels »[38] : « [Internet est] non seulement [une] médiation, mais aussi [un] espace, réel, où se déroule à chaque instant un nombre considérable d'événements qui, aussi insignifiants soient-ils, participent du Monde en devenir »[39]. Un exemple de mise en pratique de cette grille de lecture des espaces numériques est proposé par Boris Beaude à propos de l'encyclopédie participative en ligne Wikipédia vue comme un « lieu »[40]. Si les lecteurs en voient surtout la vitrine que constituent les articles, le site repose sur une architecture spatiale complexe délimitant nettement pages de discussion, historique des versions précédentes ou encore pages explicatives d'usage interne. Les contributeurs doivent acquérir des compétences spatiales pour y circuler, et pour y agir en fonction de leur degré d'implication dans le projet. Une logique de

[35] J. PREECE, D. MALONEY-KRICHMAR et C. ABRAS, « History of online communities », *Encyclopedia of community*, vol. 3, nº 1023-1027, 2003, p. 86

[36] A. FEENBERG, « Building a Global Network: The WBSI Experience », dans L. M. Harasim, *Global Networks : Computers and International Communication*, Cambridge (États-Unis), MIT Press, 1993, p. 185-197 Cette expérience pédagogique interactive s'est faite avant l'avènement d'Internet comme technologie grand public. Très onéreuse, elle n'a concerné que quelques dizaines de cadres de haut niveau des secteurs public et privé, communiquant à partir d'ordinateurs portables Apple IIe et à travers un réseau de partage de texte via une connexion téléphonique proposée par l'entreprise The Source, basée à proximité de Washington D.C. et rachetée en 1989 par CompuServe. Cette expérience « en ligne » reste néanmoins très proche de ce qu'a permis Internet à plus large échelle au cours de la décennie suivante.

[37] M. LUSSAULT, « Spatialité », dans J. Lévy et M. Lussault (éd.), *Dictionnaire de la géographie et de l'espace des sociétés*, Paris (France), Belin, 2003, p. 866-868

[38] Plus précisément, « C'est pourquoi la virtualité d'Internet n'est pas celle que l'on croit. Elle ne s'oppose pas au réel, mais à l'actuel. Elle se trouve dans chacune de nos actions. Internet offre de nouvelles potentialités d'action et chacune des virtualités qui est ainsi actualisée, conjointement, change subrepticement le monde que nous vivons. » B. BEAUDE, *Internet: changer l'espace, changer la société*, *op. cit.*, chap. introductif

[39] *Id.*

[40] B. BEAUDE, « De quoi Wikipédia est-elle le lieu ? », dans L. Barbe, L. Merzeau et V. Schafer (éd.), *Wikipédia, objet scientifique non identifié*, Nanterre, Presses universitaires de Paris Nanterre, 2015, p. 41-54

proximité préside à la critique éditoriale : les différends doivent être réglés préférentiellement sur la page de discussion d'un article, mais peuvent être progressivement étendus à d'autres espaces (comme le « Bistro » dans la version francophone) et faire appel à l'arbitrage de contributeurs plus éloignés du sujet de base ainsi qu'à des utilisateurs dotés de pouvoirs particuliers (administrateurs, révocateurs…).

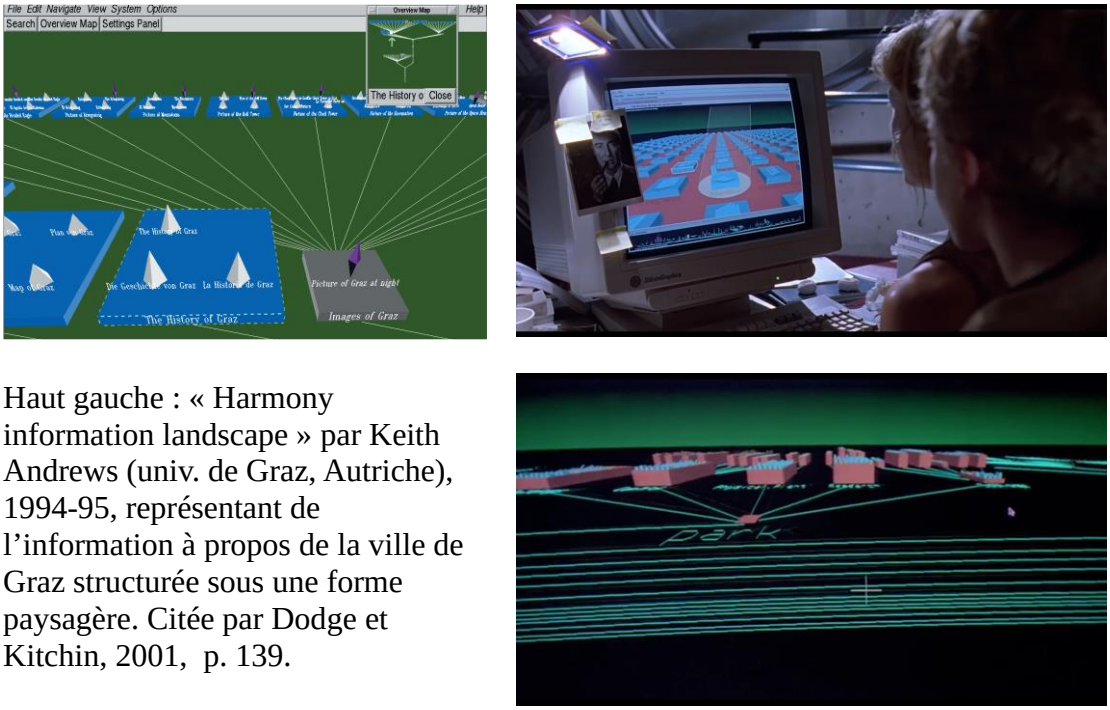
III - LA TENTATION DE LA REPRESENTATION, OU L'APORIE PARTIELLE DE LA METAPHORE SPATIALE

Mon premier travail à s'être inscrit dans cette optique de recherche est un mémoire de master 2 consacré au réseau Tor (*The Onion Router*, un réseau superposé à Internet) et notamment à ses services cachés[41], généralement désignés comme « *deep* » ou « *dark web* », quoique ces dénominations profanes et portées par un certain sensationnalisme me semblent impropres à désigner ce réseau[42]. Il visait à assumer pleinement l'idée que ces services cachés[43] étaient un ensemble de lieux méritant une investigation géographique. Il a également été notre premier travail commun avec les directeurs de cette thèse, Michel Lussault et Boris Beaude.

C'est au cours de ce travail que j'ai découvert une partie de la littérature anglophone sur la question de la géographie du numérique, qui très vite m'a semblé beaucoup plus en phase avec l'approche défendue par Boris Beaude que la plupart des travaux francophones que j'avais consultés jusque-là. Le diptyque formé par l'ouvrage théorique *Mapping Cyberspace*[44] et son pendant plus empirique *Atlas of Cyberspace*[45] en est particulièrement représentatif. Ce dernier ouvrage s'ouvre par un chapitre assez classique sur la cartographie des infrastructures et du trafic (« *mapping infrastructure and traffic* »), avant de passer aux « projets les plus passionnants [de] cartographie des paysages informationnels du cyberespace »[46]. À leur lecture, j'ai été frappé par l'exhaustivité des approches spatiales du numérique couvertes par ces deux ouvrages. Il s'agissait d'une part, donc, de traiter du numérique territorial (câbles sous-marins, *backbones*, différenciation locale dans l'accès au réseau, *traceroutes*…) mais aussi du Web

[41] J.-F. PERRAT, *Peler l'oignon*, *op. cit.*
[42] J.-F. PERRAT, « Un "deep/dark web" ? Les métaphores de la profondeur et de l'ombre sur le réseau Tor », *op. cit.*
[43] Le terme de service caché est une traduction directe du terme « *hidden service* » utilisé dans la documentation officielle du projet Tor.
[44] M. DODGE et R. KITCHIN, *Mapping cyberspace*, Londres (Royaume-Uni), New-York (États-Unis), Routledge, 2001
[45] M. DODGE et R. KITCHIN, *Atlas of Cyberspace*, 1re éd., Harlow (Royaume-Uni), Addison-Wesley, 2001
[46] « (…) perhaps the most exciting projects are occurring in relation to mapping the informational landscape of cyberspace » *Ibid.*, p. 75

comme réseau (plans et outils de conception de sites à une échelle fine, graphes de relations hypertextes à une échelle plus large) et comme espace de pratiques (cartographie des échanges de courriels, des forums et applications de discussion, ou des jeux vidéo et mondes virtuels). Une partie finale sur les imaginaires du numérique et les représentations de science-fiction concluait l'*Atlas of cyberspace*. Cette pluralité d'approches m'a alors semblé être une démonstration remarquable de la dimension éminemment spatiale du « cyberespace », même lorsqu'elle menait à l'exploration de ce qui s'est trouvé être de fausses pistes en termes de design, par exemple le recours à une métaphore éminemment topographique (le paysage) pour figurer une arborescence de fichiers ou d'instructions (voir Figure 1).



Haut gauche : « Harmony information landscape » par Keith Andrews (univ. de Graz, Autriche), 1994-95, représentant de l'information à propos de la ville de Graz structurée sous une forme paysagère. Citée par Dodge et Kitchin, 2001, p. 139.

Droite : extrait du film Jurassic Park (1:53:10 puis 1:53:20), réalisé par Steven Spielberg, 1993, représentant un « système UNIX » permettant le pilotage de toute l'infrastructure du parc à partir d'une interface également structurée sous forme paysagère. Il s'agit plus précisément de l'interface du logiciel *3D File System Navigator* pour les systèmes IRIX édité par Silicon Graphics en 1993

Figure 1 - Comparaison de deux interfaces de navigation, années 1990 - ville de Graz et Jurassic Park (film)

Mon travail de master 1 se voulait, initialement, assez englobant : il s'agissait de faire une monographie des services cachés de Tor, de rendre compte de leur topologie comme des usages y ayant lieu. À un espace tout nouvellement exploré (et d'un type peu habituel), il semblait préférable d'appliquer une méthode d'investigation éprouvée : j'ai donc abordé cet

espace dans une approche de géographie régionale, avec dans l'idée d'en proposer la première monographie. Fort de ma lecture de Robert Kitchin et de Martin Dodge, puis de la rencontre avec un utilisateur du web .onion ayant mis à ma disposition sa riche base de données de *scraping*[47], mon travail s'est néanmoins rapidement concentré sur une tentative de cartographie des services cachés de Tor. Cette première expérience de recherche a été révélatrice à plusieurs égards.

D'abord, elle a permis à mes directeurs et moi-même de constater que je restais focalisé bien davantage sur l'espace que sur les pratiques spatiales, tropisme sans doute habituel chez les jeunes géographes, mais d'autant plus marqué que je restais circonspect sur la manière de bien traiter en géographe un type d'espace inhabituel dans la discipline. Il me semblait donc opportun de recourir à une approche et à un outil éprouvé en proposant une monographie et une carte d'une région d'Internet. Bien que je me sois aussi intéressé aux représentations sur le « *deep/dark web* » et aux pratiques effectives qui y étaient déployées, le plus gros de mon travail a consisté en la mise en œuvre d'outils proches de l'analyse spatiale au moyen du logiciel de production et d'analyse de graphes Gephi, utilisé peu ou prou comme un logiciel de SIG qui aurait été dédié à un espace de métrique topologique.

Ensuite, ce travail m'a permis de mieux comprendre ce qui, dans l'approche géographique des espaces réticulaires, relevait d'une approche véritablement spatiale d'un côté ou de métaphores spatiales de l'autre. Les critiques apportées par un relecteur de mon article sur le « *deep/dark web* » dans la revue *Netcom* ont plus particulièrement joué. Je retiendrai ici deux références : *Le site et le paysage* de la philosophe Anne Cauquelin[48], et *Critique des réseaux* de Pierre Musso[49]. Elles m'ont permis de tempérer mon enthousiasme initial pour les nombreuses références géospatiales utilisées dans le langage courant pour se référer aux espaces réticulaires, et qui me semblaient un des meilleurs indices de leur caractère spatial. Pierre Musso, d'abord, m'a été précieux pour identifier « l'inflation imagière [face à laquelle] le concept de réseau ne résiste plus »[50]. Musso explique que la notion a connu un âge d'or au cours du XIXe siècle sous l'impulsion des ingénieurs saint-simoniens, qui se fonde sur une conception organiciste de la société : les grands réseaux naturels (hydriques notamment) ou artificiels (ferroviaire, télégraphique…), à l'échelle des sociétés, sont présentés comme analogues aux réseaux artériels et nerveux à l'échelle des corps. Si Musso valide le réemploi de la notion par

[47] Je remercie à nouveau ici Harry71 (pseudonyme) pour ce partage généreux et pour son intérêt.
[48] A. CAUQUELIN, *Le site et le paysage*, 3e éd., Paris (France), Presses universitaires de France, 2012
[49] P. MUSSO, *Critique des réseaux*, Paris (France), Presses universitaires de France, 2003
[50] *Ibid.*, p. 20

l'informatique au XXe siècle, il est en revanche très véhément contre l'approche de la « société en réseau » décrite autant que promue par Manuel Castells, et qu'il décrit comme une « techno-utopie » envahissante[51], une « dilapidation » du sens du terme du fait de son extension à l'ensemble de la vie en société.

Cette invitation à la prudence lexicale se retrouve également chez Anne Cauquelin, qui se concentre sur des métaphores spatiales à une échelle plus fine, comme la navigation ou, surtout, le « site ». L'auteure explore le champ notionnel du terme, qui peut renvoyer au site comme lieu, au site comme à un « là »[52], prolongeant le sens territorial classique du terme, jusqu'à la reprise d'une terminologie architecturale du site avec « son *home*, sa maison à soi (*home page*, *front page*), avec façade et adresse, et les éléments architecturaux qui s'ensuivent : portes, frontons, enseignes, balises, colonnes et portails »[53]. Il peut également renvoyer au paysage, au *sight*, espace *in situ*, par définition « en mouvement », en construction. L'usage de référents territoriaux, pour Anne Cauquelin, procède de la volonté de combler un « hiatus » entre « notre attachement au paysage, au site, aux lieux, et la nécessité d'accéder à un espace de réseaux dont la présence est sentie comme réelle, elle aussi, mais d'une autre sorte de réalité »[54] : les références territoriales volontiers employées pour décrire les espaces réticulaires seraient au fond un « tour de langage »[55].

Le dépassement de cette aporie s'est cristallisé autour de deux éléments. D'abord, une discussion critique avec le chercheur en informatique Emmanuel Saint-James après mon intervention à l'École d'été de cartographie et de visualisation de l'ENSSIB en 2017 sous l'égide d'Éric Guichard. Du fait de son appartenance disciplinaire, il a été particulièrement sensible à mes approximations techniques d'une part et à mon usage de métaphores spatiales d'autre part. Approximations et métaphores relevaient pour partie de problématiques distinctes[56], mais s'inscrivaient également dans cette même logique intellectuellement insatisfaisante pointée aux paragraphes précédents : étant géographe de formation et marqué par l'idée que les espaces internétiques étaient des espaces comme les autres, c'est donc sous

[51] *Ibid.*, p. 241
[52] A. CAUQUELIN, *Le site et le paysage*, *op. cit.*, chap. 1§14
[53] *Id.*§17
[54] *Id.*§28
[55] *Id.*§32
[56] Pour une bonne part, il s'agissait d'une nécessaire montée en compétence et en précision sur les protocoles réseau. Toujours sur les conseils d'Emmanuel Saint-James, je me suis notamment plongé dans les articles de vulgarisation du très riche blog de Stéphane Bortzmeyer, https://www.bortzmeyer.org. Ce dernier est l'un des plus éminents spécialistes français en matière de réseaux informatiques, membre de l'*Internet Engineering Task Force* et du conseil d'administration du principal point d'échange Internet national. Il a également eu l'amabilité de m'apporter ses éclairages à l'occasions de rencontres scientifiques et associatives.

un angle excessivement spatial que j'abordais le fonctionnement matériel et logique des réseaux informatiques. J'étais, en somme, pris dans le « hiatus » langagier pointé par Anne Cauquelin. Une meilleure compréhension des réseaux et de leurs protocoles m'a permis de faire la part de la métaphore et du propos techniquement juste en cette matière. On retrouve la trace de cette évolution dans mon article déjà évoqué à propos du réseau Tor, et qui propose de se garder de l'emploi des expressions *deep* ou *dark web* dans le langage expert pour évoquer les réseaux Internet superposés comme Tor, Freenet ou I2P[57].

Le deuxième moment de dépassement de cette phase de ma recherche s'inscrit plus largement dans les débats qui animent la discipline autour de la définition de son objet, l'espace. Il s'est alors agi pour moi de dépasser, là encore, un enthousiasme initial exacerbé pour une propriété d'Internet finement décrite par Boris Beaude dans *Internet : changer l'espace, changer la société* : la « permanence »[58] de ses contenus, qui fait écho aux travaux précurseurs d'Andrew Feenberg évoqués au chapitre précédent. De cette permanence découlent la possibilité d'interactions asynchrones et la synchôrisation, donc. Mais cette propriété tend également à rapprocher ontologiquement lieux réticulaires et territoriaux et, par glissement, m'a conduit à me focaliser sur l'espace plutôt que sur les spatialités d'Internet. Dans ma volonté d'affirmer la géographicité d'Internet, il était en effet plus facile d'appréhender cet objet encore relativement neuf pour la discipline en me concentrant sur l'espace qu'il est et qu'il déploie plutôt que sur ses spatialités[59]. Si le naturalisme était évidemment impossible pour décrire un objet géographique entièrement artificiel comme Internet, je me suis en somme raccroché au deuxième degré à la conception rassurante de l'« espace positionnel »[60] dans mon approche initiale d'Internet en tant que géographe. Dépassant le récit égogéographique de ce détour par de vieux réflexes disciplinaires pour aborder l'objet de la présente recherche, le chapitre 2 de la partie 1 propose une définition qui met l'accent sur une approche dimensionnelle du social[61] ainsi que sur l'importance fondamentale de l'interspatialité à l'ère numérique.

Il faut néanmoins relever que, si ce dépassement était nécessaire à un géographe forcément plus impliqué dans la prise en compte des développements épistémiques de sa discipline sur son concept central, il n'en est pas moins pertinent aujourd'hui encore de tenter

[57] J.-F. PERRAT, « Un "deep/dark web" ? Les métaphores de la profondeur et de l'ombre sur le réseau Tor », *op. cit.*, § 7
[58] B. BEAUDE, *Internet: changer l'espace, changer la société*, *op. cit.*, p. 55
[59] Pour un développement sur la géographicité comme dimension de la sociétalité adjoignant espace et spatialité, voir J. LEVY, « Espace », dans J. Lévy et M. Lussault (éd.), *Dictionnaire de la géographie et de l'espace des sociétés*, Paris (France), Belin, 2013, p. 353-360
[60] *Id.*
[61] Voir

des cartographies topologiques et non-géospatiales des objets internétiques, et généralement fondées sur des techniques de *crawling*. Il s'agit d'un effort collectif, ouvert et continu depuis 2008 pour le Web en général avec le projet *Common Crawl* (http://commoncrawl.org), qui sert de base de données à de nombreux travaux d'exploration du Web. Plus récemment et à une échelle plus fine, c'est aussi le cas pour une cartographie de YouTube fondée notamment sur les liens entre chaines de publication de vidéo par Bernhard Rieder, Ariadna Matamoros-Fernández et Òscar Coromina à travers leur travail *Mapping YouTube*[62]. Et on ne peut omettre, bien sûr, qu'il s'agit toujours de l'un des métiers fondamentaux de compagnies parmi les plus puissantes du monde, au premier rang desquelles Google au sein du groupe Alphabet.

[62] B. RIEDER, Ò. COROMINA et A. MATAMOROS-FERNANDEZ, « Mapping YouTube: A quantitative exploration of a platformed media system », *First Monday*, vol. 25, nº 8, 3 août 2020 (DOI : http://dx.doi.org/10.5210/fm.v25i8.10667 consulté le 24 mai 2021)

Chapitre 2 - AUX PREMICES DE LA THESE : UNE VOLONTE DE TRANSVERSALITE

Deux idées fortes sont restées de ce premier moment de recherche et ont guidé la suite de mon travail. D'abord, que l'étude des espaces réticulaires pour eux-mêmes et dans leur interspatialité avec l'espace territorial était aujourd'hui encore insuffisante, mais que le cadre de travail en était posé, par des auteurs comme Boris Beaude ou Rob Kitchin notamment. Ensuite, que l'étude des spatialités y était primordiale. On peut certes faire une géographie très riche de l'espace d'Internet, à travers notamment la géopolitique ou les questions d'aménagement de ses réseaux techniques ou de l'architecture et de l'agencement des sites web (WWW, ou web .onion dans mon cas). Mais retenir Internet avant tout comme un espace de synchôrisation implique que ce sont les pratiques qui s'y déploient et qui y émergent qu'il est aujourd'hui important d'étudier.

I - LE CHOIX DE LA THEMATIQUE DE LA VIE PRIVEE

Dans ce contexte épistémique, la thématique de la vie privée s'est rapidement imposée comme centrale, après avoir été la toile de fond de mon étude sur Tor. Cette notion était évidemment mobilisée par les acteurs rencontrés sur le terrain, en particulier ceux du collectif Cafés vie privée, mais aussi par les concepteurs et les promoteurs de Tor[63]. Pour autant, elle n'était pas interrogée pour elle-même dans le mémoire. Au terme de ce travail de recherche liminaire, la question s'est donc posée de savoir quels imaginaires, quelles finalités et quelles urgences motivaient la mise en place d'un réseau tel que Tor ou d'un dispositif de sensibilisation comme les chiffrofêtes[64]. Une autre question d'ouverture consistait à se demander quels étaient les pendants tangibles des pratiques en ligne autour de Tor : s'il était visiblement possible de naviguer incognito sur Internet, était-ce encore le cas dans l'espace géophysique augmenté ?

[63] Il est intéressant de relever que, dans leur présentation du premier protocole grand public de Tor, Roger Dingledine, Nick Mathewson et Paul Syverson mettent d'abord en avant la notion de « *secrecy* ». Pour autant, les nombreuses références à leurs travaux préparatoires qu'ils convoquent dans cette présentation sont clairement inscrits dans le champ des *privacy-enhancing technologies*. Voir R. DINGLEDINE, N. MATHEWSON et P. SYVERSON, « Tor: The Second-Generation Onion Router », dans *Proceedings of the 13th USENIX Security Symposium*, San Diego (États-Unis), The USENIX Association, 2004, p. 303-320 (en ligne : https://www.usenix.org/legacy/events/sec04/tech/dingledine.html)

[64] « Le principe reprend celui des « *install parties* » au cours desquels des utilisateurs et développeurs de logiciels et de systèmes d'exploitation libres (notamment GNU/Linux) aident des néophytes à installer et à prendre en main ces outils. Du reste, la porosité est grande entre ces communautés, et un CVP n'est jamais qu'une variante d'*install party* orientée vers la protection de la vie privée. » J.-F. PERRAT, *Peler l'oignon*, *op. cit.*, p. 34

Existait-il des communautés dédiées à ce sujet, refusant « IRL » (« *in real life* ») ce qu'ils refusaient en ligne ?

Ces questions m'ont notamment conduit à poursuivre mon rapprochement avec des activistes agissant depuis ou en lien avec le milieu du numérique. Depuis la fin des années 1990, des critiques d'art puis des militants et des universitaires ont plus volontiers parlé d'*hacktivisme*, mot-valise formé sur l'anglais *hacker* (ou pirate informatique) et activiste. L'association Attac, en France, en est un des premiers exemples.[65] Le collectif des Cafés vie privée s'étant essoufflé entre 2016 et 2017, je me suis plus particulièrement rapproché de la Quadrature du Net à partir de 2018. Association française historique de défense des libertés civiles dans les domaines de l'informatique et d'Internet, j'y ai trouvé des interlocuteurs nouveaux qui m'ont permis d'approfondir et d'élargir sensiblement les thématiques abordées dans les Cafés vie privée d'Île-de-France, plutôt axés autour d'une logique d'éducation populaire aux bonnes pratiques numériques.

Au-delà de l'aspect empirique de ma sensibilisation aux questions de vie privée dans ce milieu, et qui est allée croissant dans les premiers temps de mon doctorat, il faut en outre rappeler que la thématique de la vie privée numérique avait été mise au-devant de la scène médiatique quelques années auparavant avec les révélations d'Edward Snowden à l'été 2013. Administrateur-système de la Central Intelligence Agency (CIA) puis de la National Security Agency (NSA) travaillant sous couvert d'un contrat avec l'entreprise Dell[66], il fit défection en révélant à la presse l'étendue de la surveillance électronique de masse des personnes à l'échelle mondiale par les agences de renseignement étatsuniennes. Ces révélations m'avaient d'autant plus interpellé qu'elles faisaient un lointain écho à mes découvertes d'adolescent en la matière sur le réseau Échelon[67] (et son pendant français, parfois surnommé Frenchelon), entre lecture d'articles incompréhensibles sur le *phreaking* téléphonique et conversations aux dehors de complot avec mes frères férus d'informatique.

Sur le plan académique, l'importance devenue capitale d'une réflexion sur les menaces effectives que faisaient peser l'informatique connectée sur la vie privée était déjà tout à fait actée, comme en témoigne ce passage du très remarqué *Privacy in context: technology, policy,*

[65] É. GEORGE, « Les usages militants d'Internet », *Communication. Information médias théories pratiques*, vol. 22, nº 2, Editions Nota bene, 15 octobre 2003, p. 99-124 (en ligne : https://journals.openedition.org/communication/4655 ; consulté le 1er septembre 2021)
[66] E. J. SNOWDEN, *Permanent record*, Londres (Royaume-Uni), Macmillan, 2019, p. 214
[67] Le grand réseau de surveillance électronique d'alors, organisé par les États-Unis et quelques alliés, auquel un site amateur bien documenté, reseau.echelon.free.fr, était consacré : https://web.archive.org/web/20020114194508/http://reseau.echelon.free.fr/reseau.echelon/

and the integrity of social life d'Helen Nissenbaum (2010) : « l'informatique est considérée comme une menace majeure contre la vie privée parce qu'elle permet une surveillance généralisée, la création d'immenses bases de données, et la circulation de l'information à l'échelle du monde à la vitesse de l'éclair. En fait, la vie privée est l'un des enjeux sociaux les plus souvent associés aux technologies numériques. »[68] Pour autant, Nissenbaum y pointe également le fait que les théories de la vie privée encore dominantes en 2010 ne permettaient plus de comprendre les réactions individuelles contemporaines aux violations perçues de la vie privées : « Malgré la prolifération et l'omniprésence de ces technologies, systèmes et pratiques, ainsi que des institutions construites autour d'eux, les principales conceptions légales et morales de la vie privée semblent en décalage avec les réactions des individus, que ce soit en minimisant ou en exagérant certaines anxiétés »[69]. Sans diminuer l'importance philosophique ou légale des discours tenus jusqu'alors en matière de protection de la vie privée, des auteurs comme Helen Nissenbaum pointaient le besoin d'un renouvellement des approches de la vie privée, à fonder désormais sur une étude fine des contextes sociaux et pratiques[70] dans lesquels le privé se trouve toujours plus mis à l'épreuve dans la vie quotidienne et la perception des individus.

II - L'AMBITION D'UN TERRAIN A TROIS COMPOSANTES

Forts de ces constats, le choix d'une approche microgéographique s'est imposé. Il s'agissait de saisir en finesse à la fois les limites du privé, mais aussi ses mises à l'épreuve, telles que perçues et expliquées par les individus eux-mêmes. Trois axes de recherche ont alors été dégagés pour couvrir tous les pans de l'expérience géographique des personnes eu égard au problème de la vie privée à l'ère numérique :

- Un premier axe portait sur l'espace public, dans la continuité des *surveillance studies* qui s'intéressent depuis les années 1980 à la manière dont les personnes sont suivies dans leurs actes et déplacements quotidiens hors du domicile, à

[68] « *Information technology is considered a major threat to privacy because it enables pervasive surveillance, massive databases, and lightning- speed distribution of information across the globe. In fact, privacy has been one of the most enduring social issues associated with digital electronic information technologies.* » (trad. pers.) *in* H. F. NISSENBAUM, *Privacy in context: technology, policy, and the integrity of social life*, Stanford (États-Unis), Stanford Law Books, 2010, p. 1

[69] « *Despite the proliferation and virtual ubiquity of these technologies, systems, and practices and the institutions that have grown around them, the preeminent legal and moral conceptions of privacy seem out of step with the contours of public reaction, either by underplaying certain anxieties or exaggerating them.* » (trad. pers.) *in Ibid.*, p. 158

[70] Comme on le verra dans la partie « Deux approches empiriques : Helen Nissenbaum, Bénédicte Rey et la perception convergente des enjeux de vie privée par les résidents étatsuniens et français », p. 61, Nissenbaum parle plus spécifiquement de « *contextual integrity* ».

travers l'utilisation de leurs appareils mobiles (*smartphone* en tête), mais aussi par les infrastructures de contrôle que constituent par exemple badges et portiques d'accès, ou la vidéosurveillance ;

- Un deuxième axe portait sur l'espace domestique, ses limites, et son lien organique au privé, puisqu'il en est légalement et pratiquement l'espace emblématique.

- Un troisième axe consistait à prolonger l'intérêt pour les populations relevant de cas-limites eu égard à leur sensibilité et/ou à leur exposition plus grande à la surveillance numérique : activistes, hacktivistes, journalistes, utilisateurs de Tor… Dans une logique prospective, il s'agissait de voir quelles pratiques étaient déjà mises en place par ces types de personnes dans la mesure où leur cas pouvait préfigurer les niveaux de sensibilité et/ou d'exposition de la population générale à l'avenir. Il s'agissait aussi de tester l'hypothèse selon laquelle certaines personnes appliqueraient dans l'espace public les principes d'action observés dans le travail de recherche précédent sur Tor.

Un long travail initial de réflexion théorique et d'explorations empiriques nous a amenés à focaliser le sujet de la thèse autour de la question du domicile. En effet, les observations menées dans l'espace public ont rapidement montré leurs limites au cours de la première année de travail du fait de leur caractère trop surplombant, qui m'amenait à me focaliser sur les dispositifs et aménagements numériques dans l'espace public, en perdant trop de vue les pratiques et les imaginations fines des individus. En outre, ce travail était déjà largement déblayé par tout un champ de recherche organisé autour des *surveillance studies*, par ailleurs déjà en ordre de marche pour traiter de la question de recherche alors émergente du traitement algorithmique des données collectées dans l'espace public.

A contrario, une intuition de Boris Beaude début 2017 sur l'intérêt de tout nouveaux « gadgets » qu'étaient les enceintes connectées est progressivement apparue comme beaucoup plus prometteuse. Il est à noter que, si Amazon avait lancé l'enceinte Echo en juin 2015 aux États-Unis, elle n'a été disponible en France qu'en juin 2018. Quant à la Google Home, elle a été lancée en novembre 2016 aux États-Unis, et en août 2017 en France. Les premiers retours d'expérience aux États-Unis permettaient donc d'anticiper que ces nouveaux dispositifs cristalliseraient beaucoup de nos intérêts généraux sur le numérique et la vie privée, notamment autour des objets connectés et de la domotique, et qu'ils s'intégraient bien sûr idéalement à une

réflexion sur l'espace domestique. Ils présentaient en outre l'immense intérêt d'être des dispositifs d'un genre nouveau, et constituaient donc un sujet de recherche neuf, au moins pour la France. Le principal risque avec ce choix d'objet de recherche était que le travail empirique à leur sujet arriverait lui-même un peu tôt, avant que suffisamment d'enquêtés potentiels s'en équipent. En tout état de cause, il était acté début 2018 qu'elles seraient un point central du guide d'entretiens mis en œuvre cette année-là. Au bout du compte, il aura effectivement été compliqué de trouver des enquêtés en nombre au moment du travail de terrain, ce qui a limité la taille de mon échantillon. De même, les usages et le reste de l'écosystème de la domotique connectée était encore embryonnaires à l'époque – ce que compense néanmoins le fait que les *early adopters* interrogés se sont très vite équipés de toutes les nouveautés, contrairement à des utilisateurs moins enthousiastes arrivés plus tard. En contrepartie, ce travail de recherche est parfaitement contemporain de l'émergence même de son objet en France.

Quant au troisième axe possible, il a été resserré sur les hacktivistes, et en grande partie sur leur discours attendu comme critique, mais informé, à propos des enceintes connectées et des dispositifs domotiques associés.

*

Le lecteur voudra peut-être m'excuser ce long état de l'art introductif, volontairement organisé autour du récit de la construction du sujet de thèse sur un mode égogéographique. Il m'a en effet semblé que mon parcours intellectuel de jeune chercheur dans le champ de la géographie du numérique (du primat de l'espace et de sa représentation graphique à celui des spatialités, et du primat du territoire numérique à celui de l'espace augmenté), présentait l'intérêt d'être assez représentatif de l'histoire du champ lui-même, au-delà de l'éclairage apporté sur la construction de la thèse elle-même.

Chapitre 3 - LA FOCALISATION SUR LES ENCEINTES CONNECTEES

Le terme d'enceinte connectée désigne une gamme d'appareils informatiques née au cours des années 2010 adjoignant un haut-parleur, un micro, et des capacités réseau (local et internétique). L'utilisateur s'adresse vocalement à ces appareils, qui peuvent en retour simuler une conversation et fournir divers services, comme bien sûr de jouer une musique à la demande, mais aussi piloter un appareil tiers (ampoule luminescente, chauffage, machine à café…), se faire dicter un courriel ou encore passer une commande sur Internet au nom de leur utilisateur, entre autres fonctionnalités.

Si tout dans le design de ces appareils comme dans les communications de leurs fabricants invite à les considérer comme des objets d'une grande simplicité dont l'utilisation ne requiert que de savoir parler, il s'agit en réalité de dispositifs très sophistiqués.

I - « ENCEINTE CONNECTEE » : UNE DENOMINATION A LA SIMPLICITE TROMPEUSE

En première approximation, l'adjonction des termes « enceinte » et « connectée » semble décrire un objet assez banal. Dans le domaine de la technologie, même grand public, il est pourtant courant de vouloir mettre en avant la dimension innovante d'un nouvel outil ou d'une nouvelle technologie, en utilisant une dénomination d'apparence technique, et préférentiellement en anglais. Or, la traduction « enceinte connectée » a été quasi immédiate et son usage s'est très vite répandu en français. L'appellation anglaise d'origine, *smart speaker*, n'est jamais utilisée en France : ni dans le langage courant, ni dans la communication des entreprises ou dans la publicité. En urbanisme, l'expression pourtant proche de *smart city* est loin d'être systématiquement rendue par sa traduction littérale de « ville intelligente ». Il en va de même pour *smartphone* qui, réciproquement, n'est jamais appelé « téléphone intelligent ». Dans ce dernier cas, la traduction officielle dans plusieurs pays, dont la France, adopte à la rigueur une graphie en un mot-valise, ordiphone, qui, à l'instar de l'anglais, accole le terme *smart*, rendu par « ordi », à *phone*, rendant « téléphone ». Cette traduction n'est cependant pas entrée dans l'usage, et le francophone parlera volontiers de *smartphone* quand il importe de faire un distinguo avec un téléphone mobile peu élaboré (*feature phone* ou, plus plaisamment, *dumb phone*, voir Figure 2).

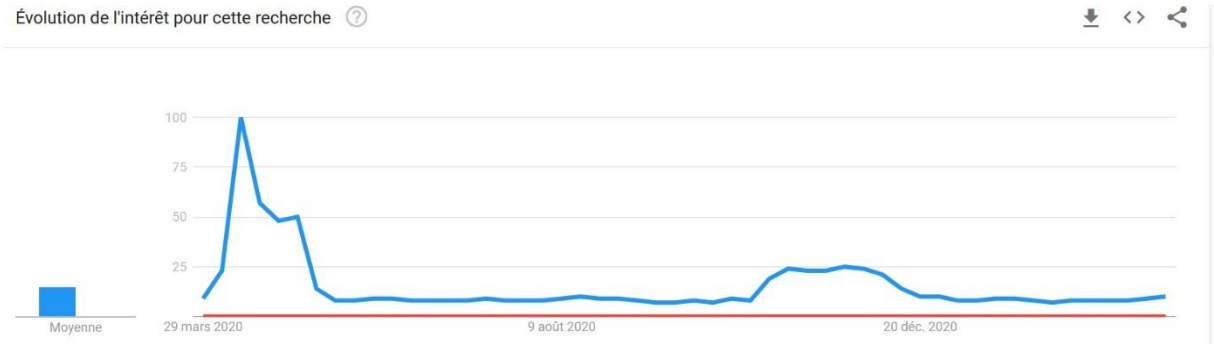


Figure 2 - Graphique Google Trends portant sur la comparaison des requêtes pour les termes « smartphone » (en bleu) et « ordiphone » (en rouge) au 30/04/2021

Ensuite, l'expression « enceinte connectée » ne sonne pas de manière outrancièrement technique. Chacun des deux termes composant l'expression est d'usage tout à fait courant. Le terme « connectée » ne connote pas (ou plus) une sophistication remarquable, comme pouvait le faire par exemple « cellulaire » en son temps par rapport à « mobile » ou « portable » dans le cas des téléphones. Il ne fait pas écho à un nom de protocole, comme 4G ou Wi-Fi, termes bien entrés dans l'usage mais qui n'ont pas de sens naïf. À plus forte raison, nous sommes à mille lieues d'expressions comme *blokchain* ou *dark web* qui recherchent pour diverses raisons la double-obscurité de la technicité et de l'usage de l'anglais.

Dans sa simplicité, l'expression « enceinte connectée » est finalement très proche de « téléphone portable », par exemple. Ni l'une, ni l'autre expression ne parvient au niveau de simplicité du terme « ordinateur », cependant, mais il faut signaler que la traduction de ce dernier terme a été remarquablement soignée[71], et que la commercialisation des *computers* IBM des années 1950 ne nécessitait pas de recourir à des termes immédiatement compréhensibles par une très large clientèle potentielle. Cette simplicité apparente de l'expression « enceintes connectée » n'en est pas moins trompeuse. J'ai ainsi observé, dans des moments de présentation de mon sujet de recherche, que mes interlocuteurs confondaient souvent les « véritables » enceintes connectées de type Amazon Alexa ou Google Home avec les « fausses » enceintes connectées que sont les enceintes pouvant fonctionner sans câble audio ni d'alimentation, généralement au moyen d'une connexion Bluetooth (voir Photographie 1). Par ailleurs, certains technophiles se proposent par exemple de « transformer » leur enceinte Hi-Fi classique en enceinte « connectée » par l'adjonction d'un nano-ordinateur Raspberry Pi et du logiciel Balena

[71] L. DEPECKER, « Que diriez-vous d' « ordinateur » ? », *Bibnum. Textes fondateurs de la science*, FMSH - Fondation Maison des sciences de l'homme, 1er juin 2015 (en ligne : http://journals.openedition.org/bibnum/534 ; consulté le 27 mars 2021)

Sound[72]. Or, les enceintes connectées au sens retenu dans cette thèse sont des objets beaucoup plus complexes que ne le laisse entendre leur dénomination.

Photographie 1 - Comparaison entre une « enceinte Bluetooth » Bose Colour et une « enceinte connectée » Amazon Echo (gen. 1), toutes deux produites en 2014. On peut relever, d'abord, un design très similaire. Les enceintes connectées ultérieures se sont davantage démarquées de l'esthétique de l'enceinte dédiée à l'audio. On peut également noter que l'enceinte connectée est dotée d'une alimentation filaire au secteur, et surmontée d'une LED circulaire très visible lorsqu'elle est activée, comme ici (JFP, 2020)

II - À QUOI SE CONNECTENT LES ASSISTANTS ELECTRONIQUES ?

On l'a dit, l'anglais connaît les enceintes connectées sous le nom de *smart speakers*, mettant l'accès sur la dimension intelligente, réactive de la machine : elle n'est pas un simple périphérique informatique, ni un instrument ne faisant que répondre à des commandes directes. Le français insiste quant à lui sur la dimension connectée de l'enceinte : la machine n'est pas fermée sur elle-même, mais « connectée ». Si l'on cherche à définir cette gamme d'appareils, les deux dimensions sont en fait d'égale importance.

[72] M. LEGOUGE, « Comment transformer votre enceinte en enceinte connectée grâce à Balena Sound et un Raspberry Pi ? », *Clubic.com*, 4 mai 2020 (en ligne : https://www.clubic.com/raspberry-pi/article-891655-1-raspberry-pi-transformer-enceintes-airplay-spotify.html ; consulté le 18 mars 2022)

La connexion est ce qui permet à ces appareils d'être des hubs domotiques, d'une part. Ils peuvent piloter une grande variété de périphériques au moyen de protocoles de communication sans fil, Wi-Fi et Bluetooth en tête, et viennent concurrencer le smartphone qui était jusque-là le principal « carrefour numérique »[73] de ce type. L'un des premiers usages mis en avant par les industriels est ainsi la mise en liaison des enceintes avec des ampoules lumineuses elles aussi connectées, dont on peut faire varier au moins l'intensité lumineuse, voire la couleur, grâce à une commande vocale adressée à l'enceinte. Si l'on ne se concentre que sur cette fonctionnalité de pilotage d'autres objets connectés, les enceintes se présentent comme une tranquille évolution dans l'histoire technique de la domotique. Leur intérêt est alors simplement de fournir une interface d'objet à objet facile à mettre en œuvre, à savoir sans fil et plus ou moins standardisée en termes de protocoles de pilotage[74]. Au-delà de cette connectivité locale sans fil, techniquement assez banale, la connexion des enceintes avec le réseau Internet est une fonctionnalité autrement plus décisive à tous points de vue, et qui permet à ces objets d'être également *smart*. En effet, les logiciels qui permettent aux enceintes connectées d'être aussi « *smart* / intelligentes » ne sont pas installés dans la mémoire des enceintes elles-mêmes, sauf exception[75], mais sur les serveurs de leurs fabricants. Les enceintes connectées sont donc avant tout des interfaces physiques entre un espace sonore et un logiciel distant associant services de reconnaissance vocale, de traitement automatisé du langage naturel (TALN) et d'agent conversationnel.

Malgré leur très faible autonomie fonctionnelle, elles n'en restent pas moins de véritables petits ordinateurs dont la carte mère supporte tous les composants habituels. Les fonctionnalités de base de ces logiciels sont installées localement, ne serait-ce que parce qu'il doit être possible de configurer son enceinte avant de l'avoir connectée à Internet et liée à un profil utilisateur, ou encore parce que l'enceinte doit pouvoir rester quelque peu fonctionnelle même en cas de perte de connexion à Internet. Prenons pour exemple l'enceinte Amazon Echo de première génération (2014), un modèle emblématique de cette gamme d'appareils, et dont il est un des premiers succès commerciaux (voir Tableau 1). Les composants embarqués dans ce modèle restent assez simples. Les normes supportées par le module Wi-Fi et Bluetooth n'étaient

[73] B. BENHAMOU, « L'internet des objets », *Esprit*, nº 3, 2009, § 4 (en ligne : https://www.cairn.info/revue-esprit-2009-3-page-137.htm)

[74] Nous verrons que cette standardisation est en fait toute relative. Les constructeurs d'enceintes connectées ont plutôt intérêt à ce que les autres acteurs industriels et les consommateurs s'inscrivent dans leur suite logicielle.

[75] Cela a notamment été la promesse de la start-up Snips de sa création en 2012 à son rachat en novembre 2019 par Sonos, un industriel historique de l'audio pour 37,5 millions de dollars (seulement). Voir « L'échec commercial de cette fonctionnalité », p. 247.

pas les plus à jour du moment. Les normes Wi-Fi 802.11ac et Bluetooth 4.1, les plus récentes au moment de la sortie de l'Echo, était alors déjà officielles depuis un an. La fiabilité a sans doute été préférée ici à la recherche de performances supérieures.

Tableau 1 – Composants informatiques d'une enceinte Amazon Echo de première génération (2014) après démontage par un technicien d'ifixit.com. Source : https://fr.ifixit.com/Vue+%C3%89clat%C3%A9e/Amazon+Echo+Teardown/33953

Type de composant	*Fonction*	*Nom commercial*	*Spécification*
Processeur	Puce exécutant les instructions du logiciel. Conditionne la réactivité de l'appareil.	ARM Cortex-A8 (2005)	1000 Mhz, un cœur[76]
Mémoire vive	Stockage des données devant être écrites ou lues rapidement (ex : requête vocale de l'utilisateur). Onéreux.	Samsung K4X2G323PD-8GD8	256 Mo
Mémoire morte	Stockage des données ne nécessitant pas de modification rapide ou récurrente (ex : microprogramme). Peu onéreux.	SanDisk SDIN7DP2-4G	4 GB iNAND Ultra Flash Memory
Module Wi-Fi et Bluetooth	Puce pilotant la télécommunication de l'enceinte.	Qualcomm Atheros QCA6234X-AM2D	Wi-Fi b/g/n Bluetooth LE – 4.0

[76] Source : https://developer.arm.com/ip-products/processors/cortex-a/cortex-a8

Le plus remarquable est cependant la capacité de stockage limitée de l'enceinte, dont les 4 Go ne sont manifestement destinés qu'au système d'exploitation de l'Echo, Fire OS, une version dérivée du système d'exploitation Android. Même en admettant que la version de Fire OS adaptée à cette enceinte connectée de première génération soit allégée de sa partie graphique (serveur d'affichage, système de fenêtrage, interface graphique), ce choix d'un stockage très limité est bien le signe que l'enceinte est conçue exclusivement comme un point d'entrée vers les véritables capacités de calcul et les bases de données distantes. Ainsi, les développeurs de *skills*, les applications dédiées à Alexa, se voient présenter le service proposé par Amazon avant tout comme une interface de reconnaissance et de synthèse vocales à laquelle connecter leurs propres logiciels et bases de données *via* des API – logiciels et bases de données qu'Amazon les enjoint bien sûr à héberger sur les serveurs de sa marque Amazon Web Service. Le schéma de la Figure 3 (ci-dessous), tiré des pages introductives des instructions aux développeurs, est à ce titre révélateur. Le service logiciel Alexa est au centre, et même si une enceinte connectée (Echo Dot) est placée au premier plan dans la partie gauche du schéma, c'est accompagnée d'autres appareils pouvant mettre en œuvre Alexa (et qui pourraient être des smartphones et/ou des tablettes, et un ordinateur et/ou une télévision connectée). Là où Amazon et les autres constructeurs insistent auprès de l'utilisateur final plutôt autour du fait que son enceinte connectée est un objet qu'il va pouvoir acquérir, ils indiquent au développeur qu'il va avoir accès à l'environnement sonore de l'utilisateur à travers les logiciels des fabricants d'enceinte. Cette intégration à d'autres appareils est encouragée par Amazon et Google, moins par Apple : en 2020, Amazon ne facturait ainsi que 4 $ aux fabricants intégrant Alexa à leurs appareils[77]. Au-delà de la vente physique d'enceintes, il faut donc aussi tenir compte de ce qu'on pourrait appeler le « *voice assistant as a service* », qui peut être mis en œuvre par des sociétés tierces.

[77] D. PRIEST, « Alexa is starting to ask questions. How should we respond? », *CNET*, s. d. (en ligne : https://www.cnet.com/home/smart-home/alexa-is-starting-to-ask-questions-how-should-we-respond/ ; consulté le 8 septembre 2020)

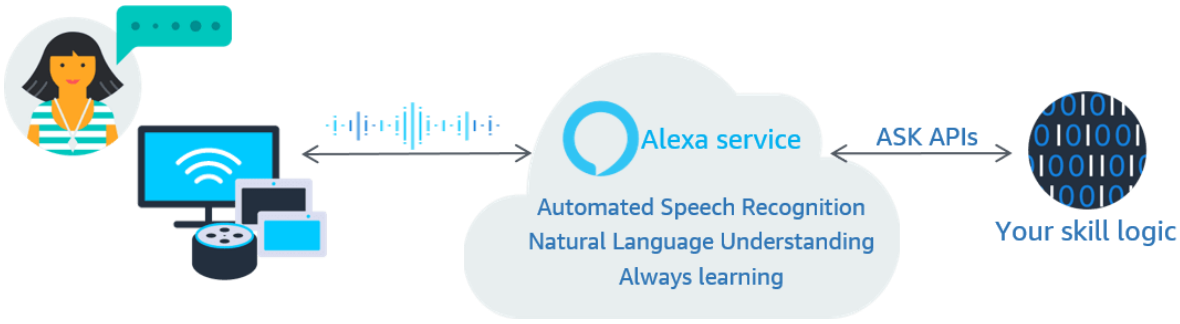


Figure 3 - Dans la documentation dédiée aux développeurs, Alexa est avant tout présentée comme un service de reconnaissance et de synthèse vocale interfaçable avec d'autres logiciels via une multitude d'API. Source: « What is the Alexa Skills Kit? », sur Alexa Developer, sans date (en ligne : https://developer.amazon.com/fr-FR/alexa/techdoc-template.html ; consulté le 9 avril 2021).

Ainsi, il faudrait idéalement adjoindre les approches anglophone et francophone en une seule et même expression pour mieux rendre compte de ce que sont les HomePod, Echo, et autres Google Home : peut-être des enceintes connectées intelligentes, ou encore des enceintes connectées à leur intelligence.

III - UN PROBLEME TERMINOLOGIQUE TRANSITOIRE

Néanmoins, le problème de la définition de l'enceinte connectée comme gamme d'appareils est un problème dont je fais l'hypothèse qu'il ne va pas durer.

La dénomination tient beaucoup au *marketing* des fabricants pour segmenter leurs produits, et la forme même de l'enceinte connectée va rapidement évoluer. Ainsi, Google et Amazon ont d'ores et déjà développé des modèles équipés d'écrans tactiles, qui ne sont donc plus de simples enceintes connectées. Le Google Home Hub doté d'un écran à la diagonale de 7 pouces a été présenté lors de la conférence annuelle de Google en octobre 2018, et il en est aujourd'hui à sa deuxième génération sous le nom de Nest Hub depuis la fusion de la marque Google Home avec la marque Nest[78]. Amazon proposait déjà une enceinte dotée d'un petit écran circulaire de 2,5 pouces de diamètre[79] à son arrivée sur le marché français en 2018, mais c'est

[78] L'entreprise Nest Labs avait été rachetée par Google en janvier 2014, mais est restée une filiale indépendante jusqu'en 2018 où le rapprochement avec la marque Google Home a été fait.

[79] Décrit en ces termes par la journaliste Marie Ciolfi du site d'information *Les Numériques* : « Il ne fait aucun doute que l'écran sert davantage à soutenir ou à étayer la parole d'Alexa qu'à profiter d'un véritable écran à part entière. » M. CIOLFI, « Test Amazon Echo Spot : quand Alexa tourne bien rond », sur *Les Numériques*, 16 septembre 2018 (en ligne : https://www.lesnumeriques.com/assistant-domotique/amazon-echo-spot-p41337/test.html ; consulté le 1er septembre 2021)

surtout début 2019 avec l'arrivée de l'Echo Show et son écran à la diagonale de 10,1 pouces[80] que l'entreprise s'est alignée avec son principal concurrent dans le domaine. L'appellation *smart display* ou écran connecté semble s'imposer pour ces produits. En outre, les assistants vocaux de Google, Amazon ou Apple, pour ne citer que les principaux, sont disponibles dans les produits d'autres marques, comme des enceintes bien sûr, mais aussi les boîtiers TV de certains fournisseurs d'accès à Internet (FAI). *A contrario*, Amazon a également brièvement commercialisé en 2019 un modèle d'Echo nommé Input totalement dénué de haut-parleurs, car destiné à être connecté à des enceintes classiques pour émettre du son[81]. En somme, il y a fort à parier que l'enceinte seule devienne rapidement désuète et que les fonctions d'assistance vocale soient intégrées à d'autres produits, ou bien qu'elle subsiste dans l'entrée d'une gamme dont les formes et les fonctionnalités sont amenées à se diversifier.

En somme, l'objet-enceinte est en soi un pas important dans la phase actuelle de domotisation et de connexion à Internet des objets du domicile, mais ce n'est pas, ou ne restera pas, le plus petit dénominateur commun de la question, à savoir les logiciels distants de dialogue humain-machine et de pilotage domotique du domicile. Un certain nombre d'enjeux en termes de vie privée continueront de se jouer dans les mêmes termes, et de nouveaux apparaîtront. On peut en voir, par exemple, un signal faible dans le nouveau standard de télécommunications 5G mis en place pour les télécommunications mobiles depuis 2019, d'abord en Finlande et en Suisse[82], avant d'être déployée plus largement dans le monde, et à partir de novembre 2020 en France[83]. Par rapport au standard précédent qu'est la 4G, la 5G est conçue pour être, entre autres, mieux adaptée à la connexion d'objets connectés beaucoup plus divers, et peu sophistiqués : sa connectivité est dite non-structurée[84], et elle peut fournir nativement et indépendamment un

[80] M. CIOLFI et V. DE BRYE, « Amazon lance enfin en France son Echo Show », sur *Les Numériques*, 27 mars 2019 (en ligne : https://www.lesnumeriques.com/assistant-domotique/amazon-echo-show-2eme-generation-p51515/amazon-lance-enfin-en-france-son-echo-show-n85315.html ; consulté le 1er septembre 2021)
[81] F. AGEZ, « Test Amazon Echo Input : le galet qui greffe Alexa à votre installation sonore », *Les Numériques*, 16 avril 2019 (en ligne : https://www.lesnumeriques.com/assistant-domotique/amazon-echo-input-p50627/test.html ; consulté le 19 mars 2022)
[82] Z. CHAFFIN, « Téléphonie : la 5G, vedette du Salon de Barcelone », *Le Monde*, 23 février 2019 (en ligne : https://www.lemonde.fr/economie/article/2019/02/23/telephonie-la-5g-vedette-du-salon-de-barcelone_5427273_3234.html)
[83] Anon., « SFR lance la 5G à Nice, avec de nouveaux forfaits », *Next INpact*, 20 novembre 2020 (en ligne : https://www.nextinpact.com/lebrief/44743/sfr-lance-5g-a-nice-avec-nouveaux-forfaits ; consulté le 1er septembre 2021)
[84] C'est-à-dire qu'en bout de chaîne, un objet n'a pas besoin de gérer son propre adressage dans la pile IP : le réseau 5G peut la lui fournir lui-même.

service de géolocalisation[85] ainsi que de notification[86]. En outre, l'un de ses trois sous-standards, mMTC (Massive Machine Type), vise notamment au développement de l'IoT en minimisant la consommation électrique liée aux communications réseaux tout en permettant de gérer la communication avec un grand nombre d'objets connectés dans un espace donné. Cette prise en compte des contraintes de l'IoT est également un des axes de travail pour le prochain standard des protocoles Wi-Fi. Théoriquement, ces technologies pourraient permettre à terme de se passer dans bien des cas de hubs locaux tels que les enceintes connectées (voir le chapitre « Le hub domotique », p. 304). Il faut cependant rester prudent quant à ces promesses de la 5G, car il est de coutume avec les normes de télécommunications que les possibilités techniques de l'heure ne soient pas suivies d'effets pratiques pour le grand public avant le lendemain[87].

L'un des enjeux de la présente thèse n'en en est pas moins de s'interroger sur ce qui fait que l'enceinte connectée, comme objet-pionnier d'usages à venir qui pourraient ne plus s'appuyer nécessairement sur elle, suscite d'intérêts ou de réticences, alors même qu'elle n'est pas en soi le cœur de ce que proposent les services d'assistants connectés. L'enceinte connectée comme objet est un vecteur important, mais non le seul, et certainement pas le dernier, de l'évolution de la conception du privé domestique à l'ère numérique. À titre d'exemple, certaines populations comme celle des personnes condamnées à un placement sous surveillance à domicile sont amenées à rester beaucoup plus contraintes dans l'espace de leur domicile par le dispositif formé par leur bracelet électronique, le boîtier téléphonique et l'institution pénitentiaire que par toutes les enceintes connectées et leurs futurs avatars possibles[88].

Au-delà de la connexion internétique aux serveurs de leurs fabricants, les enceintes connectées permettent aussi la connexion à toute une gamme d'autres objets connectés dans l'espace domestique qui ne peuvent pas tous embarquer un ordinateur et des modules les connectant à Internet, à l'instar par exemple des ampoules connectées. Si l'enceinte connectée matérialise cette connectivité comme hub facilitant le déploiement d'un Internet des objets (*Internet of things*, ou IoT), on a longtemps plutôt parlé de domotique pour désigner cette tendance à automatiser et interrelier divers capteurs, appareils et éléments de mobilier

[85] L'objet connecté peut ainsi, pour peu qu'il soit dans une zone de couverture 5G, se passer d'une puce GNSS de type GPS, Glonass, Baidu ou Galileo.
[86] Les notifications peuvent lui être faites par le fournisseur d'accès lui-même, sans échange de données avec un service tiers.
[87] On prendra pour exemple les applications de la RFC 3626 sur les réseaux mesh datant d'octobre 2003, et dont les applications commerciales n'ont été commercialement accessibles au grand public qu'avec les produits Google Wi-Fi en 2016, ou avec les répéteurs Wi-Fi de Freebox Pop en 2020.
[88] F. OLLIVON, *La prison chevillée au corps. Pour une approche géographique du placement sous surveillance électronique.*, Thèse de doctorat en géographie, Lyon (France), Université Lumière - Lyon II, 2018

domestiques, les termes plus récents comme Internet des objets ou encore *smart home* tendent aujourd'hui à s'imposer. Il s'agira donc aussi de se demander comment les enceintes connectées s'intègrent dans l'histoire technique de la domotique, et ce que nous dit cette évolution lexicale (voir « *Smart home* : l'augmentation de l'espace privé par la domotique », p. 156).

PROBLEMATISATION : LA FIN DU DOMICILE COMME ESPACE PAROXYSTIQUE DU PRIVE ?

Les enceintes connectées et la myriade de périphériques de l'IoT qui peuvent leur être associés introduisent dans l'espace domestique de nombreux capteurs, à commencer par des microphones perfectionnés, mais aussi de plus en plus des caméras ou des détecteurs de mouvement. Connectées à Internet, elles sont opérées par des entreprises très puissantes, au premier rang desquelles Google et Amazon, dont le modèle d'affaires consiste à exploiter les données produites par leurs utilisateurs afin de les profiler. D'autres entreprises comme Apple ou Sonos proposent des enceintes connectées dont le modèle d'affaires repose principalement sur la vente de l'objet même, mais la part de leurs utilisateurs est nettement inférieure, et les fabricants des périphériques connectés à leurs enceintes ne sont pas tenus de garantir un niveau de protection élevée de la vie privée des utilisateurs. De même, si le *smartphone* permet déjà techniquement de réaliser toutes les fonctionnalités des enceintes connectées et même davantage, la spécificité de l'enceinte connectée est d'être attachée en permanence à un espace domestique donné, d'être presque toujours sous tension et opérable dans des conditions optimales, et de disposer de qualités audios supérieures – pour la diffusion et surtout pour la captation du son.

L'introduction des enceintes connectées au sein des espaces domestiques, historiquement construits comme les lieux par excellence du ressourcement et de l'intimité personnelle ou familiale, provoque des réactions de rejet marquées de la part de nombreux individus. L'expérience montre en effet que les pratiques de traçage sur Internet ont déjà mené à une forte érosion de la vie privée en ligne. L'extension de la numérisation du Monde aux espaces domestiques pourrait-elle mener à la fin du domicile en tant qu'espace perçu et conçu comme le lieu paroxystique du privé ?

En prenant appui tant sur les perceptions rapportées par les enquêtés que sur la documentation technique relatives aux nouveaux dispositifs domotiques, cette thèse rendra d'abord compte du caractère éminemment spatial de la notion de vie privée, et défendra l'idée que l'immixtion croissante d'acteurs hypercentraux comme Alphabet/Google et Amazon dans les espaces domestiques entre en conflit avec l'activité immunitaire de la vie privée déployée par les habitants dans et à partir de leur logis (partie 1). Il s'agira ensuite de considérer que les espaces réticulaires ou augmentés n'en sont pas moins habités eux aussi, et peuvent même être

un support de cette activité immunitaire. Un questionnement spécifique autour du *smartphone* permettra de mettre en perspective les menaces et la perception des menaces contre la vie privée, en opposant la fixité des dispositifs domotiques et le caractère nomade et ubiquiste des *smartphones* dans les réseaux cellulaires (partie 2). Je questionnerai ensuite les manières dont le design matériel ou logiciel des dispositifs numériques ainsi que leur régulation légale sont et doivent être prises en compte pour accompagner l'activité immunitaire de la vie privée, et comment ils sont au contraire largement utilisés ou détournés pour tromper l'utilisateur contemporain (partie 3). Enfin, une exploration fine des micro-pratiques de la domotique connectée et singulièrement des enceintes sera conduite selon les quatre axes descriptifs transversaux les plus mobilisés pour décrire ces objets, à savoir la manière dont l'enceinte peut être perçue comme une espionne, un hub, une simple assistance domestique voire un agent social en devenir (partie 4).

METHODE DE RECHERCHE

La présente thèse vise d'abord à saisir le spectre des imaginations[89] et des attitudes relatives à la présence d'enceintes et d'objets connectés dans les espaces domestiques. Plusieurs pistes heuristiques ont été suivies, la notion de vie privée et l'utilisation des médiations numériques traversant l'existence des personnes. Il s'agissait de ne pas se limiter à une étude d'usages des appareils numériques (et singulièrement des objets domotiques connectés), mais aussi d'observer ces pratiques dans la mesure du possible. En outre, pour ce qui est des observations dans la sphère activiste, la question de la vie privée était posée de manière frontale, dans le cadre de réunions publiques ou d'expositions par exemple.

Le principe directeur de cette recherche empirique a été de partir d'objets tout à fait concrets, les enceintes et la domotique connectées, cristallisant aujourd'hui les réactions de défense, de défiance ou d'adhésion au modèle de la mise en médiations numériques croissante du monde et des interactions sociales. Deux hypothèses principales ont été testées :

- L'imaginaire collectif serait préparé à la méfiance envers les capteurs et collecteurs de données, au moins envers les plus ostensibles (comme pour la vidéosurveillance), notamment par les œuvres dystopiques[90] et par l'expérience historique des régimes autoritaires ;
- Il y aurait un attachement à la figure du domicile comme espace paroxystique du privé, nécessitant une protection contre les tentatives d'immixtion commerciales ou institutionnelles[91].

[89] Terme que je préfère à imaginaire lorsqu'il s'agit de marquer l'idée d'un processus de constitution de l'imaginaire.
[90] La référence à *1984* de George Orwell est un lieu commun très usité, mais des œuvres plus récentes comme la série britannique à succès *Black Mirror* (2011-) revient aussi très souvent. Voir « Domotique connectée et science-fiction », p. 354.
[91] C'est pourquoi, outre la question de la domotique qui ne concerne pas forcément directement toutes les personnes interrogées, un certain nombre de questions plus universelles sur les compteurs électriques communicants Linky, dont le déploiement a été rendu difficile au cours des années 2010 pour des raisons sanitaires ou de vie privée, ont également été inclues dans le guide d'entretien.

Observations de terrain

De nombreuses observations de terrain ont été faites, particulièrement dans la phase exploratoire de la thèse, et avant que le sujet ne soit resserré sur l'espace domestique. Dans cette première phase, des observations ont notamment été menées dans des espaces publics très fréquentés pour y observer les pratiques des personnes vis-à-vis des dispositifs numériques, qu'ils leur appartiennent (le *smartphone* est prépondérant, mais tablettes et ordinateurs restent également fréquents selon les lieux) ou qu'ils fassent partie d'infrastructures publiques. Les lieux concernés ont notamment été la dalle du quartier de la Défense à Paris et ses centres commerciaux (CNIT, 4 temps), la gare du Nord à Paris, le centre commercial et la gare de la Part-Dieu à Lyon. On l'a vu, ces observations ont été assez peu concluantes pour observer les pratiques numériques des personnes dans leur finesse, et *fortiori* en relation avec les questions de vie privée.

Des observations participantes ont également été conduites lors d'évènements organisés par des activistes de la vie privée. Je me suis plus particulièrement rendu régulièrement aux réunions publiques mensuelles de la Quadrature du Net entre février 2018 et janvier 2020 à Paris (et à Lyon pour la séance annuelle hors les murs, à l'occasion des Journées du logiciel libre qui se tiennent dans le Rhône), les « Quadrapéros », destinés à faire se rencontrer les membres et sympathisants de l'association ainsi que de collectifs proches (Fédération du Net, Franciliens.net, Résistance à l'agression publicitaire, Exodus Privacy…), après une présentation d'un ordre du jour récapitulant l'évolution des actions en cours. Des événements spéciaux plus ouverts au grand public se sont également tenus lors d'un mois actif de collecte de fonds en décembre 2018, par exemple à la Paillasse[92].

D'autres événements plus divers ont également donné lieu à observation, qu'ils soient liés ou non à la Quadrature du Net, comme une séance d'information conjointe avec le collectif Résistance à l'agression publicitaire dans le local associatif de la Commune libre d'Aligre à Paris, une projection-débat du documentaire *Nothing to hide* au Lycée autogéré de Paris, ou encore l'exposition interactive *The Glass Room Expérience* à la Gaîté Lyrique (Paris), coorganisée par le collectif Tactical Tech et la fondation Mozilla.[93] Quoique les Cafés vie privée franciliens fussent en sommeil lors de la phase de terrain de thèse, un collectif analogue

[92] Un tiers-lieu qui se présente comme « un laboratoire de recherche ouvert et citoyen où sont menées des actions d'amorçage et d'accélération de projets scientifiques, entrepreneuriaux et artistiques. » sur leur site Internet « La Paillasse », sur *La Paillasse*, s. d. (en ligne : https://lapaillasse.org ; consulté le 5 septembre 2021)

[93] « The Glass Room Experience », sur *La Gaîté Lyrique*, 2018 (en ligne : https://gaite-lyrique.net/evenement/the-glass-room-experience ; consulté le 5 septembre 2021)

organisait alors des séances du registre de la chiffrofête ou du café vie privée à Lyon, que ce soit à la bibliothèque municipale de Lyon Part-Dieu ou à la Maison des jeunes et de la culture des Rancy.

La fréquentation de ces lieux ne visait pas à observer des pratiques avec un regard strictement extérieur, proche de celui de l'entomologiste, comme dans les observations de l'espace public. En effet, les questions mêmes soulevées par mon sujet de recherche y étaient frontalement abordées par les organisateurs. Le public présent n'y était pas nécessairement acquis aux principes les plus stricts de la préservation de la vie privée numérique, comme je l'avais déjà observé lors d'observations de terrain des Cafés vie privée franciliens en 2016[94]. J'avais alors été étonné de trouver un public assez hostile à la question, notamment lors d'une séance à la médiathèque de Saint-Germain-en-Laye. De fait, beaucoup de personnes suivent de près ou de loin les ateliers organisés par leur MJC, médiathèque ou autre établissement culturel et artistique local[95]. On pourrait s'attendre à ce que le public se rendant à ce type de manifestations soit déjà sensible aux questions traitées : c'est le cas le plus courant, mais pas le seul. Ce n'était pas un problème du point de vue du recrutement potentiel d'enquêtés, puisque l'ensemble des attitudes possibles était susceptible d'investigation. Surtout, ces observations ont eu pour intérêt de me familiariser avec le discours dominant dans les sphères plus hacktivistes.

Il est à préciser que je m'y suis chaque fois présenté explicitement comme un chercheur travaillant sur la vie privée à l'ère numérique. Ma présence n'a, du reste, jamais surpris, et elle était même des plus banales dans les événements de la Quadrature du Net au cours desquels j'ai rencontré plusieurs autres chercheurs, simples sympathisants ou plus impliqués dans l'organisation ou les prises de parole publiques.

Campagne d'entretiens semi-directifs

Le principe de la campagne d'entretiens menées entre avril 2018 et mars 2020, qui constitue le cœur empirique de la thèse, était de recueillir un large éventail de propos allant des utilisateurs les plus enthousiastes aux critiques les plus affirmés, afin de saisir tout le panel des réactions possibles à l'introduction de ces objets nouveaux que sont les enceintes connectées et la domotique connectée dans les espaces domestiques, en les mettant en perspective avec les

[94] J'avais alors été étonné de trouver un public assez hostile à la question, au moins sur une séance à la médiathèque de Saint-Germain-en-Laye. De fait, beaucoup de personnes suivent de près ou de loin les ateliers organisés par leur MJC, médiathèque ou autre établissement culturel et artistique local. Même si on pourrait s'attendre à ce que le public soit déjà sensible à la question pour se rendre à ce type d'événements, ce n'est en fait pas toujours le cas.
[95] J.-F. PERRAT, *Peler l'oignon*, *op. cit.*, p. 37

conceptions plus générales du privé chez les enquêtés. Ce corpus compte 21 enquêtés[96], en plus de 18 enquêtés potentiels ayant accepté un contact initial lors de phases d'observation sans finalement donner suite pour un entretien à proprement parler, et dont certains propos informels sont rapportés. Il est constitué d'un éventail de personnes d'âges et de contextes spatiaux et professionnels variés. Les entretiens approfondis et longs, allant jusqu'à une durée de 3h30 pour un entretien de couple, ont en outre été privilégiés autant que possibles, pour assurer que l'échange dépasse le stade des réactions superficielles et que les spécificités les plus fines de chaque enquêté puissent avoir l'occasion d'être exprimées, directement ou indirectement[97].

De ce point de vue, et même si la partition entre utilisateurs et non-utilisateurs d'enceintes connectées parfois militants a davantage polarisé ma population d'enquêtés, je me suis efforcé de retenir la méthode appliquée par Bénédicte Rey dans sa thèse de doctorat en sociologie publiée chez Lavoisier sous le titre *La vie privée à l'ère du numérique* (2012) : « Pour ne pas traiter uniquement les préoccupations d'une population d'usagers très avancés gérant leur visibilité avec habitude, (population sur laquelle se base nombre d'études d'usage), les personnes rencontrées ont été [p. 16] choisies parmi une population d'usagers que l'on peut qualifier d'« ordinaires » : utilisant couramment Internet (utilisant au moins Internet — l'usage en complément d'autres technologies de communication n'étant pas exclu) ; étant inscrit sur plusieurs sites Internet ; travaillant ou ayant travaillé avec un accès Internet ; et dont le niveau de compétences informatique est variable. »[98] Cette approche a également été adoptée par Aude Danieli dans son travail de doctorat en sociologie sur les compteurs électriques connectés Linky, *La « mise en société » du compteur communicant* (2018)[99].

Il faut également rappeler que la campagne d'entretiens a été menée à une époque où les enceintes connectées étaient encore relativement peu répandues en France. Il a été difficile de rencontrer des utilisateurs d'enceintes disposés à une rencontre formelle, en particulier à leur domicile. Il s'agit de l'un des premiers résultats autant que de l'une des premières limites de

[96] Pour 16 entretiens effectifs totalisant 30h20 d'enregistrement, plus un entretien réalisé en deux fois trente minutes avec une personne refusant d'être enregistrée.

[97] Il fallait en effet pouvoir dépasser les « schémas pré-réflexifs », nombreux dans le domaine, comme les décrit Michel Lussault : « Affirmer que certains aspects d'une parole d'un individu renvoient aussi à des schémas préréflexifs et non objectivés par celui-ci ne consiste pas à dénoncer l'aveuglement funeste de la personne manipulée par les structures, mais rappelle simplement que l'individu n'est jamais totalement transparent à lui-même, souligne la présence de la société avec sa part, justement, d'opacité et de préréflexivité, dans le langage de l'acteur. » M. LUSSAULT, « Chapitre 1 - Action(s) ! », dans *Logiques de l'espace, esprit des lieux - Géographies à Cerisy*, s. l., 2000, p. 27

[98] B. REY, *La vie privée à l'ère du numérique*, Cachan (France), Lavoisier - Hermes Science, 2012, p. 16-17

[99] A. DANIELI, *La « mise en société » du compteur communicant : innovations, usages et controverses dans les mondes sociaux du compteur d'électricité Linky en France*, thèse de doctorat en sociologie, Marne-la-Vallée (France), Paris Est, 2018

cette source empirique : l'ambition de proposer, par exemple, un atlas des mises en situation d'enceintes connectées *in situ* dans l'espace du domicile n'a par exemple pas pu aboutir.

L'exploitation des entretiens a été faite au moyen du logiciel Sonal, développé principalement depuis 2009 par Alex Alber dans le cadre de ses recherches en sociologie à l'université de Tours[100]. Les enquêtés ont été principalement recrutés par trois voies, en plus de mon cercle social élargi.

Six enquêtés ont été rencontrés dans des magasins vendant des objets électroniques, fréquentés lors de phases d'observation, tels que des FNAC, Boulanger, ou Apple Store, tous situés en région parisienne (trois enquêtés) ou lyonnaise (trois enquêtés). L'intérêt était alors de rencontrer des personnes *a priori* intéressées par les enceintes connectées dans la mesure où elles flânaient dans les rayons *ad hoc*. Le but était également de rencontrer des personnes venant de se doter d'une enceinte connectée dans le but de renouveler l'entretien quelques mois plus tard afin de permettre une approche longitudinale de leurs usages et perceptions de l'objet. Un vendeur a également été rencontré à cette occasion. Les entretiens menés dans cette modalité se sont alors toujours passés sur site : même lorsque le ou les enquêtés acceptaient de me répondre et d'avoir un échange substantiel, ils ont rarement accepté de m'accorder un entretien ultérieur en bonne et due forme (et idéalement à leur domicile), ou n'ont pas redonné suite lors des prises de contact. Seul le vendeur a fait exception, puisqu'il m'a accordé un entretien long dans un café, un an après la première rencontre, et à la suite d'une deuxième rencontre sur son lieu de travail. Neuf des seize enquêtés potentiels dont j'ai finalement rapporté les quelques propos dans mon carnet de terrain plutôt que sous forme d'entretien ont été rencontrés en magasin.

Quatre enquêtés ont été rencontrés dans des événements organisés par des groupes activistes. Trois lors d'un atelier d'éducation populaire à l'utilisation d'outils numériques protégeant la vie privée de leurs utilisateurs lors d'un Café vie privée lyonnais, un lors des réunions publiques mensuelles de la Quadrature du Net à Paris. Ces entretiens ont été menés au domicile des personnes (trois) ou dans un café (un). Six prises de contact ont permis une conversation liminale sur place dans d'autres lieux et événements axés par des activistes, mais n'ont là encore été consignés que dans le journal de terrain sans déboucher sur un entretien en bonne et due forme.

[100] A. ALBER, « Voir le son : réflexions sur le traitement des entretiens enregistrés dans le logiciel Sonal », *Sociologos . Revue de l'association française de sociologie*, nº 5, Association française de sociologie, 13 avril 2010 (DOI : 10.4000/socio-logos.2482)

Trois enquêtés ont été rencontrés en ligne sur des espaces de discussion d'adeptes de domotique et d'enceintes connectées. Un couple via le forum de discussion du site hardware.fr, dédié notamment à l'équipement informatique, un homme sur un groupe Facebook actif d'entraide et d'informations sur l'enceinte Alexa adossé au site lesalexiens.fr. Un autre enquêté, modérateur de groupe des Alexiens, a accepté une rencontre sans que cela aboutisse.

Enfin, huit autres enquêtés, utilisateurs d'enceintes connectées ou plutôt neutres ou opposés au principe, ont été recrutés dans mon cercle social élargi. La plupart n'étaient pas des familiers, mais des parents ou des amis d'amis. L'un est un ami, interviewé pendant la campagne à proprement parler, avec pour particularité d'être affecté d'un handicap lourd conditionnant fortement son utilisation de la domotique et des enceintes connectées, ce qui m'a semblé légitimer le fait de l'interviewer malgré notre proximité. Les deux derniers sont des amis également, avec lesquels j'ai pu tester et affiner le guide d'entretien dans la phase préliminaire de l'enquête. Certains de leurs propos sont néanmoins utilisés dans la thèse, dans la mesure où l'essentiel du guide s'est trouvé validé après l'échange avec eux, et que les sections et questions ajoutées pour le guide lors de la campagne découlent de cette phase préliminaire.

Les enquêtés sont anonymés et nommés par la lettre E suivie d'un nombre. Une présentation synthétique des enquêtés est fournie en annexe (voir p. 431).

Médias et réseaux sociaux

Les médias constituent une part importante des références citées dans ce travail, pour deux raisons principalement. D'une part, sur la question des attitudes quant au privé, ils permettent de donner un « air du temps » relativement aux idées en circulation. À ce titre, ils sont souvent employés à des fins illustratives, comme un matériau factuel de première main. Du reste, au-delà de leur rôle habituel d'animation du débat public d'idées, ils ont parfois même joué un rôle prépondérant dans la diffusion d'informations de nature à transformer les attitudes et surtout les imaginaires sur la question de la vie privée. L'exemple le plus emblématique, dont témoigne la relativement bonne connaissance du cas par les enquêtés, en est bien sûr l'affaire Snowden, dans laquelle les journalistes Laura Poitras et Glenn Greenwald ont joué un rôle capital de relais entre le lanceur d'alerte et leurs pairs. La thèse ne propose cependant pas d'analyse systématique d'ampleur du traitement médiatique en tant que tel des questions de vie privée numérique. D'autre part, la presse, et plus particulièrement la presse spécialisée (*Next INpact*, *Les Numériques*, *Wired*…) a été d'un point de vue beaucoup plus pratique une source d'informations techniques importantes. Bien que je ne me propose pas ici de faire un audit

exhaustif de tous les modèles d'enceintes et d'objets connectés, il me fallait rendre compte de leurs évolutions et nouveautés à la fois nombreuses et contemporaines à la campagne de terrain, sans pour autant avoir un accès de première main aux objets en question, ni m'appuyer exclusivement sur la communication des fabricants. C'est par exemple le cas des écrans connectés ou *smart displays* déjà évoqués en introduction (p. 31).

Cette dernière raison vaut également pour les réseaux sociaux : j'ai notamment suivi les communautés d'entraide entre utilisateurs, très actives pour les gammes d'enceintes connectées d'Amazon et Google, que ce soit sur Facebook, le forum communautaire généraliste international Reddit, ou sur des forums de plus petite envergure, comme hardware.fr. Une veille rigoureuse y était faite par des personnes intéressées au premier titre comme utilisateurs et utilisatrices de ces outils. En outre, j'y ai maintenu une attitude observationnelle assez distante dans la phase de conception du guide d'entretien afin de constater presque *in vivo* quelles étaient les attentes d'utilisateurs potentiels venus chercher des informations, ou les difficultés rencontrées par des utilisateurs effectifs. Par la suite, deux enquêtés ont été recrutés par ce biais.

La documentation technique et promotionnelle

Je m'appuierai également sur la documentation technique produite par les fabricants d'enceintes connectées à l'intention des développeurs d'applications et des fabricants d'objets connectés compatibles. Si la présente thèse se focalise sur la manière dont sont reçus ces objets par les utilisateurs finaux effectifs ou potentiels, il n'en reste pas moins nécessaire de questionner le design de ces objets, la manière dont ils sont conçus en termes techniques et d'usages attendus. En outre, la campagne d'entretiens ayant commencé dans les premiers temps de la diffusion en France de ces objets, beaucoup d'informations sur les produits n'ont longtemps été disponibles que par ce biais, avant même d'être traitées dans la presse, en particulier en ce qui concerne les services logiciels offerts par les enceintes, et la temporalité attendue de leur mise en place marché national par marché national. Un grand nombre des services offerts par ces enceintes n'étaient alors pas encore disponibles sur le marché français – et beaucoup ne le sont toujours pas. Pour autant, ces services ont fait partie depuis le début de la diffusion des enceintes de l'argumentaire commercial, du discours médiatique et de l'horizon d'attente des utilisateurs potentiels. Il importe donc de rendre compte de ces fonctionnalités et de ces usages, ne fussent-ils encore qu'en puissance pour le terrain qui nous occupe.

Recherche-action entre Quadrature du Net et Internet Society

Enfin, une dernière source de données provient d'une recherche-action menée dans le cadre de cette thèse, née de la fréquentation de la Quadrature du Net. S'il s'agissait au départ surtout de me confronter aux discours et aux actions d'un groupe hacktiviste parmi d'autres et de recruter quelques enquêtés, la fréquentation régulière des événements de l'association a mené des membres à m'inviter à participer à un groupe de travail sur la création d'un label pour les objets connectés, porté par le chapitre français de l'Internet Society, l'un des organismes historiques de standardisation d'Internet. L'intérêt de la démarche était d'associer régulateurs publics et parapublics, industriels, milieu associatif, et chercheurs. Elle n'a abouti qu'à la rédaction d'une charte pour l'Internet des objets présentée lors du Forum de la Gouvernance de l'Internet du 4 juillet 2019, et synthétisée dans un document publié en février 2020[101]. Le résultat de ce travail collectif est d'une ampleur très inférieure à ce que le projet initial ambitionnait, mais cette démarche m'a permis d'accéder dans ce cadre à d'autres types d'acteurs que ceux envisagés jusqu'alors, les industriels en particulier, et de mettre en application tout en les questionnant en contexte les apports de ce travail de recherche.

*

Au bout du compte, on observera que des types assez variés de résultats empiriques auront été collectées dans le cadre de cette thèse. Le corpus d'entretiens en est le cœur en cela qu'il donne accès à tout l'éventail des discours sur la vie privée au regard de l'émergence de nouvelles pratiques domestiques, et qu'il informe sur les pratiques fines rapportées par les acteurs eux-mêmes, voire dans certains observées *in situ*. Les autres types de données collectées répondent aussi, quoique plus indirectement, à ces objectifs. Ils élargissent utilement le champ d'observation, même s'ils n'ont pas permis de descendre au niveau de détail permis par des entretiens approfondis. En tout état de cause, cette méthode de recherche, forcément imparfaite, me semble avoir pour mérite de dégager assez tôt les clés d'explorations ultérieures d'un champ de recherche et de régulations futures, l'espace domestique numérisé, encore en pleine transformation.

[101] « Internet Society et Internet Society France présentent 22 recommandations pour un Internet des objets de confiance », sur *Internet Society France*, 5 mars 2020 (en ligne : https://www.isoc.fr/iot-22-recommandations/ ; consulté le 8 mai 2021)

Partie 1 - LA VIE PRIVEE COMME PROBLEME GEOGRAPHIQUE

La notion de vie privée ou de *privacy* pose de redoutables problèmes de définition. Elle est pourtant une catégorie particulièrement mobilisée, que ce soit parmi les spécialistes de disciplines diverses, le législateur et les pouvoirs publics, les activistes, ou encore dans le langage courant. Elle peut être utilisée dans le sens le plus banal, par opposition notamment au travail (et plus encore pour les « personnes publiques »), ou plus largement pour marquer la frontière entre les moments et les espaces où l'individu peut se départir de son identité de personnage de et dans la Cité pour se replier dans sa sphère familiale ou plus strictement personnelle. Elle peut renvoyer aussi bien à des lieux qu'à des temps, à des rapports sociaux, à la vie la plus prosaïque comme à une valeur très abstraite – et pourtant ardemment défendue ! jusqu'à en devenir parfois plus un totem qu'une catégorie pour l'action (chapitre 1).

Rares sont les termes aussi difficiles à manipuler, même pour un géographe habitué à la gymnastique du passage du langage profane au langage savant dans sa discipline – des termes d'usages très larges, comme « espace » ou « territoire », sont par exemple des chausse-trappes épistémologiques et lexicales fameuses. La difficulté majeure posée par le terme est qu'il ne s'agit même pas ici de fustiger un faux-sens, un mésusage par rapport à une définition stable qui serait au moins connue des spécialistes[102], ni même simplement de pointer une polysémie dans laquelle on pourrait au moins dégager une série de sens possibles, des signifiés bien définis quoique placés sous la coupe d'un même signifiant un peu trop usité[103] : tous les sens qui lui sont donnés se valent, se confondent, se nourrissent les uns des autres ou s'opposent parfois. La vie privée fige parfois, mais ne stratifie jamais durablement. Elle est un magma, dont on peut au mieux identifier la cellule de convection (tout ne relève pas de la vie privée), mais dont les mouvements internes sont permanents. Il arrive qu'une de ses expressions se dégage,

[102] Ce qui est par exemple nettement plus courant dans le domaine de l'informatique ou du numérique au sens large.
[103] Toujours en géographie, le terme « région » remporte ici la mention très honorable.

advienne au grand jour et se stabilise – le « Votre vie privée est notre une priorité » dont les variantes fleurissent aujourd'hui dans les fenêtres des navigateurs Web, en est un exemple ; mais il n'y a pas à creuser beaucoup pour retrouver toute la viscosité et l'animation du terme.

Malgré l'impossibilité apparente à définir strictement la vie privée, il est pourtant douteux qu'un terme qui parle autant ne veuille rien dire. On verra dans cette partie qu'une approche interdisciplinaire de la question est féconde et même nécessaire pour aborder une notion aussi ample. L'histoire, le droit et la sociologie seront notamment convoqués pour établir en quoi la vie privée fait toujours problème, et se définit avant tout lorsqu'elle est remise en cause, ce qui est particulièrement le cas dans l'ère numérique contemporaine (chapitre 1). Pour autant, nous verrons rapidement ce qu'une approche spatiale de la vie privée et du privé, à travers des questions comme la caractérisation des lieux ou la circulation des données, apporte un éclairage capital sur la notion, plus particulièrement dans ses dimensions pratiques et pratiquées (chapitres 2 et 3).

Nous finirons par une tentative non pas de définition, mais plutôt de description dynamique du terme en empruntant à Peter Sloterdijk ses métaphores de la bulle et de l'écume pour comprendre moins la vie privée que la manière dont se vit le privé. La notion d'immunité, dans le sens où elle est développée par Sloterdijk, sera plus particulièrement reprise (chapitre 4).

Chapitre 1 - LA VIE PRIVEE, UNE APPROCHE PAR LES TENSIONS

I - UNE DEMANDE SOCIALE ANCIENNE AUTOUR DE LA VIE PRIVEE

La notion de vie privée est aujourd'hui très largement mobilisée, particulièrement dans son rapport aux TIC. En France, c'est au moment de la mise en lumière du projet de fichier SAFARI (système automatisé pour les fichiers administratifs et le répertoire des individus) que la thématique émerge puissamment dans le débat public. Dans un article au vitriol en mars 1974, Philippe Boucher, journaliste au *Monde*, dénonce la mise en place d'un programme visant à centraliser l'accès aux données contenues dans les quatre cents fichiers des services de police et de renseignement, et auxquels le ministère de l'Intérieur envisage d'adjoindre également les données du cadastre ou encore du ministère du Travail.[104] « "Safari" ou la chasse aux Français » provoque un véritable tollé. Le statisticien Michel Louis Lévy parle même d'une « campagne passionnelle »[105], qui finit par inciter le Premier ministre Pierre Messmer à interdire aux administrations de mettre en commun leurs réseaux et bases de données relatives aux personnes. Il promet en outre la création d'une commission Informatique et libertés, qui donnera naissance à la loi éponyme ainsi qu'à la commission nationale de l'informatique et des libertés ou CNIL[106]. Si l'accent est plutôt mis sur les « libertés » dans ces intitulés, l'article 1 de la loi 78-17 du 6 janvier 1978 insiste en premier lieu sur la non-atteinte à « l'identité humaine », et la protection de la « vie privée » est évoquée avant lesdites « libertés » :

> *« L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. »*

À l'époque, c'est notamment la possibilité d'interroger la base de données à partir d'un identifiant unique et individuel, le numéro Carmille, qui a suscité l'opposition. Aujourd'hui plus connu sous l'appellation de numéro de sécurité sociale, il est conçu pour être propre à chaque individu et valable toute la vie durant. Le spectre d'un fichage généralisé de la population et les

[104] P. BOUCHER, « "Safari" ou la chasse aux Français », *Le Monde*, 21 mars 1974, p. 9
[105] M. L. LEVY, « Le statisticien face aux tabous », *Sociétal*, n° 37, 2002, p. 37 (en ligne : http://archives.institut-entreprise.fr/sites/default/files/article_de_revue/docs/documents_internes/societal-37-9-levy-reperesettendances.pdf)
[106] R. FALIGOT, « Du projet Safari au contrôle biométrique : Big Brother est parmi nous », dans *Histoire secrète de la Ve République*, Paris (France), La Découverte, 2007, p. 278-288

références au régime de Vichy ont plus particulièrement justifié cette défiance.[105] Félix Tréguer parle même de « la révélation du programme SAFARI [comme] un véritable détonateur, mettant en lumière le processus d'informatisation des fichiers de police en cours depuis la fin des années 1960. »[107] En tout état de cause, ce sont fondamentalement des craintes liées à l'utilisation de données relatives à l'identité et aux actions des individus dans le cadre de leur vie ordinaire qui ont orienté la création des dispositifs liés à la loi Informatique et libertés. Ce risque a, de nouveau, été bien identifié dans l'expression de « fichier des gens honnêtes », proposée par le sénateur François Pillet (UMP), alors rapporteur de la proposition de loi relative à la protection de l'identité du 27 juillet 2010, et qui a relancé les débats sur le fichage général de la population – en l'espèce, au motif de faciliter la lutte contre les usurpations d'identité.[108] Sans entrer dans les détails de la proposition de loi en elle-même, l'expression de fichage des « gens honnêtes » pointe habilement un paradoxe : d'une part, il n'y aurait pas à s'inquiéter d'être fiché pour quelqu'un d'« honnête », qui n'aurait par définition « rien à cacher » (voir « N'avoir rien à cacher » : criminalité et surveillance, p. 298). D'autre part, si le fichage des individus n'est généralement pas remis en cause quand il est considéré comme justifié (comme dans le cas du casier judiciaire), c'est précisément le fait que ce fichage vise des gens honnêtes et des données personnelles ou biométriques[109] banales et quotidiennes qui provoque le malaise de la tendance représentée par le sénateur François Pillet.

Que retenir de la loi informatique et libertés ? D'abord, la création de quatre droits relatifs à l'inscription des citoyens dans des fichiers, qu'ils soient créés par des acteurs publics ou privés, et qu'ils soient sous format papier ou, évidemment, numérique. Il s'agit du droit d'information (l'individu doit être informé que les informations qu'il fournit abonderont un fichier), du droit d'opposition (l'individu doit pouvoir s'opposer à cette collecte), du droit d'accès (l'individu doit pouvoir accéder aux informations qui le concernent), et du droit de rectification (l'individu doit pouvoir rectifier ces informations au besoin). Ces droits sont censés garantir aux personnes qu'elles conserveront la maîtrise sur les informations qui les concernent, afin de se prémunir de leur éventuel mésusage. Outre ces droits, la loi crée également la première autorité administrative indépendante du paysage institutionnel français, la

[107] F. TREGUER, *Pouvoir et résistance dans l'espace public : une contre-histoire d'Internet (XVe -XXIe siècle)*, thèse de doctorat en histoire, Paris (France), EHESS, 2017, p. 197

[108] J.-M. MANACH, « Le «fichier des gens honnêtes», ce révélateur d'un mal français », sur *Slate.fr*, 1er mars 2017 (en ligne : http://www.slate.fr/story/138356/saga-generalisation-fichier-des-gens-honnetes ; consulté le 27 mai 2021)

[109] Cette proposition de loi incluait notamment la possibilité d'intégrer au fichier des données biométriques, comme les empreintes digitales. La disposition a d'ailleurs fini par voir le jour dans le fichier des titres électroniques sécurisés (TES), autorisé par le décret 2016-1460 du 28 octobre 2016.

commission nationale de l'informatique et des libertés (CNIL), sur laquelle nous reviendrons plus en détail (voir « De la loi informatique et libertés au RGPD », p. 223). On peut toutefois déjà relever que son indépendance par rapport aux autres organes de l'État, et notamment des administrations sous le contrôle du pouvoir exécutif, est un prérequis pour lui permettre de s'assurer de la mise en œuvre des droits suscités. Elle a en outre une mission d'alerte et de prospective à travers les « avis » qu'elle peut rendre, sur saisine ou par auto-saisine, afin d'orienter la décision et le débat publics sur les usages des données informatiques informant sur les individus, et plus largement sur les sujets « de l'identité humaine, [des] droits de l'homme, [de] vie privée, [et de] libertés individuelles ou publiques » mentionnées dans le premier article de la loi de 1978.

De fait, la constitution de fichiers n'est pas le seul motif de réticence manifestée au nom de la protection à la vie privée dans les années 1970, et les agents de la CNIL n'ont pas manqué d'utiliser rapidement son pouvoir d'alerte. Dans un autre des premiers avis de la CNIL, le 16 juin 1981, ce sont de nouveau des craintes d'« atteinte à l'identité humaine et à la vie privée » qui sont mobilisées par la CNIL pour inviter le gouvernement à rejeter le projet AUDASS-Gamin, visant à « la présélection automatisée d'enfants "à risques" susceptibles d'une surveillance médicale et sociale particulière »[110]. Mais au-delà de la question du périmètre des informations mobilisées dans ces bases de données, couvertes par les termes d'identité et de vie privée, l'automatisation est aussi au cœur des problèmes posés par l'informatisation des traitements sur ces fichiers. Dans le projet AUDASS-Gamin, c'est aussi et surtout l'ambition de prédire de futurs comportements jugés déviants sur la base des informations collectées qui a motivé le refus de la CNIL.

Ces exemples canoniques mobilisant la terminologie de la vie privée en lien avec l'outil informatique nous informent sur la nature des réticences courantes en la matière : méfiance envers la collecte et la réutilisation des données, désir de ne pas être individuellement catégorisé ou monitoré dans sa vie quotidienne. Or, les enceintes connectées sont précisément conçues pour s'intégrer dans notre espace domestique et nos activités courantes pour apprendre de nous, de nos pensées et de nos pratiques. Notre paysage sonore privé, voire intime, et plus largement tous les phénomènes pouvant être saisis par les capteurs des objets connectés au domicile, sont amenés à devenir une source de connaissances pour les fabricants et les développeurs de ces solutions techniques. Cette réalité est bien perçue par les internautes interrogés dans le cadre

[110] R. FALIGOT, « Du projet Safari au contrôle biométrique : Big Brother est parmi nous », *op. cit.*, § 13

d'une étude conjointe de la Hadopi et du CSA et, plus étonnant, par les utilisateurs d'enceintes connectées eux-mêmes dans leur panel, qui ne sont pourtant pas plus ou moins inquiets que le groupe témoin relativement à la mise en données de leur vie privée[111].

Si l'expression de « vie privée » est très souvent mobilisée depuis les premiers temps de l'informatisation des sociétés, la notion est cependant plus ancienne, très évolutive, et il convient d'en retracer brièvement l'histoire.

II - ÉVOLUTION DES CONTOURS DE LA NOTION DE VIE PRIVEE

La vie privée : une notion à historiciser

> *« Nous sommes partis de cette évidence que, de tout temps, et partout, s'est exprimé dans le vocabulaire le contraste, clairement perçu par le sens commun, qui oppose au public, ouvert à la communauté du peuple et soumis à l'autorité de ses magistrats, le privé. Qu'une aire particulière, nettement délimitée, est assignée à cette part de l'existence que tous les langages disent privée, une zone d'immunité offerte au repli, à la retraite, où chacun peut abandonner les armes et les défenses dont il lui convient d'être muni lorsqu'il se risque dans l'espace public, où l'on se détend, où l'on se met à l'aise, en « négligé », délivré de la carapace d'ostentation qui assure, au-dehors, protection. Ce lieu est de familiarité. Il est domestique. C'est aussi celui du secret. Dans le privé se trouve serré ce que l'on possède de plus précieux, qui n'appartient qu'à soi, ce qui ne regarde pas autrui, ce qu'il est interdit de divulguer, de montrer, parce que trop différent de ces apparences que l'honneur exige de sauver en public. »*[112]

La recherche universitaire sur la vie privée n'est plus, comme l'écrivait Georges Duby dans sa préface à la monumentale *Histoire de la vie privée* dont il a dirigé la rédaction avec Paul Ariès au début des années 1980, une entreprise « singulièrement périlleu[se, un] terrain

[111] « Les craintes à l'égard de la gestion des données personnelles recueillies par l'enceinte connectée demeurent chez les utilisateurs réguliers et se situent au même niveau que celles exprimées par les non utilisateurs. Les utilisateurs sont ainsi pour deux tiers environ à déclarer craindre pour la confidentialité de leurs données personnelles (62 %) et à estimer que les enceintes connectées constituent une menace pour leur vie privée (61 %). » *in Assistants vocaux et enceintes connectées: l'impact de la voix sur l'offre et les usages culturels et médias*, Paris (France), Hadopi & CSA, 2019, p. 44

[112] G. DUBY, « Préface », dans G. Duby et P. Ariès (éd.), *Histoire de la vie privée - Tome 1 - De l'Empire romain à l'an mil*, Paris (France), Seuil, 1985, p. 10

tout à fait vierge »[113]. On l'a vu, la thématique est même devenue d'une grande actualité médiatique – et scientifique. Si la notion n'a pas aujourd'hui plus qu'alors de définition définitive, le « programme de recherche » livré à leurs lecteurs par ces pionniers reste d'une grande actualité. En dignes historiens, ils ne se risquent en effet pas à une définition trop restrictive, abstraite, légale, ou culturellement située d'une notion dont, précisément, ils prétendent déployer toute la plasticité de l'Empire romain à nos jours. Dans une approche quasi anthropologique, ils proposent plutôt de rendre compte du privé comme d'une « part de l'existence que tous les langages disent privée, une zone d'immunité offerte au repli, à la retraite, où chacun peut abandonner les armes et les défenses dont il lui convient d'être muni lorsqu'il se risque dans l'espace public » (voir ci-dessus). Le point le plus remarquable de cette approche est de distinguer le privé de l'espace privé, tout en liant aussitôt les deux notions.

Le privé relève du sentiment individuel de ce que l'on peut se « [replier] », se mettre en retrait de la vie sociale, se consacrer à l'expérience de son « existence » personnelle. Cette sphère du privée englobe également « ce qui n'appartient qu'à soi » - voire ce qu'il est « interdit » de partager publiquement. En somme, est privé ce qui ressortit d'abord et avant de l'individu en tant qu'individu, indépendamment du regard ou de l'intervention directe de son groupe social.

Sans les confondre, Duby lie cette sphère du privé à un espace (du) privé : il existe des lieux destinés à cette existence privée et qui, sans lui être consubstantielle, lui sont nécessaires. Il évoque principalement les lieux de « familiarité », l'espace « [domestique] » : le domicile, en somme, dont la vocation est de permettre le ressourcement de l'individu en vue de ses responsabilités et activités publiques (travail, sociabilité, consommation…), mais également son épanouissement sans interférence extérieure. Cette thématique de l'espace domestique est un des principaux fils directeurs de l'*Histoire de la vie privée*, qui propose une analyse très détaillée de la configuration des espaces domestiques européens au cours des deux derniers millénaires.

Dans cette relation du privé et de ses espaces, il s'agit fondamentalement d'organiser « l'immunité »[114] des individus. Sous la plume du médiéviste, l'immunité est sans doute à lire dans son sens premier, juridique, de « privilège accordé par le souverain interdisant, à perpétuité,

[113] *Ibid.*, p. 9
[114] *Id.*

à tous ses agents, toute intervention sur les terres du bénéficiaire »[115]. On retrouve ici une dimension spatiale à travers la protection de « terres », appliquée par extension aux espaces domestiques ou quasi-domestiques décrits dans l'*Histoire de la vie privée*. La vie privée est ici conçue comme un domaine à défendre, dont il faut organiser et maintenir la séparation avec l'espace public et les incursions de l'extérieur social, des autres individus et des normes communes.

Tout en nous fournissant un cadre heuristique stable qui permet de traiter de la question de la vie privée sur deux mille ans, un grand apport des rédacteurs de cette *Histoire* est d'abord de montrer à travers une infinie variété d'exemples combien plastique est la notion de vie privée. Paul Veyne décrit ainsi comment un patricien romain pouvait se considérer comme seul dans son jardin ou sa chambre, alors même qu'un esclave le suivait quelques pas en arrière, ou dormait systématiquement en travers de l'entrée de la pièce, toujours à portée de voix. À l'autre bout de l'échelle sociale et en une autre époque, Antoine Prost décrit comment les Napolitains les moins riches du début du XXe siècle, dont la pièce de vie était généralement située au rez-de-chaussée, pouvaient l'étendre provisoirement dans l'espace public de la rue en sortant une table et une chaise, brouillant ainsi la distinction entre les sphères publiques et privées – mais sans, pour autant, que tout l'éventail des pratiques privées, notamment intimes, puisse s'y déployer.

Pour autant, et sans méconnaître la variété des acceptions de la notion dans l'histoire, le géographe Jean-François Staszak s'appuie en 2001 sur l'*Histoire de la vie privée* pour proposer une définition synthétique de l'espace domestique par les traits suivants :

- « anthropique »,
- « différencié » : les fonctions y diffèrent selon les lieux, eux-mêmes séparés par les murs et le mobilier,
- « privé » : les habitants sont maîtres de leur espace et y sont protégés de l'extérieur,
- « familial »,

[115] R. MARTIN, « Immunité », dans *Dictionnaire du Moyen Français*, Nancy (France), ATILF - CNRS & Université de Lorraine, 2020 (en ligne : zeus.atilf.fr/scripts/dmfX.exe?LEM=immunit%E9;XMODE=STELLa;FERMER;;AFFICHAGE=0;MENU=menu_dmf;;ISIS=isis_dmf2020.txt;MENU=menu_recherche_dictionnaire;OUVRIR_MENU=1;ONGLET=dmf2020;OO1=2;OO2=1;OO3=-1;s=s13532b0c;LANGUE=FR; ; consulté le 1er juin 2021)

- dimensionné par les « corps »,
- le « territoire fondamental » de l'individu, où il se ressource entre deux sorties à l'extérieur et avec lequel il construit un rapport affectif profond.

Cette définition est forcément contestable sur le temps long, par exemple en ce qui concerne la différenciation des lieux dont nous venons de voir qu'elle n'était pas nettement marquée encore au début du XXe siècle dans le cas napolitain décrit par Antoine Prost. Elle est tout aussi contestable aujourd'hui dans de nombreuses régions du Monde, en particulier hors des pays les plus développés, et singulièrement pour les centaines de millions de personnes habitant des bidonvilles. Elle n'en reste pas moins satisfaisante pour décrire un type assez général, surtout pour les pays d'Europe et d'Amérique du Nord, et donc pour le cas français sur lequel nous nous focalisons ici.

Les fondements de l'approche contemporaine de la vie privée

Les manifestations et les conceptions du privé ne sont donc pas fixes dans le temps, quoiqu'elles soient susceptibles d'une périodisation. On l'a vu avec l'exemple du fichier SAFARI pour la France, l'émergence de l'informatique puis des TIC dans la deuxième moitié du XXe siècle a constitué un tournant important. Mais le cadre conceptuel contemporain relativement à la vie privée commence à se mettre en place à la fin du XIXe siècle aux États-Unis avec la mise en place d'un droit à ce que l'anglais américain désigne alors sous l'appellation de *privacy*.

L'impulsion de Louis Brandeis, un avocat qui deviendra juge de la Cour suprême des États-Unis de 1916 à 1939, est de ce point de vue déterminante en cela qu'il est le principal artisan de la jurisprudence de la *privacy* aux États-Unis. Son article séminal, « *The Right to Privacy* », co-écrit avec Samuel Warren mais dont Brandeis est le principal rédacteur, est publié en 1890 dans la *Harvard Law Review*, et il est présenté encore en 1953 comme « peut-être l'un des plus connus et certainement le plus influent des articles jamais écrits dans une revue juridique »[116]. L'article est souvent présenté comme définissant le droit à la *privacy* comme un

[116] « (…) perhaps the most famous and certainly the most influential law review article ever written » M. B. NIMMER, « The Right of Publicity », *Law and Contemporary Problems*, 1953, p. 203 (en ligne : https://scholarship.law.duke.edu/cgi/viewcontent.cgi?referer=https://en.wikipedia.org/&httpsredir=1&article=2595&context=lcp)

« droit à être laissé tranquille » (« *right to be let alone* »), ce qui n'est pas tout à fait exact[117], ce qui laisserait entendre que la *privacy* renverrait à la notion de tranquillité et à d'autonomie individuelle, ce qui, là encore, est réducteur, comme on va le voir. La principale originalité de l'article et son intérêt pour nous est de formaliser juridiquement les contours du privé par rapport à une possibilité posée comme nouvelle de captation et de diffusion massives d'informations personnelles à propos des individus, du fait du développement de la photographie instantanée et de la presse à scandales. Si ces deux développements peuvent, de prime abord, sembler éloignés de celui des technologies numériques, Brandeis et Warren proposent dans leur texte un cadre de réflexion encore étonnamment pertinent pour comprendre les questions de *privacy* même cent trente ans plus tard.

Brandeis fonde sa proposition d'un *right to privacy* sur l'analyse de décisions de justice convergeant vers l'interdiction de diffuser des images ou des propos de personnes qui n'avaient pas vocation, pour les plaignants, à être diffusés. Brandeis observe que ces décisions, si elles se fondent formellement sur des droits déjà bien connus (propriété et rupture de contrat notamment), n'en réclament pas moins une extension spécifique de la notion de propriété et de protection des individus à travers la notion de *privacy*, précisément du fait d'un changement de paradigme social et technique : « tant que l'état de l'art photographique impliquait que le portrait d'une personne ne puisse facilement être pris sans qu'il pose en toute conscience, la loi relative aux contrats ou à la confiance pouvait peut-être se contenter de compter sur les précautions usuelles pour se prémunir de la circulation de son portrait » (« *While, for instance, the state of the photographic art was such that one's picture could seldom be taken without his consciously "sitting" for the purpose, the law of contract or of trust might afford the prudent man sufficient safeguards against the improper circulation of his portrait ;* (…) »). Autrement dit, c'est le contexte technique antérieur qui ne justifiait pas de penser la *privacy* en tant que telle, du moins du point de vue juridique, et sans préjuger du fait que le souci de leur *privacy* pouvait exister auparavant chez les justiciables. Brandeis poursuit : « (…) mais depuis les dernières avancées de l'art photographique qui ont rendu possible de saisir des images subrepticement, les doctrines du contrat et de la confiance sont inadéquates pour garantir les protections requises, et il faut désormais s'appuyer sur le droit délictuel » (« (…) *but since the latest advances in photographic art have rendered it possible to take pictures surreptitiously,*

[117] Il faut d'ailleurs relever que Brandeis n'invente pas ce concept juridique, qu'il emprunte au juge Cooley dans son manuel *Cooley on Torts*, publié en 1878. Ce droit étant aux immixtions par d'autres personnes privées la protection que les citoyens étatsuniens se voyaient déjà garantir par le quatrième amendement de la Constitution des États-Unis contre les immixtions sans mandat par les autorités publiques.

the doctrines of contract and of trust are inadequate to support the required protection, and the law of tort must be resorted to »). Le premier terme intéressant ici, et qui fait de nouveau fortement écho à la période présente, est « *surreptitiously* », qu'on peut rendre par « subrepticement ». Il s'agit ici de dire que les atteintes à la *privacy* sont devenues beaucoup moins directes qu'auparavant, moins visibles par les victimes, du fait d'améliorations techniques. On verra que c'est tout l'enjeu de la question du consentement éclairé (ou non) au partage de tout ou partie de leurs données personnelles pour les individus. Le deuxième duo de termes intéressants est la revendication à passer du cadre des « doctrines du contrat » à celui du *tort*, c'est-à-dire la responsabilité délictuelle et donc de la question de l'indemnisation d'un préjudice individuel du fait d'une action d'un autre individu. En somme, il s'agit moins d'assurer le respect de la parole donnée que celui de l'intégrité même des individus.

Ainsi, Brandeis inscrit l'avènement du droit à la *privacy* comme une évolution presque naturelle dans l'histoire de la *common law*. Cet avènement naît, certes, d'un moment de crise liée à une rupture technique, mais trouve ses principes dans un temps beaucoup plus long. L'auteur propose une rapide histoire de la *common law* sous l'angle de la protection des droits individuels, qui a d'abord visé à préserver l'intégrité physique des personnes (contre la « *battery* » et l'« *assault* »[118], soit les coups et blessures), celles de leurs biens et de leurs terres (droit de propriété) puis, par extension, des « *sensations* » des personnes. Là encore, sous l'angle de la physicalité d'abord, à travers la protection contre les « *nuisances* » (odeurs, fumées, vibrations) puis, finalement, sous un angle plus émotionnel et spirituel, à travers la protection des idées et sentiments constitutifs de leur identité. En somme, « toutes les formes de possession – tangibles aussi bien qu'intangibles »[119].

Au-delà de la question de la légitimité de la captation de données, le texte traite d'un autre versant de la question de la vie privée, à savoir son inscription spatiale et particulièrement la circulation des informations personnelles. Il s'agit d'abord de poser la « sacralité » des espaces de la « vie privée et domestique » : « la photographie instantanée et les journaux ont envahi l'enceinte sacrée de la vie privée et domestique »[120]. Non seulement sont-ils sacrés, mais l'expression introduit l'idée que l'espace domestique est le lieu d'élection du privé, sans forcément que tous les aspects de la vie privée (« *private life* ») s'y concentrent exclusivement

[118] S. WARREN et L. BRANDEIS, « The Right to Privacy », *Harvard Law Review*, vol. 4, n° 5, 15 décembre 1890, p. 194
[119] « *every form of possession – intangible, as well as tangible* » *Ibid.*, p. 193.
[120] « *instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life »* (trad. pers.) *in Ibid.*, p. 195

– d'où l'usage des deux adjectifs. L'idée est sans doute de ne pas exclure de la réflexion les espaces privatifs commerciaux ou partagés (hôtels, alcôves, vestiaires…) en se focalisant néanmoins sur le domicile. Rien ici de très surprenant pour nous après la lecture de l'*Histoire de la vie privée* (voir « La vie privée : une notion à historiciser », p. 50). En revanche, reprenant la thématique des nouvelles possibilités techniques de son temps, Brandeis ajoute que « (…) de nombreux appareils mécaniques menacent de faire advenir la prédiction selon laquelle « ce qui est murmuré dans le cabinet sera proclamé sur tous les toits »[121]. Il reprend une métaphore domestique en opposant le « murmure dans le cabinet » (*closet*[122]) à la « proclamation sur tous les toits ». L'expression semble dériver d'un passage de la Bible : « C'est pourquoi tout ce que vous aurez dit dans les ténèbres sera entendu dans la lumière » (Luc, 12 :3). Ce faisant, Brandeis signale un passage de l'intérieur à l'extérieur de la maison, et donc de l'espace affecté au privé, à l'espace public, l'extérieur, les toits, la rue. La transgression est renforcée par une gradation phonique, du « murmure » à la « proclamation ». Il n'est plus ici question de savoir quelle est la nature de l'information diffusée, comme lorsqu'il était question de portraits photographiques ou d'écrits épistolaires, mais de quel espace elle provient et vers quel espace elle va.

Un autre concept avec une dimension spatiale se retrouve chez Brandeis et Warren, celui d'immunité, terme également utilisé par Duby. La notion de *privacy* est en fait pour eux une catégorie : « (…) le droit à la *privacy*, en tant que partie du droit plus général à l'immunité de la personne, le droit de chacun à sa propre personnalité »[123]. Ce passage de l'article me semble mieux rendre compte de leur définition du droit à la *privacy* que « *the right to be let alone* » pourtant plus souvent cité par leurs lecteurs. En somme, chaque individu a droit au respect de son immunité, physique et mentale, et la *privacy* consisterait justement en cette immunité mentale, de sensation, d'opinion, de propos, de sentiment. On peut donc traduire la *privacy* par le privé en français, au sens de ce qui n'appartient qu'à soi. Les deux notions recouvrent notamment celle d'intimité, au sens de ce qui n'appartient qu'à soi et qu'on veut protéger du regard extérieur. Il existe en effet un registre d'informations qui relèvent du privé, qui pourraient

[121] « (…) *numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed form the house-tops"* » (trad .pers.) *in Id.*

[122] La traduction de l'expression « *coming out of the closet* » est souvent rendue par « sortir du placard », mais le terme renvoie plutôt au « cabinet » français, quoique le terme soit plus désuet dans notre langue. La première entrée du dictionnaire Merriam-Webster pour *closet* est d'ailleurs intéressante : « *an apartment or small room for privacy* ». Voir « Closet », Merriam-Webster, (en ligne : https://www.merriam-webster.com/dictionary/closet ; consulté le 18 juin 2021).

[123] « (…) *the right to privacy, as a part of the more general right to the immunity of the person, - the right to one's personality* » (trad. pers.) *in* S. WARREN et L. BRANDEIS, « The Right to Privacy », *op. cit.*, p. 207

être intime, mais qu'on consent à partager, voire à mettre en scène pour autrui : l'extime[124]. Le terme extimité, forgé par le psychanalyste Jacques Lacan, a ensuite été notamment repris par le psychiatre Serge Tisseron dans *L'Intimité surexposée* pour décrire la tendance grandissante à l'exposition de soi, dont l'émergence de la télé-réalité et notamment de l'émission *Loft Story* en 2001 en France lui semble un phénomène révélateur[125]. Il observe, au cours des deux décennies suivantes, une expansion du phénomène à une échelle beaucoup plus large avec la démocratisation d'Internet et la possibilité pour tout un chacun de s'exposer en ligne, d'abord à travers le *blogging*, puis plus fortement encore grâce aux réseaux sociaux comme Facebook par la suite[126]. Quoiqu'il en soit, il s'agit là encore d'organiser son immunité, puisque ce partage est ici choisi, et que les internautes ont appris, sur les blogs comme ensuite sur les réseaux sociaux, à mettre en place des « stratégies de mise en visibilité de soi » dans une dialectique entre l'incitation à la pudeur et l'incitation à la monstration[127]. Cette acception de la *privacy* comme consistant à réguler la diffusion de ce qu'on estime privé a été reprise par de nombreux auteurs[128].

Quant au terme de « *private life* », il est peu utilisé par Brandeis et Warren dans leur article fondateur, et plutôt dans un sens restreint qui correspond aux actes de la vie quotidienne effectué dans un cadre plutôt domestique, et plus ou moins intime. Cette acception n'est pas vraiment celle du français, qui emploie souvent l'expression « vie privée » de manière beaucoup plus large, qui correspond davantage à celle de la *privacy*. François Rigaux fait également de la vie privée ou *private life* une composante de la *privacy*[129]. Bénédicte Rey relève néanmoins que si l'expression française est d'usage courant, elle ne constitue pas toujours une bonne traduction de *privacy* : les *privacy policies* des sites web sont ainsi généralement traduites par « politique de confidentialité » ou « protection des données personnelles ». Si l'utilisation de l'expression « vie privée » ne lui semble généralement pas problématique – elle la retient

[124] Le psychiatre Serge Tisseron définit l'extimité comme « le processus par lequel des fragments du soi intime sont proposés au regard d'autrui afin d'être validés » *in* S. TISSERON, « Intimité et extimité », *Communications*, vol. 1, nº 88, 2011, p. 84 (en ligne : https://www.cairn.info/revue-communications-2011-1-page-83.htm ; consulté le 18 juin 2021)
[125] S. TISSERON, *L'Intimité surexposée*, Paris (France), Ramsay, 2001
[126] S. TISSERON, « Intimité et extimité », *op. cit.*
[127] L. MELL, « Une dialectique de la pudeur : les pratiques de mise en visibilité de soi sur Facebook », *tic&société*, vol. 10, nº 2-3, ARTIC, 30 avril 2017 (DOI : 10.4000/ticetsociete.2088)
[128] Bénédicte Rey cite notamment Westin : « le droit pour les individus, les groupes ou les institutions de déterminer pour eux-mêmes quand, comment, et dans quelle mesure de l'information les concernant peut être communiquée à autrui » A. F. WESTIN, *Privacy and Freedom*, New York (ÉUA), Atheneum, 1967 ; ou encore Ackerman (2004) ou Lancelot-Miltgen & Volle (2005).
[129] F. RIGAUX, « L'individu, sujet ou objet de la société de l'information », dans P. Tabatoni, *La protection de la vie privée dans la société d'information*, s. l., Presses Universitaires de France, 2002, p. 122-137

d'ailleurs pour le titre de son ouvrage sur la question, elle recommande de parler plutôt « du privé » ou de la « question du privé »[130].

En tout état de cause, on comprend aisément pourquoi le texte de Brandeis et Warren a fait date et continue d'être très cité. Il ne se cantonne pas à expliquer ce qui justifie de prévenir juridiquement la diffusion publique du texte d'une lettre, d'une photographie, ou d'une conversation privées – en témoigne la jurisprudence préexistant au texte, dans laquelle cette prévention était déjà effective ; il a également permis de baliser ce qu'il y avait à défendre et les raisons de le faire dans un cadre d'exposition grandissante de la vie privée du fait des évolutions techniques du temps. Il reste encore très fécond pour la réflexion contemporaine sur la vie privée, y compris dans le contexte français[131], même si nous allons voir que les évolutions techniques de l'ère numérique, quoiqu'elles prolongent certains des questionnements de Brandeis et Warren, nécessitent d'affiner encore notre appréhension du privé.

III - LA VIE PRIVEE EN SITUATION

Comme on l'a vu dans l'approche adoptée dans le texte fondateur de Brandeis et Warren, les conflits judiciaires sont une matrice puissante de la réflexion sur les contours de la *privacy* et de la vie privée. Ils permettent, ainsi que l'approche historienne des rédacteurs de l'*Histoire de la vie privée*, de cerner le champ définitionnel de la vie privée autour de principes comme son lien avec l'identité et l'intégrité mentale des personnes, articulée autour de l'idée que ces dernières devraient pouvoir conserver la maîtrise sur la circulation des informations non-publiques qui les concernent. La logique plus générale dans laquelle s'inscrivent ces questions est celle de la gestion de l'immunité du privé. On discerne bien cependant dans cette approche une difficulté d'ordre méthodologique : si l'on peut cerner les contours de ce qui relève du privé, il n'est pas possible de donner une définition positive et définitive de la vie privée, puisqu'elle relève en dernière analyse des choix de chaque individu dans sa gestion de son immunité. Dans sa préface à *Understanding privacy*, le juriste Daniel Solove décrit ainsi sa quête initiale – et infructueuse – d'une telle définition : « Lorsque j'ai commencé à explorer les problèmes de

[130] B. REY, *La vie privée à l'ère du numérique, op. cit.*, p. 14

[131] La question de savoir si la transposition des traditions et problématiques juridiques étatsuniennes et françaises fait débat. Elles seraient irréductibles d'après le postulat de Whitman, mais je suivrais plutôt en cette matière Jean-Louis Halpérin, qui montre que les intrications et références entre ces traditions sont en réalité très fortes. Voir J.-L. HALPERIN, « Protection de la vie privée et privacy : deux traditions juridiques différentes ? », *Nouveaux cahiers du conseil constitutionnel*, n° 48, juin 2015, p. 59-68 (en ligne : https://www.conseil-constitutionnel.fr/node/1308/pdf)

privacy, j'ai tenté d'atteindre une définition définitive de la « privacy », mais mon immersion dans cette question m'a forcé à l'humilité. Je n'ai pas trouvé de réponse satisfaisante. Cette lutte a fini par me faire prendre conscience du fait que la privacy est une pluralité de choses différentes et que la quête pour l'essence singulière de ce concept était une impasse. Il n'y a pas de conception surplombante de la privacy, elle ne peut qu'être péniblement cartographiée par une étude attentive de son panorama. »[132] Rey abonde plus prosaïquement, en relevant qu'« il n'existe pas de définition qui fasse l'unanimité de ce que l'on peut considérer comme relevant de la sphère du privé »[133]. Quant à Helen Nissenbaum, elle est plus critique encore : « Les tentatives pour la définir ont été notoirement controversées et critiquées comme vagues et inconsistantes – en étant trop larges, ou trop restrictives, ou insuffisamment distinctes d'autres valeurs et concepts » ; elle va jusqu'à parler d'« ambition désespérée »[134].

Le consensus scientifique auquel je souscris ici est donc que les questions de privé à l'ère numérique ne peuvent s'envisager que dans un contexte, une situation dans lequel il faut tenir compte finement de l'individu, du design des dispositifs techniques qu'il emploie, des pratiques de gestion des données des acteurs avec qui il interagit (particulièrement des entreprises, mais aussi les acteurs publics), ainsi que du cadre légal et de régulation. Chaque contexte est le lieu de tensions plus ou moins vives, dans lesquelles les limites du privé de chacun évoluent selon la manière dont ces tensions se résolvent selon les cas. Bénédicte Rey adopte ainsi une « approche [de la] notion par les tensions en étudiant les problèmes et en analysant leur sens »[135]. Nissenbaum parle quant à elle de la *privacy* comme étant « inscrite dans un contexte » (« *in context* ») - c'est le titre de son principal ouvrage sur la question, et définit plus précisément un cadre de réflexion à travers sa notion de « *contextual integrity* », sur laquelle nous reviendrons[136].

Deux attitudes se dégagent dans la littérature au sujet du privé à l'ère numérique, une fois posé le constat qu'une définition simple et unifiant de la notion est une impasse : d'une

---

[132] « *When I first began exploring privacy issues, I sought to reach a definitive conclusion about what "privacy" is, but after delving into the question, I was humbled by it. I could not reach a satisfactory answer. This struggle ultimately made me recognize that privacy is a plurality of different things and that the quest for a singular essence of privacy leads to a dead end. There is no overarching conception of privacy—it must be mapped like terrain, by painstakingly studying the landscape*. » (trad. pers.) *in* D. J. SOLOVE, *Understanding privacy*, Cambridge (États-Unis), Harvard University Press, 2008, p. IX

[133] B. REY, *La vie privée à l'ère du numérique*, *op. cit.*, p. 11

[134]« *Attempts to define it have been notoriously controversial and have been accused of vagueness and internal inconsistency – of being overly inclusive, excessively narrow, or insufficiently distinct from other value concepts* » et « (…) *hopeless ambition* ». Voir H. F. NISSENBAUM, *Privacy in context*, *op. cit.*, p. 2

[135] B. REY, *La vie privée à l'ère du numérique*, *op. cit.*, p. 16

[136] H. F. NISSENBAUM, *Privacy in context*, *op. cit.*

part, le *mapping* évoqué par Solove, que ce dernier met en œuvre à travers l'élaboration d'une taxonomie élaborée[137]. D'autre part, une approche de nature plus fondamentalement heuristique et idiologique qui privilégie les approches au cas par cas, à la manière adoptée par Rey et par Nissenbaum. L'une et l'autre approche procèdent d'allers-retours constants entre théorie et pratique, mais la première a une vocation plus formelle et descendante, là où la seconde relève davantage d'une méthode d'appréhension de l'empirie.

Une approche taxonomique

Pour Daniel Solove, il importe de ne plus chercher à définir l'essence d'un concept de *privacy*, toujours trop réducteur ou trop extensif. C'est pourquoi il prend le parti de la « [conceptualiser] par le bas plutôt que par le haut »[138], et après avoir acté l'aporie constituée selon lui par une approche d'ordre strictement philosophique. Ce, afin d'embrasser la multiplicité des acceptions de la notion. Pour autant, il argue que « toute conceptualisation doit se faire à un certain niveau de généralité », et qu'une « théorie implicite » de la *privacy* est de toute façon présente même dans les propos qui se veulent les plus pragmatiques[139]. Il va plus loin en arguant que la théorie qu'il développe « généralise au-delà de la myriade des contextes spécifiques »[140], en particulier des différents contextes culturels et historiques. Les problèmes de *privacy* qu'il analyse auraient été rencontrés, tout ou partie, dans « la quasi-intégralité des pays industrialisés à l'ère numérique »[141]. *De facto*, les cas qu'il développe dans ses recherches sont essentiellement nord-américains et européens[142]. Les sociétés ne différeraient que par l'importance accordées aux valeurs affectées par l'atteinte à la vie privée (s'introduire sciemment dans l'ordinateur d'un journaliste est universellement condamnable, mais sera

[137] Le terme d'« élaboration » vise ici à distinguer l'approche de Solove des typologies beaucoup plus courantes et de moindre ampleur explicative. Kim Bartel Sheehan évoque par exemple les « *traditional typologies of consumer privacy concern [which] suggest that consumers fall into three distinct groups: One-fourth of consumers are not concerned about privacy, one-fourth are highly concerned, and half are pragmatic, in that their concerns about privacy dépend on the situation presented.* » K. B. SHEEHAN, « Toward a Typology of Internet Users and Online Privacy Concerns », *The Information Society*, vol. 18, nº 1, 2002, p. 21-32 (en ligne : https://www.academia.edu/312464/Toward_a_Typology_of_Internet_Users_and_Online_Privacy_Concerns ; consulté le 2 juillet 2021)

[138] D. J. SOLOVE, *Understanding privacy*, *op. cit.*, p. 9

[139] « *Even if we eschew attempts to conceptualize privacy, we are relying in part on implicit understandings of privacy whenever we discuss it.* » *Ibid.*, p. 171

[140] *Ibid.*, p. 9

[141] *Ibid.*, p. 183

[142] Le principal exemple non européen qu'il développe sur quelques paragraphes, p. 184 et suivantes, est celui de la tribu Mehinacu, dans l'Amazonie brésilienne, dans laquelle les individus vivent de manière très collective, essentiellement en plein air, et dont les maisons abritent systématiquement plusieurs familles, ce qui limite fortement la possibilité d'une intimité individuelle dans l'espace domestique – que compensent les possibilités d'isolement seul ou à plusieurs dans la forêt. Sont également évoqués d'autres espaces non-atlantiques au fil de l'eau, par exemple à travers l'évocation d'un jugement de la cour suprême indienne ou autre à l'appui de son propos.

probablement davantage condamné dans une démocratie accordant une importance forte à la liberté de la presse). Si cette affirmation d'universalité est pour le moins cavalière à l'échelle du Monde, elle est sans doute recevable de part et d'autre de l'Atlantique. Enfin, Solove adopte une approche qui se veut focalisée sur les « *privacy* problems », provoquant la « disruption » des activités des individus ou, plus largement, ce qu'il appelle les « *privacy invasions* » en un sens général.

Dans le deuxième chapitre *d'Understanding Privacy* dédié aux limites des approches de la vie privée antérieures à son texte, Daniel Solove propose un panorama des différentes approches historiques de la vie privée :

> *« 1) le droit à être laissé tranquille ["the right to be let alone"] (théorisé par Samuel Warren et Louis Brandeis)*
>
> *2) l'accès limité au soi – la capacité à se prémunir des intrusions d'autrui ["limited access to the self – the ability to shield oneself from unwanted access by others"]*
>
> *3) le secret – le fait de pouvoir cacher certaines informations à autrui ["secrecy – the concealment of certain matters from others"]*
>
> *4) le contrôle sur ses informations personnelles – la capacité à contrôler les informations dont autrui dispose à propos de soi ["control over personal information – the ability to exercise control over information about oneself"]*
>
> *5) la personnalité – la protection de son individualité et de sa personnalité ["personhood – the protection of one's personality, individuality, and dignity"]*
>
> *6) l'intimité – le contrôle ou l'accès limité aux relations et aux aspects intimes de la vie d'autrui ["intimacy – control over, or limited access to, one's intimate relationships or aspects of life"] »*[143]

Cette énumération a pour principal intérêt de circonscrire le champ notionnel de la *privacy*. Implicitement, il s'agit d'une première « taxonomie » de la *privacy*, que Solove propose de dépasser à travers sa propre « *New Theory of Privacy* »[144]. Il s'agit en outre d'un cas où le privé ne traduit pas la *privacy* : il ne s'agit pas de définir ce qui est privé, mais les moments justifiant ce que j'appellerais une pratique immunitaire, de défense ou de contrôle de l'information personnelle. Chacune des approches décrites ici par Solove implique en effet un contrôle-sur ou une protection-contre, et ce plutôt du point de vue des individus.

[143] D. J. SOLOVE, *Understanding privacy*, *op. cit.*, chap. 2
[144] *Ibid.*, p. 8

Pour autant, il me semble que Solove ne fait pas à proprement parler ici une histoire de la notion, mais présente l'ensemble des facettes qu'il identifie dans la réflexion philosophique, légale et judiciaire sur la *privacy* – et pas nécessairement dans l'ordre chronologique. Du reste, notre lecture approfondie du texte de Brandeis et Warren dans la partie précédente a bien montré que leur texte insiste finalement moins sur le « *right to be let alone* » qu'ils reprennent à Cooley, et traite au moins autant de ce que Solove décrit comme le « *control other personal information* » la « *personhood* » ou l'« *intimacy* », et mêle donc plusieurs « approches » différentes dans le texte même qui fonde la première qu'identifie Solove. Au bout du compte, et ce dernier le dit d'ailleurs lui-même : « chacune de ces conceptions de la *privacy* développent une ou plusieurs dimensions de la notion, et chacune est éclairante à de nombreux égards »[145].

Cette énumération semble donc avant tout préparer la proposition de taxonomie de Solove lui-même, qu'il reprend dans *Understanding Privacy* en 2008 après l'avoir proposée une première fois dans l'article « *A Taxonomy of privacy* » en 2006[146] (voir Tableau 2 ci-dessous).

[145]»« (…) *each of the conceptions of privacy described in this chapter elaborates upon certain dimensions of privacy and contains many insights* » (trad. pers.) *in Ibid.*, p. 37

[146] D. J. SOLOVE, « A Taxonomy of Privacy », *University of Pennsylvania Law Review*, vol. 154, nº 3, janvier 2006, p. 477-560 (en ligne : https://papers.ssrn.com/abstract=667622 ; consulté le 21 juin 2017)

Tableau 2 - La taxonomie des atteintes à la vie privée de Daniel Solove (2006)

Collecte d'information (*information collection*)	Surveillance (surveillance)
	Interrogation (*interrogation*)
Traitement de l'information (*information processing*)	Agrégation (*aggregation*)
	Identification (*identification*)
	Insécurité (*insecurity*)
	Utilisation secondaire (*secondary use*)
	Exclusion (*exclusion*)
Dissémination de l'information (*information dissemination*)	Rupture de confidentialité (*breach of confidentiality*)
	Divulgation (*disclosure*)
	Mise en lumière (*exposure*)
	Facilitation de l'accès (*increased accessibility*)
	Chantage (*blackmail*)
	Appropriation (*appropriation*)
	Distortion (*distortion*)
Invasion (*invasion*)	Intrusion (*intrusion*)
	Interférence décisionnelle (*decisional interference*)

Pour le juriste qu'est Solove, ces *privacy problems* sont d'abord à voir sous l'angle du conflit : il s'agit explicitement pour lui non de se perdre dans « le labyrinthe conceptuel de la *privacy* »[147] - comme l'auraient fait ses prédécesseurs - mais de fournir un outillage conceptuel

[147] « (…) *the conceptual labyrinth of privacy* » dans D. J. SOLOVE, *Understanding privacy*, *op. cit.*, p. 11

« lucide, exhaustif et concret »[148], à l'intention notamment du législateur. C'est pourquoi sa taxonomie se fonde avant tout sur des pratiques (« *activities* ») pouvant attenter à la *privacy*. En somme, Solove consacre un temps à la présentation de la variété des options philosophiques et des attitudes des personnes quant aux questions de *privacy*, puis une typologie des cas où cette *privacy* est mise en cause. On sent davantage, dans cette deuxième taxonomie, que Solove raisonne en juriste, et donc sur la base du contentieux possible, à la manière de Brandeis et Warren notamment. Sa taxonomie s'appuie d'ailleurs sur celle de William Prosser[149], célèbre juriste spécialisé de la responsabilité délictuelle, et qui avait fait la synthèse des cas judiciaires appuyés sur « *The Right to Privacy* » dans la cinquantaine d'années qui ont suivi sa publication. Solove justifie cette mise à jour, pour ainsi dire, de la taxonomie de Prosser, par l'émergence postérieure des TIC.

Les problèmes de *privacy* identifiés par Prosser portaient essentiellement sur l'identité et la réputation des personnes, qu'il s'agisse de salir une réputation ou de se l'approprier notamment, et ce, que l'information diffusée soit vraie ou fausse. Dans la taxonomie de Solove, l'appropriation d'identité n'est plus posée comme un problème fondamentalement lié à la *privacy*, et l'essentiel des enjeux relève désormais de la captation ou de l'élaboration de données personnelles autant que de leur diffusion. Le deuxième point de la taxonomie de Solove, « *Information processing* », qui développe le plus grand nombre de pratiques problématiques, est ainsi absent ou très implicite dans la taxonomie de Prosser. Il est le point qui acte le plus nettement le passage à l'ère numérique : c'est désormais moins l'accès aux informations ou à la vie privée d'une personne qui pose problème que leur circulation. La divulgation (*disclosure*) simple est toujours un problème, par exemple dans la presse à scandales que visaient déjà Warren et Brandeis dès la fin du XIXe siècle. Mais la nouveauté est l'importance prise par l'agrégation (*aggregation*) et l'utilisation secondaire (*secondary use*) des données, rendues possibles à très large échelle grâce aux TIC ; ces usages sont plus particulièrement le fait des entreprises de courtage de données publicitaire (*data broking*) dont le modèle d'affaires consiste à maximiser le profilage des consommateurs afin de vendre aux annonceurs l'accès à une base de données d'individus à la fois large et détaillée, pour assurer une diffusion de publicités ciblée

[148] *Id.*

[149] « 1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity that places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness. » Dans W. PROSSER, « Privacy », *California Law Review*, nº 48, 1960, p. 383-389

pour espérer le plus grand nombre possible de « conversions » (à savoir un achat faisant suite à l'exposition à une publicité).

Dans l'approche de Solove, c'est donc moins qu'auparavant l'individu ou son identité en soi qui importent dans le questionnement sur les atteintes à la vie privée. Sans qu'il le formule ainsi, Solove affirme le besoin d'un changement d'échelle dans l'appréhension des problèmes du privé. Il prend le contrepied de l'idée longtemps admise que le droit à la *privacy* serait d'abord un droit individuel :

> *« Par contraste, j'ai avancé l'idée que, lorsque la privacy protège l'individu, elle le fait dans l'intérêt de la société. Les libertés individuelles devraient être justifiées selon leur contribution à la vie sociale. La privacy ne protège pas seulement du contrôle social, elle est en fait une forme socialement construite de protection. Sa valeur n'émerge pas de [chacune des acceptions du terme], mais de l'éventail des pratiques qu'elle protège. »*[150]

Cette thèse est également une des bases argumentatives de l'essai *'I've Got Nothing to Hide' and Other Misunderstandings of Privacy*[151], dans le contexte post-attentats de New York en 2001 qui a vu les droits individuels nettement affaiblis par le *Patriot Act*. L'argument est notamment développé dans le chapitre « Pourquoi la vie privée n'est pas seulement un droit individuel » (« *Why Privacy Isn't Merely an Individual Right* »)[152]. Il ne s'agit donc pas pour Solove de promouvoir le droit à la vie privée seulement pour protéger l'identité ou les données personnelles d'une personne, que ce soit contre l'État ou contre des acteurs privés.

À l'arrivée, il défend son approche comme étant « assez souple pour tenir compte de l'évolution des attitudes concernant la vie privée, et malgré tout assez rigide pour demeurer stable et utile »[153]. C'est ce dernier point qui limite pour nous la portée du propos de Solove. Sa vocation, on l'a vu, est de servir d'abord au législateur et aux magistrats. Bien qu'il s'appuie

---

[150] « In contrast, I have argued that when privacy protects the individual, it does so because it is in society's interest. Individual liberties should be justified in terms of their social contribution. Privacy is not just freedom from social control but is in fact a socially constructed form of protection. The value of privacy does not emerge from each form of privacy itself but from the range of activities it protects. » D. J. SOLOVE, *Understanding privacy*, *op. cit.*, p. 173-174

[151] D. J. SOLOVE, *« I've Got Nothing to Hide » and Other Misunderstandings of Privacy*, Rochester (États-Unis), Social Science Research Network, 2007

[152] *Ibid.*, p. 47

[153] « *(…) flexible enough to accommodate changing attitudes toward privacy, yet firm enough to remain stable and useful »* D. J. SOLOVE, *Understanding privacy*, *op. cit.*, p. 9

sur des cas concrets notamment issus de la jurisprudence et que son texte soit nourri de réflexions issues d'autres champs disciplinaires, en particulier la philosophie, cette approche des problèmes de vie privée ne fournit pas un outillage conceptuel suffisamment varié pour véritablement « comprendre la vie privée », ou du moins enquêter sur le sujet du point de vue plus large des sciences sociales. En revanche, la taxonomie de Solove reste tout à fait utile pour décrire les pratiques attentatoires à la vie privée en stabilisant le vocabulaire sur les manières dont sont utilisées les données personnelles à l'ère numérique.

Deux approches empiriques : Helen Nissenbaum, Bénédicte Rey et la perception convergente des enjeux de vie privée par les résidents étatsuniens et français

Helen Nissenbaum et Bénédicte Rey s'accordent avec Daniel Solove sur l'impossibilité de définir conceptuellement la vie privée ou la *privacy* dans l'absolu. Elles s'accordent également avec lui sur l'idée que c'est en mettant la vie privée à l'épreuve que ses contours se dessinent. En revanche, là où Solove a cherché à monter en généralité à partir de cas judiciaires pour établir une taxonomie des pratiques attentatoires à la vie privée, Nissenbaum et Rey proposent une méthode plus empirique, une heuristique de la vie privée.

C'est plus particulièrement chez Nissenbaum qu'on lit une prise de position très tranchée sur la question. Après avoir énuméré les nombreuses approches possibles des travaux plus essentialistes, qui ont eu à décider si la *privacy* était un concept descriptif, normatif ou légal, si elle s'appliquait à l'information, aux pratiques, aux corps, de la manière de définir les informations personnelles devant véritablement être protégées au nom de la *privacy* ou encore les liens de la notion avec l'intimité, le secret, la confidentialité, etc., Nissenbaum affirme vouloir prendre parti pour la rupture, et travailler « sur » la *privacy*, sans forcément en donner une définition absolue :

> *« Par contraste, ce livre n'explore pas cet inquiétant torrent de systèmes et de pratiques à travers le concept de vie privée. Il ne prétend pas dégager de chemin dans ce bourbier conceptuel pour atteindre une définition, ma définition, de la vie privée. Il n'en reste pas moins un livre sur la privacy car il explique pourquoi le gigantesque et grandissant ensemble de systèmes techniques et de pratiques appuyées sur ces technologies continue de*

provoquer de l'anxiété, des protestations et des résistances au nom de la vie privée »[154]

Elle met plus particulièrement « l'anxiété, les protestations et les résistances au nom de la *privacy* », avant d'évoquer la « confusion, la résistance et parfois la résignation exprimées tant par les experts que par les profanes ».[155] Autrement dit, elle met l'accent sur les attitudes individuelles *en réaction aux* problèmes de vie privée plutôt que *sur les* problèmes de vie privée eux-mêmes, comme le fait Solove.

Rey adopte aussi une approche centrée sur les individus et les problèmes qu'ils rencontrent, avec une justification mettant plutôt l'emphase sur le fait que ce n'est qu'en cas de problème que les individus se soucient vraiment de leur vie privée :

> *« Afin de saisir ce que peut être le privé à l'ère du numérique, le choix a été fait d'approcher cette notion par les tensions en étudiant les problèmes et en analysant leur sens : « étant donné que les individus ne semblent pas concernés par la question de la privacy à moins qu'elle soit menacée ou qu'elle subisse une ingérence, la définition de la privacy découle de la nature de la menace » dont il est question, note Sheehan (2002)*[156]*. »*[157]

Si je souscris à l'idée que c'est lorsque le privé est en jeu qu'on peut mieux en dessiner les « contours mouvants », je suis plus circonspect quant à l'affirmation reprise de Kim Bartel Sheehan sur l'apparente désinvolture des internautes quant à leur vie privée hors de moments où elle serait mise en jeu. Sheehan utilise une fois dans son article le terme « paradoxe »[158] sans s'y appesantir, mais les prémisses du *privacy paradox* sont ici bien présentes. Nous reviendrons dans la partie dédiée à la critique de cette notion (voir « Le chantage du *privacy paradox* », p. 195). En tout état de cause, Nissenbaum et Rey partagent bien ici avec Solove cette même approche fondée sur l'étude des *privacy problems*, même si ces deux premières se focalisent davantage sur les individus et leurs attitudes que ce dernier.

---

[154] *« In contrast, this book does not mediate its investigation of the unsettling stream of systems and practices through the concept of privacy. It does not carve a pathway through the conceptual quagmire to claim a definition — its definition — of privacy. Nevertheless, it is a book about privacy because it explains why the huge and growing set of technical systems and technology based practices have provoked and continue to provoke anxiety, protest, and resistance in the name of privacy. »* (trad. pers.) *in* H. F. NISSENBAUM, *Privacy in context*, *op. cit.*, p. 2

[155] « *bewilderment, resistance, and sometimes resignation expressed by experts and nonexperts alike* » *Ibid.*, p. 3

[156] K. B. SHEEHAN, « Toward a Typology of Internet Users and Online Privacy Concerns », *op. cit.*

[157] B. REY, *La vie privée à l'ère du numérique*, *op. cit.*, p. 16

[158] K. B. SHEEHAN, « Toward a Typology of Internet Users and Online Privacy Concerns », *op. cit.*, p. 21

Chez Rey, la méthode est assez directe, et consiste par exemple à évoquer une technique nouvelle pour sonder les réactions de ses enquêtés. Dans sa partie 3.2, elle développe ainsi la question de la RFID[159] en rendant compte des réactions des personnes interrogées. Rey va ensuite distinguer entre celles et ceux qui en acceptent le principe, qui le tolèrent sur une carte de transports en commun mais refuseraient l'implantation d'une puce RFID sous-cutanée, ou encore qui préfèreraient que l'identifiant soit anonyme[160]. Cette méthode robuste au cas par cas est filée dans l'ensemble de son texte, et les divers aspects de telle ou telle technique sont évoqués selon la manière dont ils révèlent un problème de privé.

Nissenbaum a quant à elle une ambition plus générale. En particulier, et par opposition avec Solove notamment, le cadre juridique lui semble une mauvaise approche à long terme pour la régulation des conflits de vie privée en cela que les acteurs les plus puissants (États, entreprises) y auraient des ressources supérieures aux particuliers[161]. De même, les plaidoyers fondés sur des valeurs jugées fondamentales, comme l'intégrité des personnes ou la liberté d'expression, lui semblent peu opérationnels pour régler les litiges comme pour les législateurs. C'est dans l'entre-deux qu'elle inscrit sa proposition : poser la question du cadre d'intégrité contextuelle (*framework of contextual integrity*) dans lequel sont inscrits les échanges de données à caractère privé entre des acteurs. Il ne s'agit donc pas seulement d'espérer trouver une définition absolue de ce qu'est la vie privée, et qui subsumerait l'ensemble des litiges possibles – l'auteure acte le caractère éminemment protéiforme et relatif aux personnes comme aux cultures de la notion de vie privée. Il ne s'agit pas non plus de se fonder seulement sur l'ensemble des litiges déjà résolus pour dire la jurisprudence de la vie privée.

Dans l'entre-deux, Nissenbaum propose donc de tenir des « contextes », c'est-à-dire d'« arrangements socialement structurés dont les caractéristiques évoluent dans un temps parfois long, et qui résultent des causes et des contingences à la fois des finalités attendues, de

[159] Pour *radio frequency identification*. L'appellation désigne de petits systèmes, pouvant être intégrés dans une étiquette, un badge d'accès aux transports en commun, une puce sous-cutanée… et qui joignent une puce contenant des données d'identification et une antenne qui permet à cette puce de communiquer avec un terminal extérieur via des ondes radioélectriques. Les dispositifs RFID peuvent être équipés d'une batterie ou, très souvent, être "passifs": c'est alors le lecteur RFID qui va fournir de l'énergie à courte distance à la puce RFID et lui permettre d'être lue.

[160] B. REY, *La vie privée à l'ère du numérique*, *op. cit.*, p. 113-115

[161] « *The trouble with settling conflicts through brute clashes among interest holders is the advantage it gives to those possessing advantages of power, resources, and the capacity for unremitting persistence, favouring corporate and governmental actors over the public interest in the long run.* » H. F. NISSENBAUM, *Privacy in context*, *op. cit.*, p. 8

leur cadre spatial, culturel, historique, et plus encore. »[162] En somme, de tenir compte du contexte social dans lequel s'inscrivent acteurs et actions. Plus spécifiquement, Nissenbaum suggère de s'appuyer sur les « rôles », les « activités », les « normes » et les « finalités[163] » dans lesquels s'inscrivent la circulation des informations privées[164]. Cela lui permet notamment de détacher la notion de privé des seuls secret (« *secrecy* ») ou contrôle (« *control* ») de chacun sur ses données personnelles – j'ajouterais également la notion d'intimité à cette liste. Un exemple utilisé à plusieurs reprises par l'auteure s'appuie sur les données de santé : un patient hospitalisé peut se trouver sous une surveillance extrêmement fine par une équipe médicale connaissant tout de son état physique et de ses paramètres physiologiques en temps réel. La plupart des patients n'y trouvent rien à redire, puisqu'ils sont justement des patients suivis par des médecins (rôles) dans le cadre d'une démarche thérapeutique (activité) encadrée par des règles et une déontologie strictes (normes) afin de les conserver ou de les rendre en bonne santé (finalité). Tant que l'intégrité de ce contexte est maintenue, aucun problème de vie privée ne fera jour. Si l'intégrité de ce contexte est changée ou remise en cause ultérieurement, la donne change : par exemple, si le médecin transmettait les données de santé de son patient à une entreprise à but commercial sans consentement explicite. *A contrario*, il est possible d'envisager des ajustements de ce contexte qui ne remettent pas fondamentalement en cause son intégrité. L'auteure évoque les réflexions de la fin des années 2000 sur l'évolution du cadre déontologique de la confidentialité médecin-patient par le département de la Santé et des Services sociaux des États-Unis (*United States Department of Health and Human Services*) : dans le cas où la santé du patient est liée à des facteurs environnementaux pouvant affecter d'autres personnes et/ou si son état est susceptible d'avoir une incidence sur la santé d'autres personnes, la stricte confidentialité individuelle ne vaudrait plus, et les médecins pourraient voire devraient légitimement alerter les pouvoirs publics afin de prévenir d'autres dommages sanitaires. Il s'agirait ici d'un changement marginal et acceptable de la norme dans un contexte où il est de plus en plus admis que la santé individuelle est liée à la santé publique et vice-versa : il s'agit alors, même indirectement, de contribuer à la santé du patient individuel.[165]

[162] « *By contexts, I mean structured social settings with characteristics that have evolved over time (sometimes long periods of time) and are subject to a host of causes and contingencies of purpose, place, culture, historical accident, and more*. » *Ibid.*, p. 130
[163] Ma traduction s'éloigne ici du mot-à-mot : Nissenbaum parle textuellement de *values* mais les définit comme la « téléologie » du contexte, « ses objectifs, ses fonctions et ses fins » (« *goals, purposes, and ends* »). Ce que le français entend par le terme « valeurs » relève plutôt de la catégorie des « normes » (« *norms* ») dans l'ouvrage.
[164] H. F. NISSENBAUM, *Privacy in context*, *op. cit.*, p. 133-134
[165] *Ibid.*, p. 172

L'approche contextuelle défendue par Nissenbaum est en somme assez souple pour tenir compte finement de variations dans les situations décrites, expliciter leur configuration ainsi que les réponses des acteurs engagés – particulièrement celles des individus – dans une situation de mise en jeu du privé. La comparaison avec le travail de Rey est ici intéressante. Cette dernière s'appuie sur un riche matériel d'enquête produit dans le cadre de sa thèse de doctorat. Les deux textes ont été rédigés sensiblement à la même époque, à la fin des années 2000. Rey ne cite donc pas Nissenbaum dans l'ouvrage tiré de son manuscrit de thèse[166]. Elle partage avec Nissenbaum le souci d'une approche par le bas, et notamment focalisée sur les utilisateurs et les consommateurs, mais en s'appuyant pour sa part sur son propre travail de terrain. Beaucoup plus empirique, l'ouvrage n'en dégage pas moins une « approche par les tensions » très proche du « *contextual integrity framework* ». Le chapitre 2 sur la « protection du privé à l'ère numérique » décrit plutôt les normes, tandis que les chapitres 3, 4 et 5 mêlent davantage rôles (consommateur, travailleur, membre d'un couple, citoyen, blogueur, membre d'un forum…), activités (déplacements en transport en commun, diffusion de contenu sur Internet, constitution d'une base de données utilisateurs pour une entreprise…) et finalités (avec pour principaux focus le travail et la consommation). Au bout du compte, le travail de Rey me semble mettre en œuvre dans sa propre enquête une méthode tout à fait comparable à celle que Nissenbaum défend dans un registre plus théorique.

La principale différence entre les ouvrages respectifs de Rey et Nissenbaum réside donc dans le caractère finement descriptif de l'un et théorisant de l'autre. Mais quelques points plus déterminants les rapprochent, et qui semblent devoir être retenus pour la suite du travail :

- La vie privée doit s'envisager en situation, dans un « contexte », et préférablement « en tension » ;
    - Ce, pas exclusivement dans des cas de conflit ouvert, et singulièrement de conflit judiciaire ;
- Les comparaisons internationales sont valides de part et d'autre de l'Atlantique.

Ces travaux partagent également un angle spatial que nous allons maintenant développer. Nissenbaum évoque notamment la question du « flux de données » (« *flow of data* ») et des « principes de transmission » (« *transmission principles* ») qu'elle élabore au sein de son cadre d'intégrité contextuelle[167]. Elle avance également l'idée que les contextes élaborés dans

[166] Pour note, elle ne le fera pas non plus dans ses textes ultérieurs sur la question.
[167] H. F. NISSENBAUM, *Privacy in context*, *op. cit.*, p. 145

l’espace matériel peuvent et doivent être transposés dans l’espace numérique. L’approche de Solove a également un caractère spatial patent dans beaucoup d’items de sa taxonomie des atteintes à la *privacy*, comme les brèches, la dissémination, etc. L’espace est moins directement présent chez Rey, si ce n’est dans la distinction des espaces (en fait, plutôt des sphères ou des domaines) public et privé ou dans la notion d’informatique ambiante. En tout état de cause, il manque à ces auteurs une appréhension plus spécifiquement spatiale de problèmes du privé qu’ils abordent plutôt sous l’angle des relations sociales. Comment donc lire spatialement les enjeux de vie privée numérique au prisme de ces théories du privé, et au-delà ? En termes spatiaux, nous allons voir que l’enjeu fondamental est devenu la circulation des données, de leur collecte à leur traitement puis leur exploitation. Si le privé s’étudie « en situation », c’est aussi, et de façon privilégiée, dans l’espace et dans les pratiques spatiales.

Chapitre 2 - ESPACES DE LA VIE PRIVEE ET CIRCULATION DES DONNEES PERSONNELLES

En cherchant à circonscrire le champ notionnel de la vie privée, nous avons pu constater que la question du privée avait une composante spatiale forte, particulièrement à travers la question de la circulation des données considérées comme privées. Plus classiquement, une des catégorisations spatiales les plus usitées en géographie consiste justement à distinguer l'espace privé et l'espace public. S'il faut se garder d'une approche essentialiste de la vie privée et aborder la notion dans sa complexité mouvante, en contexte, comment lire l'espace à travers ce prisme ? Puisqu'il renvoie souvent à une dimension intérieure, au mental, à l'identité, le privé peut-il même avoir lieu sans espace ? Est-ce le lieu qui fait le privé, ou le privé qui fait le lieu ?

I - L'ESPACE MATERIEL COMME INTERFACE DE CAPTATION

Internet et la « fin de l'espace »

Dans les premières pages de *City of bits*, William Mitchell rend compte d'un lieu commun des années 1990 selon lequel le numérique, et en l'occurrence « le Net » serait fondamentalement « antispatial », « une négation de la géométrie » au caractère immanent, « ambient »[168]. De fait, en raison de la complète accessibilité (au moins théorique) à tous les points du réseau depuis n'importe quel point d'accès dans le monde physique, Internet comme technologie de l'espace a puissamment nourri l'imaginaire d'un espace sans distance et sans friction. Cette thématique a notamment été développée à la même époque en France par le philosophe et urbaniste Paul Virilio, d'abord dans *L'espace critique*[169] puis dans *La bombe informatique*[170] et dans un article du *Monde diplomatique* dans lequel il affirme la fin de la pertinence des distances et des territoires physiques au profit d'interactions immatérielles à l'échelle globale : dans ce dernier stade de la mondialisation dissolvant les « limites » et la

[168] « *The Net negates geometry. While it does have a definite topology of computational nodes and radiating boulevards for bits, and while the locations of the nodes and links can be plotted on plans to produce surprisingly Haussman-like diagrams, it is fundamentally and profoundly antispatial. It is nothing like the Piazza Navone or Copley Square. But you can find things in it without knowing where they are. The Net is ambient – nowhere in particular but everywhere at once. You do not go to it; you log in from wherever you physically happen to be. I doing this you are bot making a visit in the usual sense, you are executing and electronically mediated speech act that provides access – an « open sesame* ». » W. J. MITCHELL, *City of bits: space, place, and the infobahn*, 6e éd., Cambridge (États-Unis), MIT Press, 1999 [1996], p. 8-9

[169] P. VIRILIO, *L'espace critique*, Paris (France), C. Bourgois, 1984

[170] P. VIRILIO, *La bombe informatique*, Paris (France), Galilée, 1998

différenciation locales des « cultures » dans un creuset « cybernétique »[171]. Dans la foulée de la « fin de l'histoire » de Francis Fukuyama après l'effondrement de l'URSS, Virilio annonce une « fin de la géographie » du fait de l'avènement d'Internet. Quelques années plus tard, en 2005, le journaliste et essayiste Thomas Friedman reprendra les mêmes idées, associant cinq « aplatisseurs » (« *flatteners* ») numériques à cinq aplatisseurs territoriaux pour affirmer dans une formule percutante et efficace que le « Monde est plat » (« *The World is flat* ») dans un ouvrage éponyme à grand succès[172]. En rendant prétendument caduque la notion de « distance », la numérisation du Monde était présentée comme une « bombe épistémologique » à retardement censée précipiter la fin de la science de l'espace qu'est la géographie[173]. Dans le même temps, les géographes ont longtemps été eux-mêmes réticents à intégrer la montée en puissance des télécommunications à travers les technologies de l'information et de la communication, pris qu'ils étaient dans une « attitude défensive et critique » fondée sur une tradition et un outillage disciplinaire très axés sur l'étude de la matérialité des échanges et des espaces[174], qualifié par la suite de « paradigme territorial » par Eveno[175].

L'explosion de cette « bombe épistémologique » n'a cependant pas eu lieu, et la thématique de la fin de l'espace et des distances a cependant été très vite remise en cause, notamment dans un numéro de la revue *Netcom* en 2000 dont l'introduction Par Henry Bakis et Emmanuel Eveno affirmait avec force l'inanité d'une conception de « la société de l'information » comme « a-géographique », malgré l'insuffisance du traitement de la question numérique par la géographie universitaire. Mieux : les auteurs y affirmaient plutôt que les

---

[171] « Après l'importance politique extrême de la géophysique du globe sur l'histoire de sociétés qui étaient moins séparées par leurs frontières nationales que par les délais et les distances de la communication d'un point à un autre, vient de se révéler, depuis peu, l'importance transpolitique de cette sorte de métagéophysique que représente pour nous l'interactivité quasi cybernétique du monde contemporain.
Puisque toute présence n'est présente qu'à distance, la téléprésence de l'ère de la mondialisation des échanges ne saurait s'installer que dans l'écartement le plus vaste qui soit. Ecartement qui s'étend désormais aux antipodes du globe, d'une rive à l'autre de la réalité présente, mais d'une réalité métagéophysique qui ajuste étroitement les télécontinents d'une réalité virtuelle qui accapare l'essentiel de l'activité économique des nations, et, a contrario, désintègre des cultures précisément situées dans l'espace physique du globe. » P. VIRILIO, « Un monde surexposé - Fin de l'histoire, ou fin de la géographie ? », *Le Monde diplomatique*, 1er août 1997 (en ligne : https://www.monde-diplomatique.fr/1997/08/VIRILIO/4878 ; consulté le 23 mai 2019)

[172] T. L. FRIEDMAN, *The world is flat: a brief history of the twenty-first century*, New York (États-Unis), Farrar, Straus and Giroux, 2005

[173] H. BAKIS et E. EVENO, « Les géographes et la société de l'information. Des effets pervers d'un champ réputé a-géographique », *Géocarrefour*, vol. 75, no 1, 2000, p. 7 (en ligne : http://www.persee.fr/doc/geoca_1627-4873_2000_num_75_1_2448)

[174] E. EVENO, « Pour une géographie de la Société de l'Information », *NETCOM : Réseaux, communication et territoires / Networks and communication studies*, vol. 11, no 2, Persée - Portail des revues scientifiques en SHS, 1997, p. 435 (en ligne : https://www.persee.fr/doc/netco_0987-6014_1997_num_11_2_1369)

[175] E. EVENO, « Le paradigme territorial de la Société de l'Information », *NETCOM : Réseaux, communication et territoires / Networks and communication studies*, vol. 18, no 1, Persée - Portail des revues scientifiques en SHS, 2004, p. 89-132 (en ligne : https://www.persee.fr/doc/netco_0987-6014_2004_num_18_1_1601 ; consulté le 16 février 2023)

quelques premiers travaux de géographie du numérique « contredis[ai]ent dans leur grande majorité les thèses catastrophistes de l'effondrement des distances »[176]. Les aménageurs ont ainsi pointé qu'Internet n'était pas un « éther »[177], mais qu'il se fondait au contraire sur une infrastructure technique complexe dont les composantes étaient et continuent d'être inégalement distribuées dans le monde. Gabriel Dupuy a notamment développé la notion de « fracture numérique »[178] pour montrer combien la montée en puissance d'Internet profitait essentiellement aux territoires urbains, et que la logique réticulaire d'Internet valait également hors-ligne en laissant de larges parts de l'espace géographique dans des mailles éloignées des points d'accès au réseau, les zones blanches où l'accès à Internet est soit impossible, soit difficile du fait de la lenteur ou de l'intermittence des connexions. À titre d'exemple, la question de la résorption des zones blanches est encore à l'ordre du jour d'un rapport de l'Arcep[179] sur le déploiement de l'Internet mobile en France en avril 2021[180]. Cette « fracture numérique » vaut également pour les individus eux-mêmes : il ne suffit pas qu'un territoire soit connecté à Internet pour que cela se traduise par un usage généralisé d'Internet. On parle d'illectronisme pour décrire l'absence de compétence à l'utilisation d'Internet. En France en 2019, « une personne sur six n'utilise pas Internet, plus d'un usager sur trois manque de compétences numériques de base »[181] d'après les résultats de l'enquête TIC Ménages rapportés dans une publication de l'INSEE. C'est entre autres choses pourquoi Gabriel Dupuy dit bien lui-même que « la fracture numérique dénonce une dislocation **[sociale]** liée aux Nouvelles Technologies d'Information et de Communication (NTIC) »[182].

Dans le domaine de la mobilité également, les premières attentes quant au numérique étaient plutôt à la substitution des déplacements physiques par la télécommunication. Si ce processus de substitution est avéré et a fait l'objet d'une littérature scientifique importante, la

[176] H. BAKIS et E. EVENO, « Les géographes et la société de l'information. Des effets pervers d'un champ réputé a-géographique », *op. cit.*, p. 7
[177] P. VIRILIO, « Un monde surexposé », *op. cit.*
[178] G. DUPUY, *La fracture numérique*, *op. cit.*
[179] Autorité de régulation des communications électroniques des postes et de la distribution de la presse. L'Arcep est l'une des agences de l'Etat français qui contribue, entre autres missions, au design de l'aménagement du territoire en matière numérique.
[180] *La régulation de l'Arcep au service des territoires connectés - Tome 2*, Paris (France), Arcep, 2021, p. 10
[181] S. LEGLEYE et A. ROLLAND, *Une personne sur six n'utilise pas Internet, plus d'un usager sur trois manque de compétences numériques de base*, Montrouge (France), INSEE, 2019
[182] G. DUPUY, « Fracture et dépendance : l'enfer des réseaux? », *Flux*, vol. 83, n° 1, 1er mars 2011, § 4 (en ligne : https://www.cairn.info/revue-flux1-2011-1-page-6.htm)

tendance actuelle est plutôt de se demander comment le numérique accompagne (ou augmente) les déplacements physiques[183].

Ainsi, malgré le caractère frappant de la thématique de la fin de l'espace ou de la géographie à l'ère numérique, la réponse apportée par Frédéric Lasserre dès 1996 dans un article consacré à la question semble toujours pertinente : « (…) nulle disparition de la dynamique géopolitique, ni de la spatialité des phénomènes sociaux, politiques et économiques : le système-monde se transforme, voilà tout, même si cette transformation est d'importance »[184]. L'année suivante, c'est Emmanuel Eveno qui invitait la géographie à investiguer cette transformation et à dépasser le faux débat de l'aspatialité du numérique pour « s'attribue[r] plutôt la mission de voir en quoi cet espace « cybernétisé » se confronte aux autres catégories d'espaces (vécus, perçus ou représentés) » et de bien comprendre que les médiations numériques « s'inscrivent dans des temps et des distances sociales » autant qu'elles « s'intègrent dans les rapports socio-territoriaux, dans les formes de territorialité des organisations politiques ou économiques »[185]. Pour Boris Beaude une dizaine d'années plus tard, c'est même plutôt l'isotropie d'Internet qui, après s'être longtemps assez bien vérifiée en matière de circulation de l'information dans les espaces réticulaires en ligne, a été largement remise en cause dans les années 2000 et 2010 par des acteurs territoriaux puissants, au premier rang desquels les États. Dans *Les fins d'Internet* (2014), l'auteur met plutôt en garde contre l'anisotropie grandissante de l'espace réticulaire. Il prend notamment pour exemple la montée en puissance de véritables intranets nationaux, notamment en Chine[186] ou en Iran, et dans une moindre mesure en Russie[187], résultant de la volonté de régimes autoritaires de maîtriser l'information circulant dans leur pays[188].

Il ne faut donc pas exagérer ou généraliser outre-mesure les effets spatiaux *aplatissants* ou réticulants du numérique : s'il est un des facteurs les plus puissants de la mondialisation et participe à un accroissement sans précédent de l'interconnexion des êtres et des choses, l'espace

[183] T. SCHWANEN, « Information Technology and Mobility », dans *International Encyclopedia of Geography*, s. l., John Wiley & Sons, Ltd, 2022, p. 1-4
[184] F. LASSERRE, « Internet », *op. cit.*, p. 2
[185] E. EVENO, « Pour une géographie de la Société de l'Information », *op. cit.*, p. 437
[186] Plus de 311 000 domaines, notamment étrangers, seraient bloqués par le « Grand Pare-feu Chinois » au moyen d'un filtrage de la résolution de nom de domaine (DNS) en juin 2021. Voir N. P. HOANG *et al.*, « How Great is the Great Firewall? Measuring China's DNS Censorship », *arXiv*, 3 juin 2021 (en ligne : http://arxiv.org/abs/2106.02167 ; consulté le 13 juillet 2021)
[187] K. LIMONIER, « Vers un « Runet souverain » ? Perspectives et limites de la stratégie russe de contrôle de l'Internet », *EchoGéo*, nº 56, Pôle de recherche pour l'organisation et la diffusion de l'information géographique (CNRS UMR 8586), 25 mai 2021, § 4-5 (DOI : 10.4000/echogeo.21804 consulté le 17 juillet 2021)
[188] B. BEAUDE, *Les fins d'Internet*, *op. cit.*

territorial et son inertie matérielle en restent à la fois une condition d'existence et une limite fortes. Pour autant, il ne s'agit pas de nier l'enchâssement croissant du numérique dans l'espace et dans les pratiques spatiales, l'interspatialité de ce qu'Henry Bakis décrivait comme le géoespace et le cyberespace. Cet enchâssement s'observe d'autant mieux à une échelle plus fine, en s'intéressant à la manière dont les réalités matérielles s'hybrident d'une réalité réticulaire.

L'espace augmenté : la logique de l'*opt-in*

Si l'espace géographique est diversement mobilisé dans les médiations numériques, les lieux et les réalités matérielles à l'interspatialité la plus marquée avec Internet et les médiations numériques sont subsumés dans l'appellation (ou l'épithète) d'espace *augmenté*. Cette distinction est floue et toujours à questionner, à la manière de la distinction ancienne de l'érème et de l'écoumène dans l'étendue spatiale. En première hypothèse, l'espace n'est jamais tout à fait augmenté pour tous et pour toutes les pratiques. Il n'y a d'ailleurs pas de terme général décrivant l'espace non-augmenté, et bien souvent pas de terme du tout. Les zones blanches de la téléphonie mobile en sont probablement le cas le plus étudié. Si l'on prend le cas-limite d'un espace naturel très peu ou pas anthropisé, et malgré tout couvert par une antenne téléphonique, un même lieu pourra être considéré comme quelque peu augmenté par le possesseur d'un téléphone mobile et plus encore d'un *smartphone*, et pas du tout par un individu ne disposant pas d'un tel terminal. À l'opposé, même le possesseur d'un *smartphone* rudimentaire ne profitera pas à fond de l'augmentation maximale d'un espace urbain central doté de tous les dispositifs numériques possibles : peut-être n'aura-t-il accès qu'à un réseau mobile 3G ; ou qu'il ne disposera pas des moyens de paiement ou d'identification RFID dits « sans-contact » qui lui permettraient de régler ses achats ou d'accéder au réseau de transports en commun au moyen de son appareil ; peut-être aussi tel lieu dans un quartier par ailleurs très connecté sera-t-il une micro zone blanche (le sous-sol inaccessible aux ondes de tel restaurant, la salle de cinéma équipée d'un brouilleur pour prévenir les sonneries intempestives…). L'augmentation de l'espace est donc toujours fragmentaire et partielle, et implique nécessairement de demander pour qui, en quoi et par quoi elle est effective ou non.

Le philosophe Pierre Musso, dans un article consacré aux « territoires numériques » en 2008, propose ainsi que « La notion de territoire augmenté, ou hyperterritoire, doit être comprise de manière à la fois extensive (territoire étendu) et intensive (intensification des capacités du territoire et de ses résidents). Le territoire est « augmenté » quand les capacités des personnes, des entreprises et autres institutions se trouvent amplifiées par des ressources

auxquelles on accède via le réseau : informations, outils, applications, services.[189] » On le comprend, Musso propose ici une lecture de l'espace numérique comme mis au service des acteurs qui le pratiquent, « résidents » et « entreprises » notamment. Sa réflexion est celle d'un penseur de l'aménagement cherchant à rendre possible l'interspatialité d'Internet, vu comme un espace réticulaire autonome, et l'espace matériel des pratiques habituelles : « Ils se nouent en quelque sorte avec le territoire pour *l'augmenter* – au sens où l'on parle de « réalité augmentée » –, pour l'enrichir et enrichir les actions et les rencontres entre acteurs[190]. »

La formulation même de l'expression « espace augmenté » signale cette volonté d'enrichir une réalité préexistante, l'espace, à comprendre comme l'espace territorial classique, d'une augmentation qui lui est extérieure et seconde, l'espace numérique et singulièrement Internet. La résultante en est bien un espace augmenté, c'est-à-dire complété, enrichi de nouvelles possibilités d'interconnexion. Cette conception de l'interspatialité des espaces territoriaux et réticulaires a deux corollaires, qui sont aussi des formes de présupposés. D'une part, l'espace territorial prime toujours. C'est lui qu'il importe d'augmenter, et qui constitue l'espace primordial, quoique Musso ne conteste par leur caractère spatial aux « réseaux exclusivement topologiques ». Ainsi, ces derniers sont « Superposés aux territoires, ils ne coïncident pas avec eux »[191]. D'autre part, le numérique est pour Musso une possibilité offerte aux acteurs du territoire qui l'embrasse, une aménité qui permet d'abord et avant tout l'augmentation de leur pouvoir d'agir et d'interagir. Le régime de la participation des acteurs au numérique selon Musso relève, pour ainsi dire, de l'*opt-in*, du choix, de la démarche délibérée et donc consentie. L'augmentation est une proposition ; elle est par définition superfétatoire, puisque seconde. Elle a certes un véritable effet spatial et « [soulève] des questionnements nouveaux »[192], mais ne transforme pas fondamentalement le territoire dans lequel elle se déploie.

Cette conception des choses n'est pas sans réalité, ni sans intérêt. Un autre corollaire possible, plus critique, en est ainsi que le numérique territorial vertueux devrait toujours augmenter et jamais retrancher des facultés – par exemple, la possibilité d'accéder à un guichet matériel de service public, et pas dématérialiser toutes les démarches, ne serait-ce que pour les usagers n'ayant pas choisi d'*opt-in* au numérique par choix ou par contrainte. En se focalisant

[189] P. MUSSO, « Territoires numériques », *op. cit.*, p. 33
[190] *Ibid.*, p. 32
[191] *Id.*
[192] « Ils [les réseaux numériques topologiques] soulèvent donc des questionnements nouveaux, car ce ne sont pas seulement des réseaux techniques qui font circuler de l'information à grande distance et à grande vitesse. » *Id.*

sur la proposition et sur l'*opt-in*, elle n'envisage cependant pas sérieusement la possibilité que l'*opt-out*[193] devienne très rapidement la norme, voire qu'il ne soit plus possible de refuser, de faire sans le numérique. Ce faisait, elle sous-estime la profondeur de la transformation de territoires non seulement augmentés, mais (re)codés.

L'espace sous surveillance: plus de refus possible ?

Si la notion d'espace augmenté décrit la diffusion des points d'accès et dispositifs numériques et informatiques à une échelle large, d'une manière plutôt positive et sur le mode de l'*opt-in*, d'autres conceptions du phénomène ont une posture plus critique, et à une échelle plus fine.

Dans un chapitre de l'ouvrage *Data Politics - Worlds, Subjects, Rights*, David Lyon revient sur les trente dernières années du champ des *surveillance studies*[194] dont il est un des auteurs de référence jusqu'à son départ à la retraite en juin 2021[195]. Ce champ s'est particulièrement structuré et a fait école autour du Surveillance Studies Centre de l'université de Queens (Canada) et de sa revue *Surveillance & Society*, créée en 2002[196]. Selon Lyon, la conversation scientifique autour d'une « société de la surveillance » (« *surveillance society* ») aurait débuté un peu plus tôt, au milieu des années 1980, autour de thématiques comme le traçage des achats *via* les cartes bancaires ou de fidélité, mais aussi et surtout de la vidéosurveillance et de « l'emblématique caméra », qui a « souvent [cristallisé] » la question.[197] Sur les 854 articles publiés dans la revue entre 2002 et l'été 2021, 304 incluent le terme « CCTV » pour *closed-circuit television*, à savoir la vidéosurveillance par opposition à la télévision diffusée. La vidéosurveillance est emblématique de ce champ de recherche en cela qu'elle est à la fois massivement présente dans les espaces publics ou partagés (lieux de travail et de consommation inclus), concrètement visible voire signalée par des panonceaux, entièrement dédiée à la surveillance du public, et qu'elle est imposée aux personnes dans le

[193] Dans le vocabulaire de la publicité en ligne, l'*opt-out* est le consentement par défaut de l'utilisateur qui recevra donc de la publicité ou des *cookies* de traçage (on peut encore refuser, mais par une démarche active), et l'*opt-in* est le consentement acquis dès le départ, après demande explicite à l'utilisateur.
[194] D. LYON, « Surveillance capitalism, surveillance culture and data politics », dans D. Bigo, E. Isin et E. Ruppert, *Data Politics - Worlds, Subjects, Rights*, Londres (Royaume-Uni), Routledge, 2019, p. 69
[195] « David Lyon retires from Queen's; remains P.I. of Big Data Surveillance », sur *The Surveillance Studies Centre*, 6 juillet 2021 (en ligne : https://www.sscqueens.org/news/david-lyon-retires-from-queens-remains-pi-of-big-data-surveillance ; consulté le 23 juillet 2021)
[196] O. AÏM, *Les théories de la surveillance - Du panoptique aux Surveillance Studies*, Paris (France), Armand Colin, 2020
[197] « *policing and workplace surveillance, often crystallized in the iconic video camera* ». D. LYON, « Surveillance capitalism, surveillance culture and data politics », *op. cit.*, p. 69

champ de captation de la caméra, sans *opt-out* possible[198]. Elle a longtemps constitué la matrice de la réflexion sur la surveillance dans les espaces partagés. D'autres technologies sont perçues comme potentiellement surveillantes, et sont presque autant traitées par les chercheurs du domaine, en particulier les cartes à puce permettant d'identifier quelle carte (et quel nom associé) transite par telle station de transports en commun ou effectue tel paiement dans tel magasin. Mais la caméra, par son caractère fixe et matériel, active puissamment le sentiment d'être presque constamment sous l'œil d'un agent ou, aujourd'hui, d'un logiciel de surveillance. Ce sentiment est parfois nettement vérifié. Dans certaines villes, la concentration de caméras les rend presque omniprésentes dans les espaces publics, l'exemple de Londres étant particulièrement mobilisé avec 439,6 caméras / km² en 2021, soit une caméra pour 23 m² au sol dans toute l'agglomération, à la première position parmi les métropoles européennes de plus de trois millions d'habitants (Paris arrive en septième place avec 14,9 caméras par km²)[199]. La surveillance y devient une dimension ancrée dans l'espace parcouru au quotidien, là où le fait de passer une carte dans un lecteur, par exemple, peut sembler plus anodin – outre qu'il est souvent possible de se prémunir de cette forme de traçage, en utilisant des tickets ou de l'argent liquide, et que ces dispositifs ne sont pas fondamentalement dédiés à la surveillance, mais aussi et surtout au simple paiement d'un service ou d'un bien qui relève d'un autre registre de justifiabilité. Cette volonté d'échapper à la saisie numérique de ses actions quotidiennes est nettement marquée chez E5. Étant arrivé avec un peu d'avance dans son quartier pour mener l'entretien chez lui, il m'invite à le rejoindre dans un magasin proche, où je constate sans surprise qu'il règle en liquide. Au cours de l'entretien, il m'indiquera aussi sortir parfois sans son *smartphone* ou l'éteindre aléatoirement dans le but de ne pas être tracé dans ses déplacements ou, plus exactement, de ne pas toujours vérifier l'hypothèse que son *smartphone* soit un traceur fiable du moindre de ses déplacements :

> « Pour moi, l'enjeu, c'est problématique de vivre avec ça (il soulève son Fairphone de la table) qui n'est jamais à plus de cinquante centimètres de mon cul. Vivre comme ça pour moi c'est problématique. Et du coup pour moi c'est important de laisser des espaces où cette condition n'est pas vraie. » (entretien 3, 1 h 32 min 45 s)

[198] Il est possible de déployer des tactiques pour échapper à la surveillance en évitant les espaces directement surveillés ou en dissimulant ses traits, mais ces options restent marginales.

[199] T. GAUDIAUT, « Les métropoles européennes avec le plus de caméras au km² », sur *Statista Infographies*, 23 juin 2021 (en ligne : https://fr.statista.com/infographie/25143/densite-de-cameras-de-videosurveillance-dans-les-grandes-villes-europeennes/ ; consulté le 25 juin 2021)

L'ensemble de ces dispositifs entrent dans le cadre de ce que David Lyon définit comme une « culture de la surveillance », par opposition au « capitalisme de surveillance »[200], sur lequel nous reviendrons plus tard (voir « Une approche peu explicitement spatiale de la circulation des données », p. 88). Cette prise de conscience académique s'est doublée d'un riche mouvement militant qui vise à lutter contre cette culture de la surveillance : d'une part, en la mettant en évidence, d'autre part, en fournissant les moyens de lutter contre elle. Un très bon indice du caractère éminemment spatial de la problématique de la captation de données dans l'espace public se révèle à travers l'utilisation remarquable et massive de l'outil cartographique par de nombreux groupes militants. L'une des initiatives les plus remarquables en ce qui concerne la vidéosurveillance est le projet *Surveillance under surveillance* qui s'appuie sur les données de la base de données cartographiques *OpenStreetMap* pour localiser les caméras dans les espaces publics ou accessibles au public (comme les magasins ou les banques). Outre la localisation de la caméra, des données peuvent être renseignées sur son type (dôme, fixe, pivotante, fixée sur un mur ou un mât et à quelle hauteur, avec ou sans enregistrement, passive ou opérée par un agent de sécurité…), sa date d'installation, son opérateur, et jusqu'à l'angle de prise de vue et la zone couverte, comme dans l'exemple ci-dessous d'une caméra publique fixée à un mur sur le campus de l'ENS de Lyon et couvrant le sud-ouest de sa position (voir Figure 4).

[200] D. LYON, « Surveillance capitalism, surveillance culture and data politics », *op. cit.*, p. 71

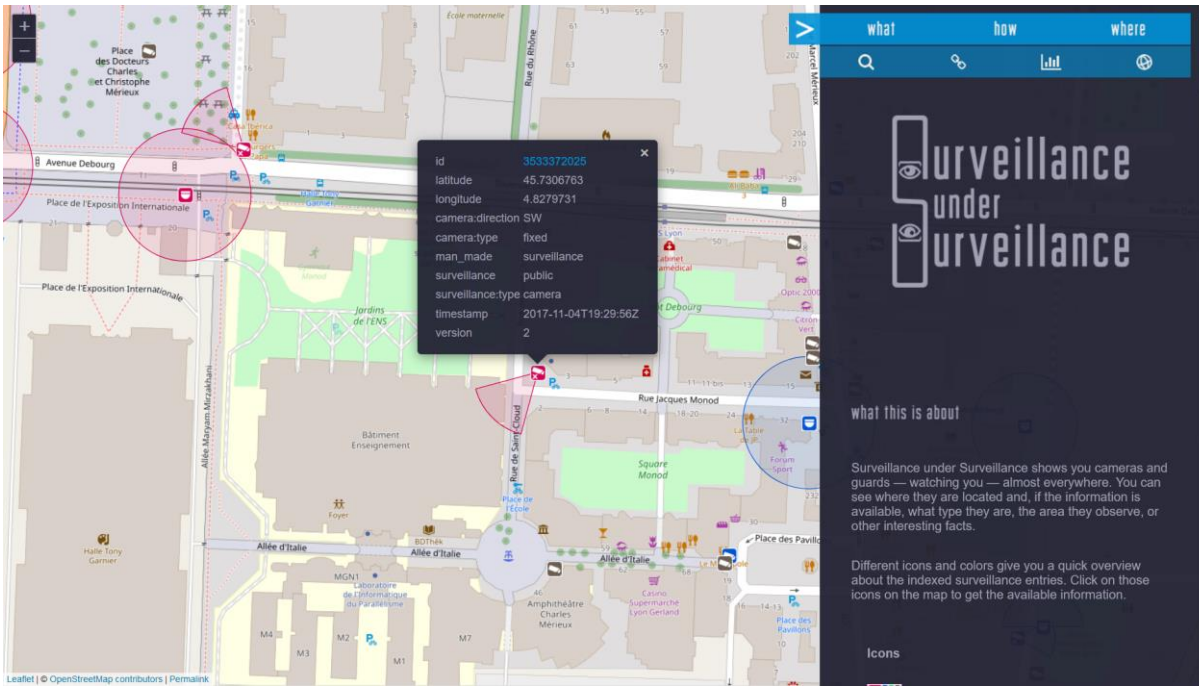


Figure 4 - Capture d'écran de la carte Surveillance under surveillance [en ligne: https://sunders.uber.space/?lat=45.7578137&lon=4.8320114&zoom=14#what, consultée le 23/07/2021)

Ces initiatives cartographiques ne se limitent pas à la vidéosurveillance. L'Electronic Frontier Foundation propose ainsi un *Atlas of surveillance* [201] qui répertorie les programmes et infrastructures de surveillance les plus divers aux États-Unis, comme le fait qu'un département de police soit équipé de drones aériens, ou la localisation d'un centre de traitement de données de surveillance. En France, le groupe Technopolice [202] de la Quadrature du Net propose également un tel outil, à la granularité et à l'élaboration sémiologique moins fines, mais qui renvoie à des articles détaillés sur chacune des opérations recensées. Dans tous les cas, l'outil cartographique est exploité dans ce double mouvement de monstration et de lutte, et vise *in fine* à ce que la surveillance ne soit pas normalisée, à lutter contre l'intériorisation de cette culture de la surveillance par l'information du public. Et ce parfois jusqu'à un niveau tactique, c'est-à-dire qui permette de mettre en œuvre des mesures de contournement concrètes de la surveillance, par exemple en choisissant un itinéraire évitant les zones vidéosurveillées. Autrement dit, de permettre, à la marge, un refus à la surveillance de l'espace public.

[201] Voir https://atlasofsurveillance.org/about
[202] Voir https://technopolice.fr/villes/

Il faut cependant signaler une évolution récente et singulière de la surveillance vidéo et audio de l'espace public aux États-Unis, et qui ne s'appuie plus sur une infrastructure déployée par des institutions publiques ou privés, mais y compris par les particuliers eux-mêmes. Le décennie 2010 a vu l'émergence d'un nouveau segment du marché domotique à travers les sonnettes connectées, particulièrement porté par la sonnette vidéo Doorbell de l'entreprise Ring. Sans surprise, ce nouvel objet a fait l'objet de débats attendus en matière de vie privée ou de sécurité. L'une des principales critiques a longtemps concerné l'absence de chiffrement des communications entre les serveurs de Ring et la Doorbell. Cette fonctionnalité est finalement en cours d'intégration en juillet 2021[203], le chiffrement de bout-en-bout devant protéger à la fois la transmission des données de l'appareil vers les serveurs[204], et assurer que les données une fois téléversées ne soient consultables que par les utilisateurs – après qu'Amazon a dû reconnaître début 2020 que plusieurs employés avaient tenté indûment d'accéder à des enregistrements vidéo[205]. Mais la principale critique contemporaine de ce système concerne les partenariats que Ring avait déjà passé en mai 2021 avec plus de 1 800 départements de police aux États-Unis, soit 10 % des départements de police du pays, afin de créer un réseau de surveillance vidéo s'appuyant sur les caméras individuelles des propriétaires de Doorbell[206]. L'intérêt pour la police est bien sûr d'obtenir en temps réel une visibilité sur l'espace public adjacent aux domiciles équipés, sans avoir à installer de caméras

L'entreprise Ring

Ring est une entreprise de sonnettes connectées fondée en 2013 sous le nom de Doorbot par Jamie Siminoff. Elle a été rachetée par Amazon en février 2018 pour une valeur estimée entre 1,2 et 1,8 milliard de dollars étatsuniens.

Son produit-phare est la Video Doorbell, une sonnette connectée équipée d'une vidéo, d'un micro et de haut-parleurs permettant de surveiller à distance son pas de porte.

[203] J. LAUSSON, « Les caméras de Ring passent enfin au chiffrement de bout en bout (si on active l'option) », *Numerama - Cyberguerre*, 14 juillet 2021 (en ligne : https://cyberguerre.numerama.com/12711-les-cameras-de-ring-passent-enfin-au-chiffrement-de-bout-en-bout-si-on-active-loption.html ; consulté le 27 juillet 2021)

[204] Des données sensibles circulaient jusqu'ici en clair vers les serveurs de Ring, comme le mot de passe du réseau Wi-Fi des utilisateurs.

[205] Anon., « Des employés Ring ont tenté d'accéder aux vidéos des caméras », *Next INpact*, 9 janvier 2020 (en ligne : https://www.nextinpact.com/lebrief/41088/10844-des-employes-ring-ont-tente-d-acceder-aux-videos-des-cameras ; consulté le 27 juillet 2021)

[206] L. BRIDGES, « Amazon's Ring is the largest civilian surveillance network the US has ever seen », *The Guardian*, 18 mai 2021 (en ligne : https://amp.theguardian.com/commentisfree/2021/may/18/amazon-ring-largest-civilian-surveillance-network-us ; consulté le 23 mai 2021)

publiques, et sans mandat[207]. En outre, le système étant lié à des sonnettes connectées, l'impact visuel de la présence de caméras est nettement amoindri. Il y a donc aussi un enjeu de discrétion qui s'ajoute à l'intérêt d'une diffusion fine et massive dans des quartiers par ailleurs moins densément peuplés où l'installation d'autant de caméras de surveillance publiques serait exagérément coûteux, du moins en ce qui concerne les *suburbs*. Amazon a même proposé aux unités de police et au législateur étatsunien d'ajouter une fonction de reconnaissance faciale à son réseau de Doorbells pour en augmenter l'efficacité[208]. L' EFF a fait de ces partenariats entre Ring et les divers services de police concernés l'un de ses chevaux de bataille médiatiques. C'est moins la vie privée des utilisateurs eux-mêmes que celle des passants qui fait ici l'objet de la vigilance de l'EFF, présentant ce dispositif d'association avec des polices locales comme une « déferlante parfaite de menaces contre la vie privée ».[209] En outre, l'organisation craint des effets de bord considérable de cette logique de surveillance publique-privée généralisée, en particulier à l'encontre des minorités ethniques aux États-Unis, notamment des Noirs, plus susceptibles d'être suspectés d'intentions malveillantes et de subir des violences illégitimes de la part de particuliers ou des forces de police.[210] Par ailleurs, il semble que la société civile soit réticente encore à cette logique. En témoigne par exemple l'émoi qui a suivi la diffusion par Ring à des fins promotionnelles des images et vidéos de *trick-or-treaters* sur le perron des maisons des utilisateurs qui se voyaient réclamer des bonbons à l'occasion d'Halloween. Ces réticences tenaient essentiellement au questionnement autour du consentement des personnes à voir ces vidéos diffusées, qu'il s'agisse des propriétaires des sonnettes ou de leurs visiteurs. Ce, malgré le caractère humoristique et décalé de la vidéo. Il semblerait que ces images aient été diffusées via l'application *Neighbors* de Ring, dont les conditions générales d'utilisation lui permettent la réutilisation des images diffusées par les utilisateurs[211].

---

[207] *Id.*

[208] M. O'BRIEN, « Amazon says it's considered face scanning in Ring doorbells - Canadian Business », *Canadian Business*, 20 novembre 2019 (en ligne : https://archive.canadianbusiness.com/business-news/amazon-says-its-considered-face-scanning-in-ring-doorbells/ ; consulté le 18 mars 2022)

[209] M. GUARIGLIA, « Amazon's Ring Is a Perfect Storm of Privacy Threats », sur *Electronic Frontier Foundation*, 8 août 2019 (en ligne : https://www.eff.org/deeplinks/2019/08/amazons-ring-perfect-storm-privacy-threats ; consulté le 12 septembre 2019)

[210] J. KELLEY et M. GUARIGLIA, « Amazon Ring Must End Its Dangerous Partnerships With Police », sur *Electronic Frontier Foundation*, 10 juin 2020 (en ligne : https://www.eff.org/fr/deeplinks/2020/06/amazon-ring-must-end-its-dangerous-partnerships-police ; consulté le 13 septembre 2021)

[211] R. KRAUS, « Ring watched your kids trick or treat and then bragged about it », sur *Mashable*, 1er novembre 2019 (en ligne : https://mashable.com/article/ring-halloween-surveillance/ ; consulté le 24 mai 2021)

Cette nouvelle pratique d'Amazon s'inscrit plus généralement dans la thématique de « *surveillance as a service* » décrite par Emily West[212], particulièrement à propos d'Amazon et des enceintes connectées Alexa. La nouveauté est ici que, là où la surveillance était auparavant plutôt descendante, des pouvoirs publics vers les particuliers ou des entreprises vers leurs travailleurs, il y a désormais une diffusion auprès des particuliers eux-mêmes d'outils de surveillance pour leur compte qui, à travers leur agrégation et leur centralisation, sont mis au service d'une surveillance globale de l'espace public. Pour reprendre les termes de David Lyon, la question des partenariats entre Ring et les services de police pour la surveillance de l'espace public semble être une nouvelle étape et un paroxysme dans la diffusion de la « culture de la surveillance »[213]. Le sujet reste sensible pour les entreprises elles-mêmes : le service de relations publiques d'Amazon a par exemple fait pression sur des journalistes de *ABC Action News* en octobre 2019, à la suite d'un article rapportant les liens entre le réseau de vidéosurveillance de Ring et les polices locales de plusieurs dizaines de municipalités de Floride.[214]

Plus largement, on peut aussi y voir l'une des plus récentes manifestations de la thématique de la *smart city* qui vise à augmenter de capteurs les espaces du quotidien afin d'optimiser et de réguler les flux et les pratiques dans les villes contemporaines. L'engagement des habitants dans les processus de la *smart city* est d'habitude une difficulté essentielle pour les opérateurs.[215] Les géographes Paolo Cardullo et Rob Kitchin, en prenant appui sur les travaux de Sherry Arnstein, proposent même un « échafaudage »[216] (ou une échelle) permettant de mesurer le degré de « citadino-centrisme » (trad. pers.) des projets de *smart city*, qui ont essuyé par le monde de nombreuses critiques en technocratie et en approche descendante des questions urbaines (voir Tableau 3)[217].

---

[212] E. WEST, « Amazon: Surveillance as a Service », *Surveillance & Society*, vol. 17, nº 1/2, 31 mars 2019, p. 27-33 (en ligne : https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/13008 ; consulté le 26 juillet 2021)

[213] D. LYON, « Surveillance capitalism, surveillance culture and data politics », *op. cit.*

[214] A. BRELAND, « How Amazon bullies, manipulates, and lies to reporters », sur *Mother Jones*, 25 juin 2021 (en ligne : https://www.motherjones.com/politics/2021/06/amazon-journalists-pr-tactics/ ; consulté le 26 juin 2021)

[215] D. BOUNAZEF et N. CRUTZEN, « Les citoyens et stratégies communales à l'ère de la smart city : Echanges et interactions entre sourds ? », Bruxelles (Belgique), 2019 (en ligne : https://orbi.uliege.be/handle/2268/237154)

[216] Traduit à partir du terme *scaffold* qu'ils utilisent eux-mêmes pour se démarquer de la *ladder* d'Arnstein dans leur expression « the scaffold of smart citizen participation » P. CARDULLO et R. KITCHIN, « Being a 'citizen' in the smart city: up and down the scaffold of smart citizen participation in Dublin, Ireland », *GeoJournal*, vol. 84, nº 1, 1er février 2019, p. 2 (en ligne : https://doi.org/10.1007/s10708-018-9845-8)

[217] P. CARDULLO et R. KITCHIN, « Being a 'citizen' in the smart city », *op. cit.*

Tableau 3 - "Scaffold of smart citizen participation" (Carullo, Kitchin, 2019)

<table>
<tr><th colspan="2">Form and Level of Participation</th><th>Role</th><th>Citizen Involvement</th><th>Political discourse/ framing</th><th>Modality</th><th>Dublin Examples</th></tr>
<tr><td rowspan="3">Citizen Power</td><td>Citizen Control</td><td>Leader, Member</td><td rowspan="2">Ideas, Vision, Leadership, Ownership, Create</td><td rowspan="2">Rights, Social/Political Citizenship, Commons</td><td rowspan="2">Inclusive, Bottom-up, Collective, Autonomy, Experimental</td><td>Code for Ireland, Tog</td></tr>
<tr><td>Delegated Power</td><td>Decision-maker, Maker</td><td>Civic Hacking, Hackathons, Living Labs, Dublin Beta</td></tr>
<tr><td>Partnership</td><td>Co-creator</td><td>Negotiate, Produce</td><td rowspan="2">Participation, Co-creation</td></tr>
<tr><td rowspan="3">Tokenism</td><td>Placation</td><td>Proposer</td><td>Suggest</td><td rowspan="4">Top-down, Civic Paternalism, Stewardship, Bound-to-succeed</td><td>Fix-Your-Street, Smart Dublin Advisory Network</td></tr>
<tr><td>Consultation</td><td>Participant, Tester, Player</td><td>Feedback</td><td rowspan="2">Civic Engagement</td><td>CIVIQ, Smart Stadium</td></tr>
<tr><td>Information</td><td>Recipient</td><td rowspan="2">Browse, Consume, Act</td><td>Dublinked, Dublin Dashboard, RTPI</td></tr>
<tr><td>Consumerism</td><td>Choice</td><td>Resident, Consumer</td><td>Capitalism, Market</td><td>Smart building/ Smart district</td></tr>
<tr><td rowspan="2">Non-Participation</td><td>Therapy</td><td rowspan="2">Patient, Learner, User, Product, Data-point</td><td rowspan="2">Steered, Nudged, Controlled</td><td rowspan="2">Stewardship, Technocracy, Paternalism</td><td>Smart meters, Mobile/locative media</td></tr>
<tr><td>Manipulation</td><td>Dublin Bikes, Smart Dublin</td><td>Traffic control</td></tr>
</table>

Le cas du projet avorté de réaménagement du quartier entier de Quayside (Toronto) sur le mode de la *smart city* par la filiale Sidewalk Labs de Google en est l'exemple emblématique le plus récent. Sur le plan de son augmentation numérique, le projet prévoyait quatre axes : « capter, modéliser, cartographier, représenter » (trad. pers.).[218] La majorité des pratiques et des aspects de la vie quotidienne devaient être captés, qu'il s'agisse des mobilités ou de la consommation en fluide des logements, pour permettre une hypervision et l'établissement de *patterns* par l'autorité régulatrice, tout en permettant aux habitants d'être représentés à distance – par exemple, en donnant accès à leur logement à des employés d'entretien, ou en ayant accès à une partie des données produites par le système[219]. Quoique le projet de Google se soit voulu à la pointe de l'innovation urbaine en dépassant les critiques habituelles sur le désinvestissement des résidents, c'est l'irrésolution de la négociation sur le mode de gouvernance du quartier par rapport à la gestion des données à caractère personnel des potentiels habitants qui a fini par entraîner l'arrêt du projet dans la forme la plus ambitieuse d'abord envisagée. L'instance centrale censée assurer la gestion des données produites et de la plupart des infrastructures et services collectifs, le « *Urban Data Trust* » était, selon Lisa Austin

[218] « *sense, model, map, and account* » K. PEEL et E. TRETTER, « Waterfront Toronto: Privacy or Piracy? », *Global Urban Research at the University of Calgary Working Paper*, 12 juin 2019, p. 3 (DOI : 10.31235/osf.io/xgz2s)
[219] *Id.*

et David Lie, affecté d'un « décalage fondamental entre les lois sur la protection des données et l'écosystème du « *smart* ». Les lois sur la protection des données reposent sur les idées de contrôle individuel sur les données à caractère personnel, et sont centrées sur les relations entre individus et organisations (publiques ou privées). Mais la collecte de données dans un système *smart* ne se modèle pas facilement sur l'intention individuelle de partage d'informations à caractère personnel avec une organisation prodiguant un produit ou des services. Au contraire, elle implique une collecte opaque d'informations, qui peuvent ou non concerner des individus, et qui peuvent permettre ou non leur identification » (trad. pers.)[220]. En l'absence de réalisation du projet, la possible réticence des habitants à partager des informations tirées de leurs pratiques quotidiennes les plus fines n'a pas pu être observée *in situ*. Cependant, c'est bien de la question de l'impossible recueil du consentement des habitants potentiels au partage de leurs données à caractère personnel qui a motivé les autorités ontariennes à reprendre la main sur le Data Hub, et Google à se retirer d'un projet qui ne présentait à ce titre plus d'intérêt pour sa filiale[221]. Si l'on reprend l'échafaudage de Carullo et Kitchin (voir Tableau 3), on observe du reste que la « modalité » du projet de Google relevait finalement d'abord du « paternalisme civique » plus que de « l'autonomisation » des habitants, malgré un caractère relativement « inclusif » à travers la possibilité prévue de fournir le maximum possible de données ouvertes par Sidewalk Labs.

D'une certaine manière, Amazon/Ring a finalement mieux réussi dans le domaine de la *smart city* que Google/Sidewalk Labs, en affichant une ambition certes beaucoup plus modeste, mais surtout en avançant masqué. Dans le cas de la mise en place d'un réseau de vidéosurveillance de l'espace public fondé sur l'utilisation des serrures connectées *Ring*, ce sont les habitants eux-mêmes qui choisissent de s'équiper des dispositifs qui rendent possible la *smart city* dans sa dimension sécuritaire. Pour Francisco Klauser *et al.*, la question sécuritaire n'est d'ailleurs pas seulement une dimension mais bien le fondement de toute démarche de

[220] *« The mismatch between data protection law and "smart" environments is fundamental. Data protection law is premised on ideas of individual control over personal information and centred on relationships between individuals and (private or public) organizations. But collecting data in smart environments is not easily modelled on the intentional sharing of personal information with an organization providing you with a product or services. Instead, it involves opaque collection of information that may or may not be about people and may or may not be identifiable. This collection is mediated through ubiquitous sensor technology as a by-product of the use of public space, and it is meant to enable multiple future (and often unspecified) innovative uses. Data becomes part of our public infrastructure rather than a feature of a particular transaction or relationship, unmoored from specific individuals and from specific projects and purposes, and created through complex private-public partnerships.* » L. AUSTIN et D. LIE, « Data Trusts and the Governance of Smart Environments: Lessons from the Failure of Sidewalk Labs' Urban Data Trust », *Surveillance & Society*, vol. 19, nº 2, 25 juin 2021, p. 259 (en ligne : https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/14409)

[221] L. AUSTIN et D. LIE, « Data Trusts and the Governance of Smart Environments », *op. cit.*

smart city[222]. Avec une infrastructure de vidéosurveillance presque largement assumée par des citoyens/consommateurs, le coût est quasi nul pour la puissance publique, et Amazon y est même rémunéré pour ses ventes. En ne proposant pas, au moins formellement, de mettre en place le système à la manière d'un aménageur classique, Amazon renforce en outre l'acceptabilité du dispositif aggloméré – ses briques étant individuellement déjà posées. En tout état de cause, le refus d'être surveillé par ce système reste impossible pour les passants[223], et les capacités scopique du pouvoir sont encore étendues.

Des pistes sont aujourd'hui explorées pour permettre aux individus d'imposer leur *opt-out* aux capteurs. Pour la vidéo, des maquillages faciaux ou des motifs particuliers peuvent empêcher la reconnaissance faciale plus subtilement qu'une capuche ou un masque, souvent interprétés comme suspects par les logiciels de reconnaissance. Pour l'audio, des chercheurs ont proposé un prototype d'émetteur transposant l'option « Do Not Track » des navigateurs web vers l'espace sonore : la requête est diffusée autour de la personne refusant l'enregistrement, à une fréquence de plus de 22 kHz inaudible pour l'oreille humaine, et les enceintes connectées la captant pourraient alors désactiver l'envoi de séquences audio sur les serveurs de leur fabricant[224]. Pour autant, ces pistes sont encore bien loin de la généralisation facile d'options d'*opt-out*, et rien ou presque n'empêche aujourd'hui la circulation massive de ce type de données.

II - LA CIRCULATION DES DONNEES

La question de l'espace augmenté, on l'a vu, est première dans la réflexion sur la vie privée et la surveillance. Pour autant, elle est bien loin de l'épuiser : les cas où le problème perçu se limite à la captation de données en un lieu pour elle-même est limitée. Elle correspond bien au cadre de la vidéosurveillance quand les bandes, d'abord analogiques, circulaient finalement peu, quand elles existaient seulement, et que l'œil de la caméra servait surtout à démultiplier les angles de vue du regard d'un agent de sécurité ou d'un commerçant. À travers

[222] F. KLAUSER, T. PAASCHE et O. SÖDERSTRÖM, « Michel Foucault and the Smart City: Power Dynamics Inherent in Contemporary Governing through Code », *Environment and Planning D: Society and Space*, vol. 32, nº 5, SAGE Publications Ltd STM, 1er octobre 2014, p. 869-885 (en ligne : https://doi.org/10.1068/d13041p)

[223] Ce qui explique d'ailleurs que la protection des données desdits passants soit une des bases argumentaires de l'EFF dans son combat contre Ring.

[224] P. CHENG *et al.*, « Smart Speaker privacy control - acoustic tagging for Personal Voice Assistants », San Francisco (États-Unis), IEEE, 2019 (en ligne : https://cora.ucc.ie/handle/10468/8396 ; consulté le 17 novembre 2021)

le cas des sonnettes connectées Ring, on voit bien que l'enjeu de la circulation des données captées dans un lieu augmenté ne prend vraiment d'ampleur que lorsque les données circulent.

Une approche peu explicitement spatiale de la circulation des données

Comme nous l'avons déjà dit, la question spatiale est présente dans les analyses de Solove et Nissenbaum notamment, et constitue une nouveauté par rapport aux approches antérieures du privé comme chez William Prosser, par rapport auquel se positionne Solove avec sa nouvelle théorie de la *privacy*. Pour autant, l'espace n'est pas abordé comme une question en tant que telle par ces auteurs, ou plutôt la spatialité des questions de privé n'est pas explicitement évoquée. Ce, bien que cette question apparaisse dans la terminologie utilisée par Solove pour sa typologie (diffusion, dissémination, brèche…), ainsi que chez Nissenbaum lorsqu'elle évoque les contextes qui spécifient le caractère privé ou non de telle ou telle information en fonction de *transmission principles*. Chez ces deux auteurs, l'espace est un quasi impensé, quoi qu'ils le mobilisent finalement de manière presque systématique. En effet, leur pensée du privé s'articule notamment autour des données à caractère personnel, ce qui implique nécessairement de penser la circulation de ces données, soit dès après leur collecte, soit après traitement et recoupement avec d'autres sources de données pour la création de profils, puisqu'il n'y aurait sans cela jamais transgression où mise en jeu de l'intimité ou des informations des personnes.

Chez Solove, cela apparait nettement dans un schéma qu'il propose comme un « modèle » de sa taxonomie, et dans lequel il recourt à l'utilisation de nombreuses flèches pour signifier la circulation des données personnelles depuis un individu vers une entité figurée dans un carré, les « *data holders* », entreprises ou organisations ayant accès à ou traitant les données en question (voir Figure 5). Sans qu'il soit explicitement figuré, ce que Moles et Rohmer ne rechigneraient probablement pas à désigner comme la coquille du « vaste monde »[225], est suggérée dans la partie droite et dans la partie basse du schéma. C'est de cette zone floue que proviennent la pluralité des intrusions directes dans l'intimité des personnes, et vers cette zone que se fait la « dissémination » des données collectées. La grande simplicité de ce schéma est à prendre au sérieux, car Solove produit lui-même un grand nombre d'illustrations et d'infographies de grande qualité, souvent sous forme de petites bandes dessinées, pour illustrer ses cours et ses présentations. Sans doute la simplicité du schéma était-elle liée à des contraintes éditoriales, mais elle illustre d'une manière d'autant plus directe la manière dont Solove pense et conçoit spatialement la mise en œuvre des pratiques attentatoires au privé décrites dans sa

[225] A. A. MOLES et E. ROHMER-MOLES, *Psychosociologie de l'espace*, Paris (France), l'Harmattan, 1998, p. 102

taxonomie, sans pour autant s'attarder sur la spatialité de ces pratiques dans le corps du texte. En outre, elle permet de conserver au schéma son ouverture à tous les cas possibles, puisque ces pratiques peuvent être mises en œuvre par une grande diversité d'acteurs, à toutes les échelles et à toutes les métriques. En tout état de cause, ce schéma montre bien que, pour Solove, c'est la mise en relation d'une source de données liées à un individu et d'acteurs qui lui sont extérieurs qui met à l'épreuve le privé aujourd'hui.

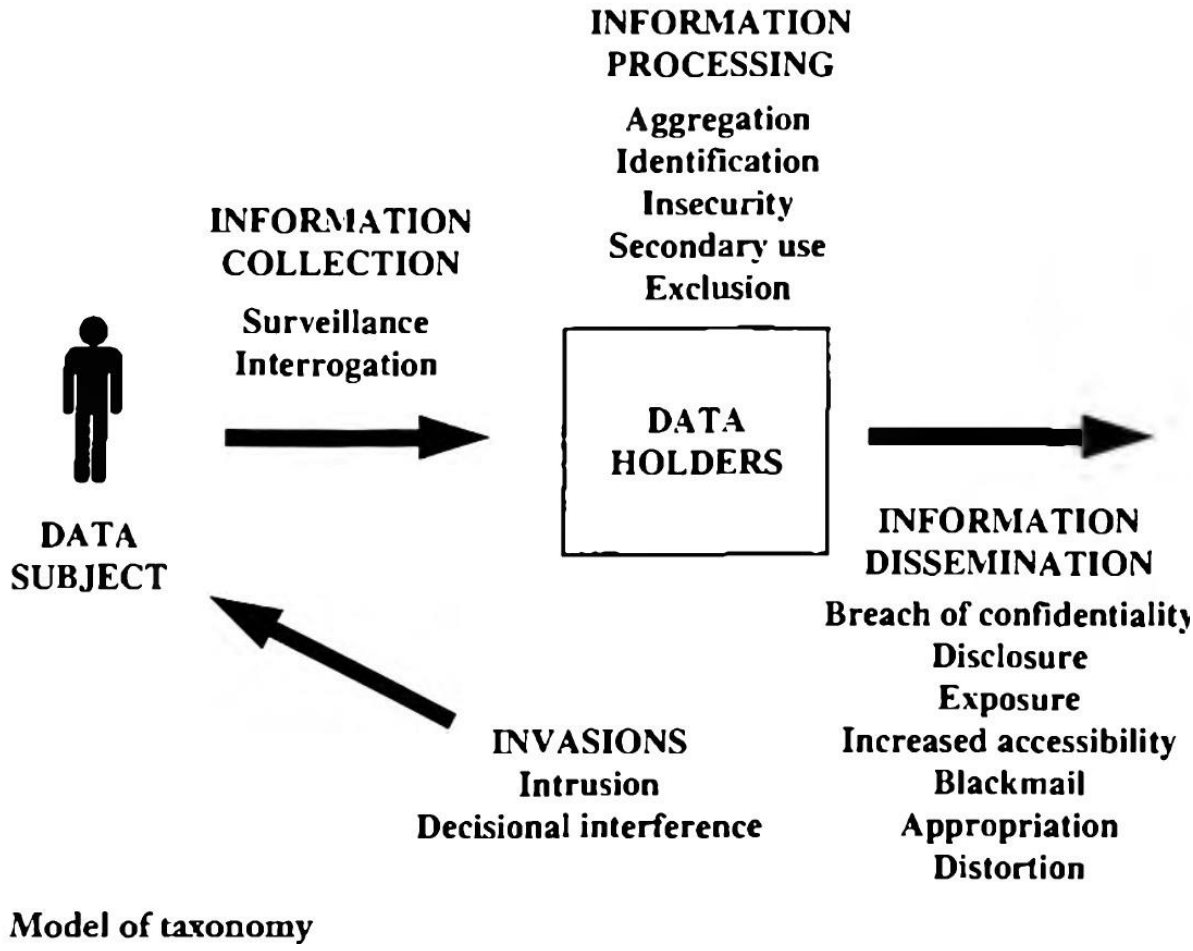


Figure 5 - Représentation graphique de la taxonomie de la privacy *de Daniel Solove (*Understanding Privacy*, p. 104)*

Chez Nissenbaum, c'est aussi la circulation qui importe. La question spatiale apparaît de façon plus explicite dans son texte, en particulier à travers la notion de « *transmission principles* ». Comme Solove, elle traite surtout des pratiques de collecte, traitement, et divulgation d'information qui font attaque au privé. Pour autant, il est intéressant de constater qu'elle fait une place particulière à des *transmission principles* qu'elle estime être un apport particulier de son approche du privé par rapport à d'autres référentiels : « L'idée d'un principe de transmission est probablement l'élément le plus distinctif du cadre de l'intégrité contextuelle ;

bien que ce que cela dénote soit facile à voir, on n'y prête généralement pas attention »[226]. Cette formulation laisse entendre qu'il n'y aurait pas directement d'enjeu dans la circulation même des données à caractère personnel, ce qui explique d'ailleurs que la question ne lui semble à elle non plus pas traitée outre-mesure par ses pairs (« *it (…) is plain to see, it usually goes unnoticed* »). De fait, Nissenbaum ne voit pas plus qu'eux dans la circulation des données à caractère personnel un problème en soi, et elle évoque beaucoup de cas où elles circuleraient de fait sans dommage, comme on l'a vu avec son exemple des données médicales partagées au sein d'une équipe de soignants. Néanmoins, elle estime tout de même nécessaire de traiter des « principes » encadrant cette circulation de données, dont elle fait un des éléments distinctifs de son approche (« *[maybe] the most distinguishing element of the framework of contextual integrity* »). Pour elle, c'est encore et toujours de l'atteinte à l'intégrité du contexte dans lequel se fait la circulation des données que peuvent éventuellement naître des problèmes de vie privée.

Il faut par ailleurs signaler que Nissenbaum, contrairement à Solove, n'élude pas totalement l'espace dans sa réflexion. Après avoir présenté l'exemple d'un processus d'achat dans un magasin physique, et la manière dont on peut choisir ou non de communiquer ses données au vendeur en réglant en espèce ou par carte de crédit, Nissenbaum décrit la même expérience, « par contraste, dans le cyberespace » où « l'exception » du traçage permis par la carte de crédit « devient la norme ». Elle semble néanmoins rétive à considérer que les espaces en ligne soient pleinement des espaces : le référentiel géospatial classique est présenté avant tout comme un moyen (fut-il « le meilleur moyen ») de comprendre par analogie ce qui se passe dans les transactions en ligne. Mais cette analogie n'est « à prendre au sérieux [que] pour un moment », et le cyberespace lui semble avant tout une « métaphore » spatiale[227].

Une autre auteure contemporaine étatsunienne, Shoshana Zuboff, met pour sa part la question de la circulation des données à caractère personnel au cœur de son système de pensée. C'est en effet de la captation et de la circulation des données personnelles que dépend selon elle le « capitalisme de surveillance ». Il est intéressant de constater que la plupart des items relatifs à la création de valeur identifié par Zuboff correspondent peu ou prou aux divers types d'atteinte à la vie privée identifiés par Solove, médiés par son concept central de surplus comportemental

[226] « *The idea of a transmission principle may be the most distinguishing element of the framework of contextual integrity; although what it denotes is plain to see, it usually goes unnoticed* » (trad. pers.) *in* H. F. NISSENBAUM, *Privacy in context*, *op. cit.*, p. 145

[227] « *By contrast, in cyberspace, the exception becomes the norm: Every interaction is like the credit card purchase. The best way to grasp this point is to take seriously, if only for a moment, the metaphor that cyberspace is an actual place, a computer- constructed world, a virtual reality. In this alternate universe, you are invisibly stamped with a bar code as soon as you venture outside your home*. » *Ibid.*, p. 28

(« *behavioural surplus* »). Zuboff parle de surplus pour signifier que les entreprises dont le modèle d'affaires repose sur l'exploitation des données ne se contentent pas de collecter des données afin de fournir un service à leurs clients, mais que ces données – et d'autres – seront également utilisées à des fins commerciales n'ayant rien à voir avec le besoin exprimé. Elle fait ici un parallèle avec la théorie marxienne de la captation de la plus-value ou de la survaleur (*surplus value*, en anglais) du travail du salarié par son patron capitaliste afin de générer un profit résultant de l'écart entre la valeur ajoutée par le travailleur et la rémunération de sa force de travail. Dans le cas du capitalisme de surveillance, c'est l'écart entre le profit généré par l'exploitation des données de l'utilisateur et le coût du service qui lui est rendu qui crée un surplus, et donc une forme nouvelle de plus-value qui justifie, pour Zuboff, de distinguer le capitalisme de surveillance du capitalisme historique. Ce profit résulte en particulier des possibilités offertes par les données captées ou renseignées en termes de profilage et de prédiction des autres besoins de l'utilisateur, inférés algorithmiquement, afin de lui adresser des publicités mieux ciblées et plus rémunératrices pour les différentes entreprises intégrées à la chaîne du capitalisme de surveillance (voir Figure 6).

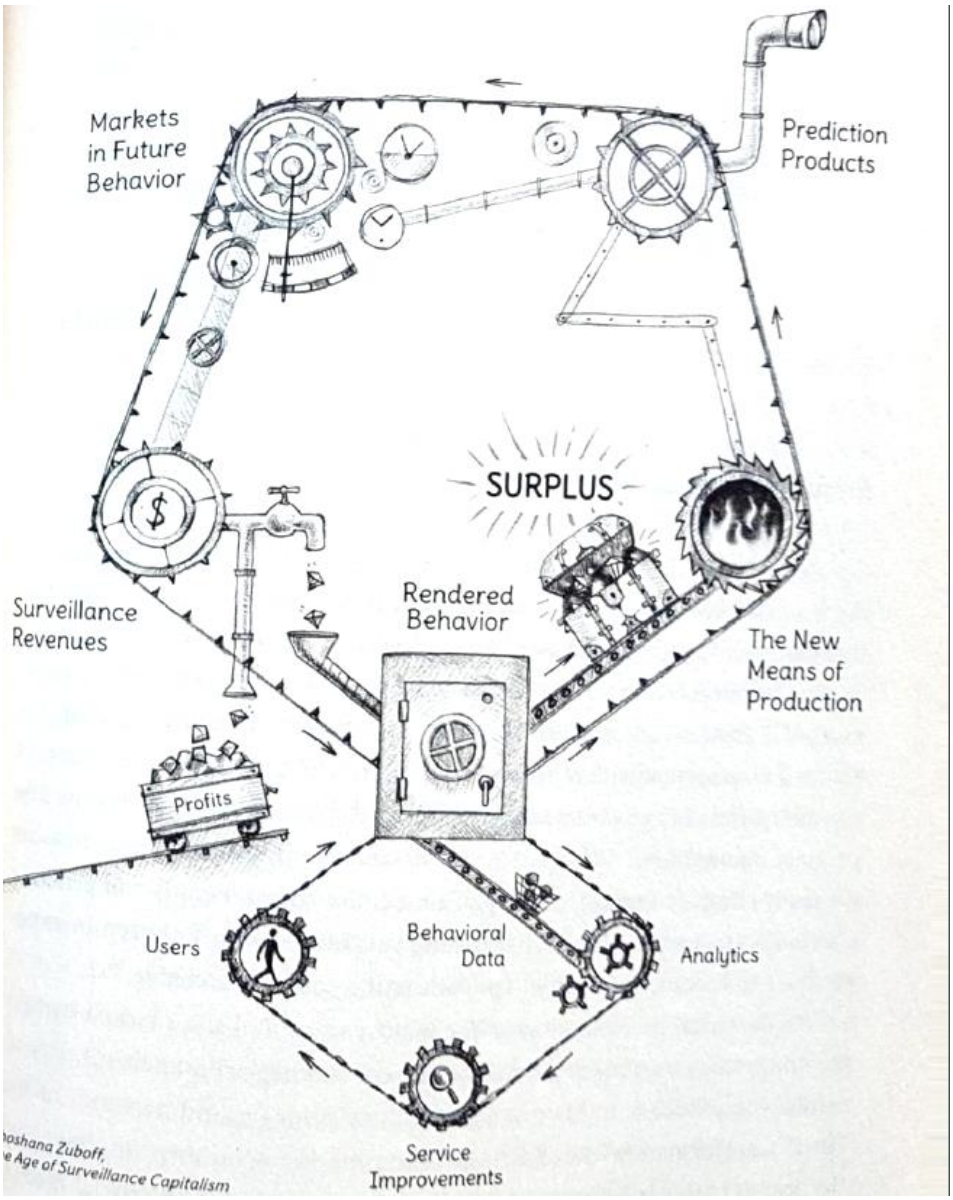


Figure 6 - The Discovery of Behavioral Surplus (Zuboff, 2019, p. 97)

Cette idée illustrée par Zuboff que les données produites par les utilisateurs d'appareils et de services numériques circulent avec une grande facilité par Internet est très bien comprise de l'ensemble des enquêtés, et ce même pour des informations triviales. Au moment d'expliquer son refus de posséder une enceinte connectée, E19 explique par exemple « (…) que j'ai pas envie que même si c'est au fin fond du Texas ou de je-ne-sais-où on vienne savoir que moi j'écoute France Inter plutôt que RTL. J'ai pas envie de savoir que... (elle rit) Guillaume Meurice il me fait marrer ! (je ris à mon tour) » (entretien 12 ; 17 min). Âgée de 62 ans au moment de l'entretien, et ayant connu l'informatique d'abord à travers ses outils de travail, E19 évoque sans doute le Texas dans la mesure où il était l'État emblématique du développement de l'informatique au début de sa vie professionnelle, à travers des entreprises comme Dell ou Texas

Instruments, avant l'apogée que connaît actuellement la Californie. Son « je-ne-sais-où » laisse entendre qu'elle a bien conscience, d'une part, que l'essentiel des questions liées au numérique ne se joue plus spécialement au Texas et, d'autre part, que la circulation des données passe désormais à travers un semis beaucoup plus diffus et distribué de *data lakes* et autres centres de calcul. En outre, elle a bien conscience du caractère non-anecdotique d'informations à caractère personnel comme sa station de radio préférée, France Inter, qui renseigne par exemple sur son positionnement politique d'auditrice – de fait, au moment de me faire la démonstration de la manière dont fonctionne l'Assistant de Google sur son téléphone une quarantaine de minutes plus tard, son mari, E18, choisira de poser à plusieurs reprises la question « quel est l'âge de François Hollande ? ». Elle craint notamment la publicité ciblée, qu'elle abhorre, et réagira fortement plus tard dans l'entretien au sujet des manipulations politiques comme Cambridge Analytica. En somme, E19 a conscience qu'une information aussi simple que de savoir quelle émission de radio elle écoute est une information d'ordre privé susceptible d'être collectée et diffusée de par le monde (pratiques de *collection* et de *dissemination* / Solove), que cette information est susceptible de circuler dans un contexte publicitaire auquel elle n'adhère pas (rupture de *contextual integrity* par dérogation aux *transmission principles* auxquels elle adhère, à savoir écouter anonymement sa radio sans que cette information ne sorte de chez elle / Nissenbaum) et que de telles pratiques serviraient à nourrir des outils de profilage publicitaire ou d'influence politique (création de *behavioral surplus* / Zuboff).

Le courtage en données et le ciblage publicitaire et commercial

Une hypothèse de travail déjà bien corroborée par des travaux antérieurs et les observations préludant aux entretiens est que c'est d'abord à travers la question du ciblage publicitaire et commercial par des entreprises privées que les personnes prennent conscience de l'exploitation de leurs pratiques numériques. Elle saute même littéralement aux yeux lorsqu'une recherche sur Internet pour un produit donné entraîne l'affichage de publicités sous forme d'encarts ou de *pop-ups* sur d'autres sites sans lien apparent avec le premier dans les jours de navigation qui suivent cette recherche. Les infinies variantes individuelles de cette expérience sont un lieu commun des discours sur la vie privée numérique. Le fait qu'une information entrée sur un premier site (par exemple, « je cherche des sandales pour femme en taille 39 ») se traduise par l'apparition de publicités pour un produit répondant au besoin exprimé sur une grande partie des pages et applications visitées ultérieurement révèle sans doute possible que la première information a circulé, puisqu'elle a été mise à profit pour l'affichage de publicités sur d'autres sites que le premier visité.

« E18: Moi, ce qui m'ennuie, c'est que... c'est que c'est par Internet. C'est-à-dire on se connecte à Internet ou à un site, Google sait... enfin, ou autre, d'ailleurs, sait parfaitement tout ce qu'on consulte à telle heure, a des idées sur tout, sur notre rythme de vie, sur les sites qui nous intéressent, enfin bon... Sur le téléphone, ou sur l'ordi, à chaque fois il nous propose des pubs qu'ils essaient de cibler de plus en plus, quoi.

JF: Ouais.

E18: Donc, heu... c'est vrai que moi ça me dérange et ça m'énerve. Et... d'ailleurs ça a un effet inverse. Par exemple, quand je suis sur ma messagerie Google, la boîte de réception, ben les promotions que je regarde parce que c'est des trucs auxquels je me suis abonné (= onglet de tri automatique de Google, pas tout à fait du spam) , il y a toujours le petit bandeau avec les deux pubs, là, ciblées, et... donc au début je regardais parfois, maintenant je ne les regarde plus. J'arrive pas à comprendre aussi l'intérêt puisque... j'ai ça, je les regarde pas, et même à un moment j'ai même... quand je les regardais, je les ouvrais pas mais je regardais un truc, j'avais même envie de ne PAS, heu... de faire de l'anti-pub, c'est-à-dire...

JF: (interrompant) ...ne pas cliquer.

E18: J'ai la pub, ces trucs-là ça m'énerve parce que c'est répétitif, aussi pareil sur le téléphone quand ils font des publicités ciblées. Heu... Même le petit bandeau en-haut ça m'énerve, et quand je vois le truc, j'aurais plutôt envie de ne pas acheter le truc. De, de, d'avoir une position volontaire pour dire "ça c'est... ça me perturbe, ça m'énerve, et donc je le prendrai pas".» (entretien 12 ; 18 min 40 s)

L'exemple de E18 est intéressant en cela qu'il confirme l' idée que la question du privé est fondamentalement spatial : ce qui le gêne est qu'une information communiquée en un lieu où sa circulation est légitime (le champ du moteur de recherche Google) soit disséminée à d'autres fins que de lui rendre service en lui fournissant une liste de liens pertinents, et qu'il en ait conscience par le fait qu'il retrouve la marque d'intérêt exprimée par sa recherche sous forme de publicités « ciblées » qui lui sont diffusées en d'autres lieux (comme sa messagerie), voire d'un terminal à l'autre (entre son ordinateur et son téléphone). Nous verrons que cette réticence à la dissémination d'informations de recherche s'exprime plus puissamment encore chez les utilisateurs actifs ou passifs d'assistants vocaux.

III - HYPERCENTRALITE ET DISSEMINATION DES DONNEES

Concentration des acteurs économiques

D'un point de vue spatial, une des tendances les plus fortes de l'ère numérique est la concentration des flux de données entre les mains d'un nombre restreint d'acteurs dominants.

La discipline économique décrit bien le phénomène de concentration d'un point de vue industriel et commercial : l'acronyme GAFAM désigne ainsi, en première analyse, un simple oligopole. On peut même choisir de ne le traiter que sous cet angle[228]. Il est indéniable que les capacités financières des principales entreprises du numérique leur permettent des pratiques d'acquisition très agressives, et donc l'achat de tout nouveau concurrent potentiel avant qu'il n'ait pris l'ampleur des membres existants de l'oligopole – et si l'on exclut les marchés réservés, comme pour l'Internet chinois qui dispose de son propre oligopole avec les BATX (Baidu, Alibaba, Tencent et Xiaomi). Il est tout aussi indéniable que tout nouveau concurrent, même déterminé à exister hors de la perspective d'un rachat par l'un des GAFAM, doit subséquemment se hisser au niveau d'entreprises parmi les plus puissantes au monde. L'approche strictement économique de ce secteur n'en serait pas moins extrêmement réductrice. Ce serait méconnaître le fait que ces entreprises n'opèrent pas sur un marché tout aussi banal que le fait qu'elles aient, en droit, une personnalité morale certes comparable à celle de toute autre société commerciale. Ainsi, pour Boris Beaude,

> *« Les propriétés spécifiques des lieux de synchôrisation réticulaires accentuent considérablement les logiques de concentration, au point de remettre en cause la notion même de centralité. Cela se traduit par ce que l'on peut appeler de l'hypercentralité, une centralité qui, par coalescence, tend à concentrer l'essentiel des pratiques en un nombre très limité d'espaces. À présent, cette spatialité, résultant de milliards d'actions individuelles, est maîtrisée par quelques acteurs privés. Ils disposent ainsi d'une connaissance et d'un contrôle inédit sur nos pratiques et notre vie privée, que nous n'accepterions d'aucun acteur territorial. »*[229]

Il illustre ce concept à travers l'exemple de Google, qui est sans doute l'entreprise la plus hypercentrale en matière de pratiques en ligne : « Si Internet avait un centre, ce serait probablement Google. Si Internet n'avait pas de centre, Internet serait probablement Google. »[230] Brigitte Simonnot et Gabriel Gallezot, qui ont consacré un livre à Google en 2009,

[228] Nikos Smyranaios avance par exemple que « la forme actuelle de l'internet ne doit rien à ces caractéristiques techniques supposément intrinsèques que j'ai mentionnées précédemment, mais résulte des relations complexes entre acteurs dont les intérêts économiques et politiques sont à la fois puissants et antagoniques. » N. SMYRNAIOS, « L'effet GAFAM : stratégies et logiques de l'oligopole de l'internet », *Communication & Langages*, vol. 2, n° 188, NecPlus, 2016, p. 61-83 (en ligne : https://www.cairn.info/journal-communication-et-langages1-2016-2-page-61.htm)
[229] B. BEAUDE, *Internet: changer l'espace, changer la société*, *op. cit.*, chap. 2
[230] *Ibid.*, p. 102

le décrivaient pour leur part comme un « entonnoir » captant requêtes et données des utilisateurs comme des sites tiers à travers ses services[231]. Une « spatialisation » de la designeuse Louise Drulhe reprend d'ailleurs graphiquement cette forme (voir Figure 7).

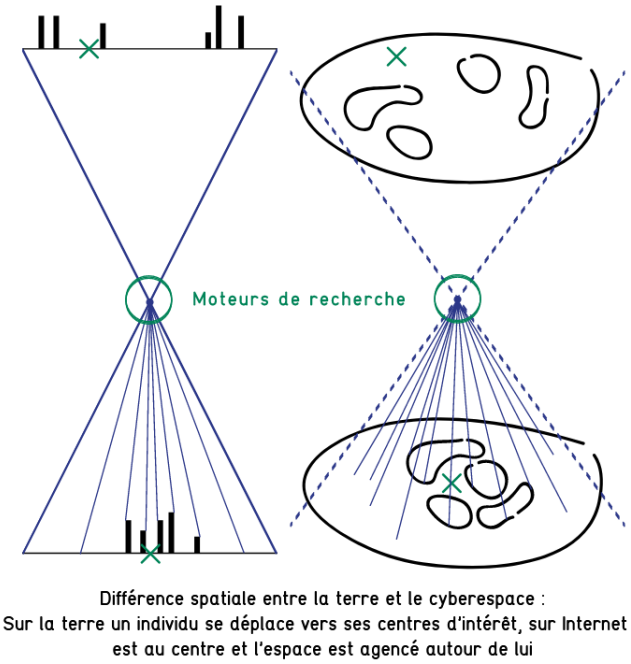


Figure 7 - Mise en forme graphique d'une citation de Boris Beaude par la designeuse Louise Druhle[232]

> « Imaginons un monde dont toute nouvelle action spatiale partirait d'un centre, composé pour l'occasion par une entreprise spécialisée, chargée d'agencer autour de vous les espaces qui répondent le mieux à vos attentes. »
>
> Boris Beaude - Internet, changer l'espace changer la société

Il est bien connu que les moteurs de recherche sont depuis longtemps les « portiers » (« *gatekeepers* ») de la navigation sur Internet, contre son fonctionnement initial en « rhizome »[233], et le moteur de recherche de Google plus que tout autre, à travers lequel déjà 86,3 % des recherches étaient effectuées dans le monde en avril 2010, malgré la concurrence localement forte de quelques autres acteurs, comme Baidu en Chine[234]. En continuant de prendre la question à rebours de l'approche strictement économique, on peut dire que les dépenses faites en ce sens sont, plus encore qu'une simple stratégie de visibilité de marque, surtout révélatrices de l'enjeu colossal qu'il y a à maintenir son hypercentralité dans un espace

[231] B. SIMONNOT et G. GALLEZOT (éd.), *L'entonnoir: Google sous la loupe des sciences de l'information et de la communication*, Caen (France), C&F éditions, 2009
[232] L. DRULHE, *Atlas critique d'Internet - Spatialisation d'un objet complexe en vue d'en comprendre les enjeux socio-politiques*, Paris (France), 2015
[233] A. HESS, « Reconsidering the Rhizome: A Textual Analysis of Web Search Engines as Gatekeepers of the Internet », dans A. Spink et M. Zimmer (éd.), *Web Search: Multidisciplinary Perspectives*, Berlin & Heidelberg (Allemagne), Springer, 2008, p. 35-50
[234] T. SEYMOUR, D. FRANTSVOG et S. KUMAR, « History Of Search Engines », *International Journal of Management & Information Systems*, vol. 15, nº 4, 12 septembre 2011, p. 56 (en ligne : https://www.clutejournals.com)

et un marché tel qu'Internet. En 2021 encore, il est ainsi estimé que Google aurait versé quinze milliards de dollars à la seule entreprise Apple[235] simplement pour rester le moteur de recherche par défaut sur ses terminaux[236].

Si l'on transpose cette logique aux pratiques numériques médiées par une enceinte connectée, j'avance que la logique d'hypercentralité s'applique là encore, même si l'on pourrait opposer de prime abord que la vente de biens manufacturés répond à une logique économique plus classique. D'une part, parce que les enceintes connectées ne sont pas de simples objets, mais des terminaux donnant un accès exclusif à un assistant vocal lié à un fabricant, sauf très rares exceptions[237]. Plus encore que sur un ordinateur ou sur un téléphone, dont on peut le plus souvent changer le moteur de recherche par défaut du navigateur, le navigateur lui-même, voire le système d'exploitation, et sur lequel on peut toujours choisir de visiter la page d'un autre moteur de recherche, le choix d'un modèle d'enceinte connectée lie entièrement son utilisateur à un assistant vocal donné. D'autre part, en l'absence de protocole standard pour la domotique, il est également à noter que le choix de l'assistant conditionne l'éventail d'objets connectés compatibles (voir « Maximiser la compatibilité avec les applications et objets possédés ou désirés », p. 325). Il y a ainsi une forme d'effet de réseau ou de club pour les enceintes connectées, dont Beaude expliquait déjà qu'il était un moyen de parvenir à l'hypercentralité, mais jusqu'ici plutôt pour les sites et logiciels voués aux interactions sociales. Par exemple, il est plus logique de choisir de s'inscrire sur tel réseau social ou d'utiliser telle application de messagerie instantanée si les personnes que l'on désire y retrouver y sont déjà inscrites – c'est ce qui a longtemps expliqué le succès sans partage de Facebook, même face à une solution concurrente techniquement comparable comme Google Plus, ou qui explique encore que WhatsApp soit l'application de messagerie la plus utilisée, voire qu'elle soit presque un standard *de facto* pour la messagerie dans certains pays[238]. Dans le cas des enceintes connectées,

[235] Qui concentre, certes, un nombre important de clients au niveau de vie moyen élevé, donc intéressant à capter pour une régie publicitaire.
[236] A. PLANCHER, « Google va payer 15 milliards de dollars à Apple pour rester le moteur de recherche par défaut », sur *Siècle Digital*, 27 août 2021 (en ligne : https://siecledigital.fr/2021/08/27/google-va-payer-15-milliards-de-dollars-a-apple-pour-rester-le-moteur-de-recherche-par-defaut/ ; consulté le 16 septembre 2021)
[237] Sonos a notamment commercialisé une enceinte, Sonos One, dont la première génération a été compatible avec Alexa et Google Assistant. Mais ce type de produit reste exceptionnel. Voir M. GEORGESCU DE HILLERIN et M. CIOLFI, « Sonos One, la première enceinte qui mixe Alexa et Google Assistant », *Les Numériques*, 5 octobre 2017 (en ligne : https://www.lesnumeriques.com/platine-musicale-serveur-audio/sonos-one-p41423/sonos-one-premiere-enceinte-qui-mixe-alexa-google-assistant-n67073.html ; consulté le 17 septembre 2021)
[238] Ainsi, au Liban, l'annonce d'une possible taxe sur l'utilisation de WhatsApp a contribué à nourrir le grand mouvement contestataire de 2019. L. STEPHAN, « « L'annonce de la taxe sur WhatsApp est l'étincelle » : colère contre de nouveaux prélèvements à Beyrouth », *Le Monde*, 18 octobre 2019 (en ligne : https://www.lemonde.fr/international/article/2019/10/18/tout-est-cher-au-liban-on-n-en-peut-plus-a-beyrouth-des-milliers-des-manifestants-contre-de-nouvelles-taxes_6016010_3210.html ; consulté le 17 septembre 2021)

c’est plutôt pour les services tiers que joue le phénomène : il n’est pas intéressant de développer une *app* ou *skill* pour un grand nombre de systèmes différents, et un Spotify (pour l’écoute de musique en ligne), un Philips (pour l’éclairage connecté) ou un Krups (qui vend, entre autres choses, des cafetières connectées) préfèrera concentrer son développement logiciel sur les systèmes les plus répandus, à savoir Google Assistant, Alexa d’Amazon ou Siri d’Apple.

Cette situation n’est pas forcément pérenne. Il est tout à fait possible que plus de produits proposeront à terme l’utilisation de l’un ou l’autre assistant vocal, et certaines marques tentent encore de proposer leurs propres écosystèmes (comme Samsung avec Bixby). Pour autant, on a déjà pu constater dans le cas d’un objet connecté comparable, le *smartphone*, que dix ans ont suffi à ce que l’offre se structure autour de deux systèmes d’exploitation, Android de Google et iOS d’Apple, là où une concurrence non-négligeable existait au départ (voir Figure 8).

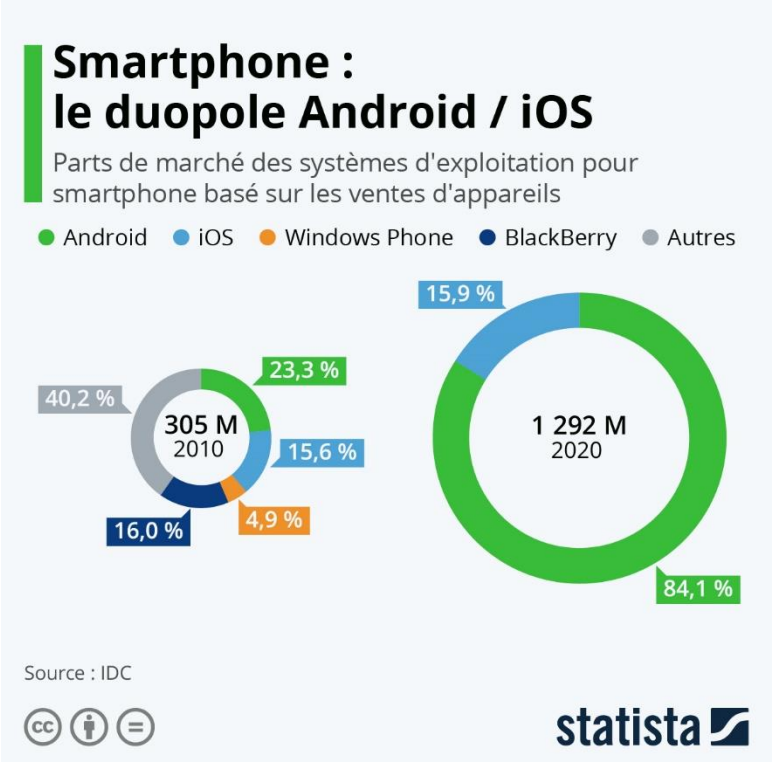


Figure 8 - "Smartphone : le duopole Android / iOS" (Tristan Gaudiot, Statista, 2021)

Des effets contrastés sur la vie privée : logique d’État et logique commerciale

De prime abord, la concentration de la collecte et du traitement des données à caractère personnel par un petit nombre d’acteurs en situation d’hypercentralité est potentiellement très dommageable pour la protection de la vie privée des individus. Dans le cas des fichiers publics rassemblant des informations sur les citoyens, comme SAFARI, la logique de compartimentation a longtemps été vue comme le meilleur garde-fou contre le potentiel de nuisance de la puissance étatique (voir « Une demande sociale ancienne autour de la vie

privée », p. 47). Or, des sociétés comme Google, Amazon ou Facebook en particulier ont un accès privilégié à une quantité et à une diversité colossale d'informations sur leurs utilisateurs, « que nous n'accepterions d'aucun acteur territorial »[229], pour reprendre les termes de Boris Beaude. Toutes ne sont pas également hypercentrales, ou pas dans tous les domaines (voir Tableau 4).

Tableau 4 - Comparaison des niveaux de collecte de données à caractère personnel selon le modèle d'affaires et le nombre d'utilisateurs de l'entreprise dans différents domaines. Vert : fort, jaune : intermédiaire, rouge : faible (JFP, 2021)

Entreprise	**Navigation en ligne**	**Enceintes connectées**	**Objets connectés hors *smartphone***	***Smartphones***	**Messageries, réseaux sociaux**
Google					
Amazon					
Facebook					
Apple					

Grâce à Android, son moteur de recherche et à la multitude de ses services (YouTube, Gmail, Google Maps…), et désormais aux objets connectés à Google Home, Google est sans doute l'acteur le plus hypercentral aujourd'hui. Cela se constate d'ailleurs assez bien dans le discours des enquêtés. Une analyse textométrique simple avec le logiciel *Sonal* permet de distinguer quelles sont les marques les plus citées au cours des entretiens (voir Tableau 5).

Tableau 5 - Analyse textométrique de l'évocation d'entreprises du numérique au cours des entretiens (JFP, 2021)

	Nombre d'occurrences			Évocation en entretien		
	Total	Dans les questions	Taux de suggestion	Spontanée	Total	Taux de spontanéité
Google	641	245	38%	9	16	56%
Facebook	251	68	27%	10	14	71%
Amazon	166	79	48%	9	15	60%
Apple	161	62	39%	7	12	58%
Microsoft	7	5	71%	2	6	33%
Orange	7	2	28%	2	4	50%
Bose	3	0	0%	2	2	100%
Free	3	1	33%	2	2	100%
Snips	2	2	100%	0	2	0%

Google est très nettement la première marque citée, totalisant même à elle seule plus d'évocations que toutes les autres entreprises citées réunies (voir Figure 9). Cette statistique est légèrement faussée par le fait que 66 occurrences du mot Google sont incluses dans le groupe nominal « Google Home », qui désigne l'enceinte connectée plutôt que la marque elle-même.[239] Même alors, près de la moitié des occurrences vont à la seule Google.

[239] La même remarque peut s'appliquer, en principe, au groupe nominal « Amazon Alexa », parfois usité, qui ne concerne cependant que quatre occurrences du corpus, dans les faits.

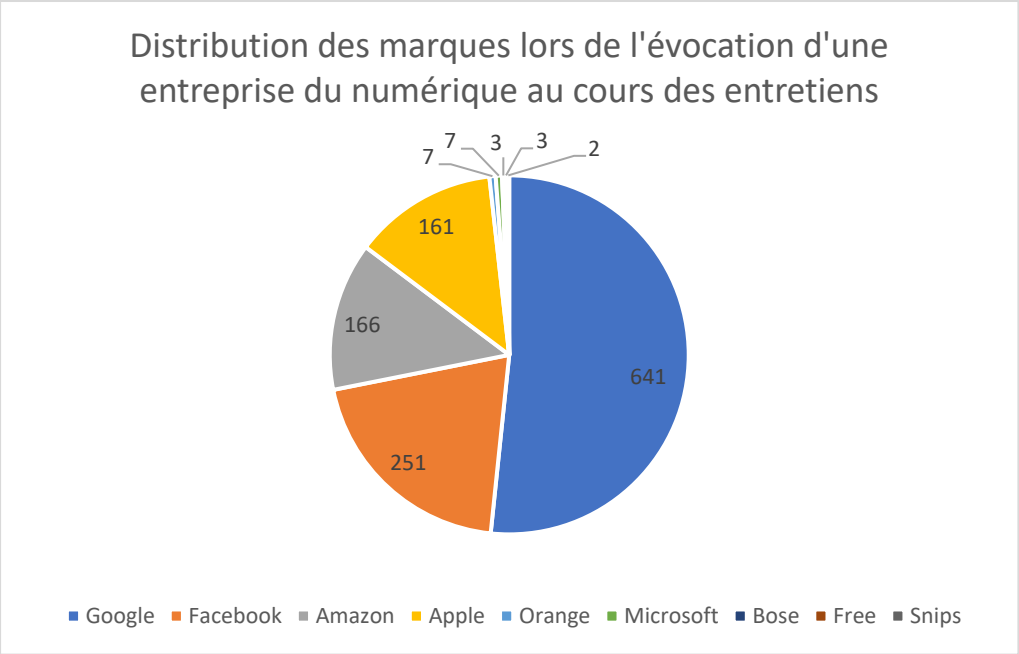


Figure 9 - Distribution des marques lors de l'évocation d'une entreprise du numérique au cours des entretiens (JFP, 2021)

Ce sentiment est partagé par bien des enquêtés, qui parlent souvent des GAFAM comme sachant tout d'eux, et Google au premier chef. Rencontrés dans le magasin Boulanger de Lyon Cordeliers, E12 et E13, qui travaillent dans l'informatique, axent beaucoup la conversation sur la comparaison technique des fonctionnalités et des « philosophies » des différentes marques :

> « JF: sur les questions vie privée et tout, vous avez un avis ? Des réticences ?
> E13: bah, Amazon, Google, euh voilà quoi ! Il n'y a pas de vie privée, avec ça !
> E12: à mon avis c'est mort.
> JF: c'est limité parce que ?
> E12: C'est limité à cause de ça.
> JF: parce qu'ils ont pas autant de données qu'ils veulent, ouais.
> E12: ils gardent en mémoire, je crois trois mois, toutes les recherches. Au bout de trois mois, sur Siri, les recherches sont effacées automatiquement, c'est pour dire, quand on lui redit une phrase, « rappelle-moi que … » que justement Siri se rappelle bien ce qu'on a demandé y a, la semaine dernière par exemple.
> JF: ouais
> E12: mais sinon par contre il n'y a aucune donnée qui est partagée, à l'inverse de là (avec Amazon et Google), parce que là, le produit, c'est nous, faut le savoir ! » (entretien 12, 8 min)

Bien informés, ils opposent ainsi Apple à Google et à Amazon. Ils semblent convaincus par la volonté affichée d'Apple de ne pas exploiter les données de leurs utilisateurs pour produire de la valeur publicitaire. E12 est même au fait des pratiques affichées de conservation des données de l'entreprise (« ils gardent en mémoire, je crois trois mois, toutes les recherches. Au bout de trois mois, sur Siri, les recherches sont effacées automatiquement, c'est pour dire, quand on lui redit une phrase, « rappelle-moi que … » que justement Siri se rappelle bien ce qu'on a demandé y a, la semaine dernière par exemple. »). Cette confiance en Apple n'est pas forcément si répandue parmi les enquêtés, qui ont dans l'ensemble plutôt tendance à mettre tous fabricants dans le même sac. Les remarques d'E12 et E13 sur Google et sur Amazon sont, en revanche, sans appel : E13 déclare « bah, Amazon, Google, euh voilà quoi ! Il n'y a pas de vie privée, avec ça ! », et E12 renchérit une minute plus tard d'un « (avec Amazon et Google), parce que là, le produit, c'est nous, faut le savoir ! ». Dans les deux cas, et même si le reste de la conversation avec eux portent beaucoup plus sur Google que sur Amazon quand nous évoquons des services numériques plus généraux (*Google Maps* notamment), ces deux enquêtés expriment bien l'idée qu'il y a de la part de ces entreprises une mise à profit de leur position d'hypercentralité dans nos pratiques numériques pour faire de « nous » des « produits », selon un adage désormais répandu.

A contrario du discours sur l'hypercentralité des GAFAM comme un facteur de risque pour la vie privée des utilisateurs, E5 voit d'un mauvais œil la dissémination des données entre plusieurs acteurs pour limiter les possibilités d'agrégation de données en « fichiers » uniques comme SAFARI, dont on a vu qu'elle était pourtant un des axes majeurs de la protection des individus contre les acteurs étatiques :

> « E5: C'est même pire, que ce soit émietté entre plusieurs acteurs. Parce que si c'était, s'il n'y avait que, je sais pas, JC Decaux qui mettait des panneaux, ben on pourrait tous s'attaquer et se coaliser pour dire que JC Decaux est mal et essayer de le mettre à bas. Si c'est partout, ça infuse dans la société. Et ça nuit à la possibilité d'identifier ça comme un élément perturbateur. Et... Parce qu'on va dire "moi ça me pose problème ça", et on va répondre "mais c'est partout, même dans le métro, c'est même...". Du coup, la construction d'un discours, heu... qui permette de prendre conscience de ces violations devient plus difficile. Donc l'émiettement des acteurs facilite la perméabilité et la perméation (sic) du discours ou du phénomène. Fait accepter ces, ces... une action diffuse et constante de conditionnement. » (entretien 2 ; 24 min 50 s)

Un tel « émiettement » peut se lire comme un problème à deux niveaux, à un niveau tactique et à un niveau stratégique. Du point de vue tactique, il implique de se confronter à une multitude

d'acteurs pour la moindre lutte contre la dissémination des données. Du point de vue stratégique, il pense que cette multiplicité d'acteurs contribue à la diffusion fine de ces pratiques dans tous les aspects de notre « [perméable] » vie quotidienne, et y « [conditionne] » les individus. Le point de vue est intéressant, et très révélateur des réflexes de militance d'E5. Il est peut-être trop pessimiste cependant. En premier lieu, il n'est pas dit qu'il y ait un lien si clair que cela entre l'échelle très fine à laquelle s'insinuent capteurs physiques et logiciels dans les quotidiens individuels et l'échelle régionale voire mondiale à laquelle opèrent les acteurs économiques ou gouvernementaux les plus puissants. Les objets connectés utilisant les systèmes d'exploitation de Google (Android) notamment sont d'un nombre et d'une variété considérables, et présents partout dans le monde. C'est aussi vrai pour Amazon, mais plus spécifiquement dans le domaine de la domotique. Quoique la marque soit très puissante, c'est moins vrai en ce qui concerne Apple, qui ne permet par ailleurs pas l'ajout de surcouche logicielle par des constructeurs tiers, et dont le modèle d'affaires ne s'appuie pas ou très peu sur le courtage des données de ses utilisateurs. Certes, ces entreprises et leur pouvoir sur les données personnelles de leurs utilisateurs sont bien identifiés, et donnent d'ailleurs lieu à des campagnes d'information ou de contre-lobbying diversement efficaces, dont la mise en place du RGPD en Europe et les premières applications de sanctions sérieuses sont un résultat non-négligeable.

Pour autant, c'est bien leur hypercentralité qui leur confère leur pouvoir, qui continue de se traduire par le fait qu'elles sont encore en 2021 respectivement première et quatrième entreprises mondiales par la capitalisation boursière.

*

Au terme de ce chapitre, un constat finalement assez banal se dégage : comme beaucoup de faits sociaux la vie privée à l'ère numérique a été jusqu'ici essentiellement traitée sous l'angle du droit, de la sociologie ou de l'économie. Ces approches sont, bien sûr, essentielles, mais elles décrivent avant tout la « substance »[240] de ce fait social, et n'abordent qu'assez peu sa géographicité. Il ne s'agit pas là seulement de tirer à soi la couverture épistémologique, en reprochant aux autres disciplines les angles morts bien naturels de leur réflexion[241], mais plutôt de relever une certaine incongruité historique, et de pointer un véritable défaut conceptuel. De

[240] Dans le sens que Jacques Lévy donne au mot substance comme « composante non spatiale d'une configuration spatiale ». J. LEVY, « Substance », dans J. Lévy et M. Lussault (éd.), *Dictionnaire de la géographie et de l'espace des sociétés*, Paris (France), Belin, 2003, p. 880-881

[241] L'entretien de Michel Foucault avec la rédaction de la revue *Hérodote* dans son premier numéro en 1976 en est un des meilleurs exemples. Voir Anon., « Questions à Michel Foucault sur la géographie », *Hérodote - Revue de géographie et de géopolitique*, nº 1, 1976, p. 71-85 (en ligne : https://gallica.bnf.fr/ark:/12148/bpt6k5621035h/f80.vertical)

fait, dans la réflexion sur la vie privée avant l'ère numérique, la question spatiale était abordée de manière beaucoup plus directe. La réflexion était très structurée, notamment, par l'interrogation des limites entre espace privé et espace public, ainsi que par la proxémie. Cette approche, très féconde, constitue par exemple l'un des fils directeurs de toute l'*Histoire de la vie privée* dirigée par Duby et Ariès, des *Tyrannies de l'intimité* de Richard Sennett[242] ou du questionnement juridique de Marcela Iacub sur le « mur de la pudeur » dans *Par le trou de la serrure*[243].

Au moment de l'entrée dans l'ère numérique, pourtant, la réflexion spatiale sur les questions de privée se trouve réduite à sa portion congrue. Il ne s'agit plus guère que de décrire sommairement une circulation de données ou de diluer les rapports de distance entre les acteurs dans la notion de « contexte ». D'une certaine manière, il semble que l'idée d'une fin de l'espace à l'ère numérique et la difficulté à envisager la spatialités des médiations numériques aient contribué à évacuer l'espace, les distances et les métriques de la réflexion sur le privé de beaucoup d'auteurs majeurs travaillant sur la thématique du privé, au profit des seuls rapports sociaux, politiques et économiques entre des acteurs évoluant dans un espace plus ou moins flou, ou redevenu un simple décor pour des interactions fondamentalement aspatiales.

À contre-courant de cette tendance, il me semble au contraire que le privé est fondamentalement une question spatiale, et que c'est de l'espace, son espace que l'individu engage dans les « questions du privé » - et non seulement *par* l'espace qu'il met en jeu tout autre chose. Le micro-géotype emblématique du privé est, de ce point de vue, le domicile. Son importance est telle dans le champ qu'il constitue, encore aujourd'hui, un point de passage obligé même dans les analyses semblant aspatiales. L'essor de la domotique et de la *smart home* ne constitue pas un changement de paradigme technique, quoiqu'il relève d'enjeux économiques importants pour les entreprises des TIC. Cet essor n'est qu'un des bras du *megatrend* de la mise en numérique du Monde. En revanche, il constitue un moment important pour réintroduire sérieusement l'espace dans la réflexion sur le privé à l'ère numérique.

[242] R. SENNETT, *Les tyrannies de l'intimité*, A. Berman et R. Folkman (trad.), Paris (France), Seuil, 1995
[243] M. IACUB, *Par le trou de la serrure: histoire de la pudeur publique (XIXe-XXIe siècle)*, Paris (France), Fayard, 2008

Chapitre 3 - LE DOMICILE, LE GEOTYPE EMBLEMATIQUE DU PRIVE

« Pour beaucoup d'intelligences, la pensée des intimités familières est liée à un sentiment spontané de vague écœurement – raison pour laquelle il n'existe pas plus de philosophie de la suavité qu'une ontologie élaborée de l'intime. Il faut avoir conscience de la nature de cette résistance pour surmonter les aversions typiques des premiers temps. Vu de loin, le sujet paraît si peu séduisant que pour le moment, seuls les niais férus de d'harmonie ou les castrats théologiques peuvent y rester suspendus. L'intellect qui concentre sa force sur les objets dignes aime en général que les choses soient hot, pas suaves. On n'offre pas de bonbons aux héros. Compte tenu de cette orientation vers la vivacité intellectuelle et existentielle, qu'est-ce qui pourrait paraître plus suave, plus collant, moins héroïque que l'exigence scandaleuse de participer à une étude sur un espace pâteux, vague, humblement matriarcal ? Un espace où les hommes, dans un premier temps et la plupart du temps, se sont installés comme chercheurs de certitudes, comme habitants bienveillants de la normalité et occupants des asiles où ils trouvent satisfaction ? Qu'est-ce qui serait plus atteint par le mépris a priori que le dévouement des individus à l'espace existentiel parochial qui semble leur garantir une certaine commodité détendue auprès de soi-même ? »[244]

Selon Jean-François Staszak, l'espace domestique a longtemps fait l'objet de « négligence » par « les sciences sociales et particulièrement la géographie »[245]. Son caractère de quotidienneté, l'absence de « dignité » de cet espace pris dans une « suavité » l'aurait longtemps rendu incompatible avec des aspirations intellectuelles plus hautes dans la pensée du monde contemporain, pour reprendre Sloterdijk (voir ci-dessus). Au-delà de son intérêt général en tant que tel, précisément comme espace incontournable dans les pratiques quotidiennes, le logis est fondamental dans la pensée du privé. Je distinguerai ici le logis comme l'espace domestique de l'appartement ou de la maison, par rapport à un espace domestique qui peut être ponctuellement élargi à d'autres lieux – une chambre d'hôtel, une portion d'espace public occupée par une personne sans-abri, une tente de camping, etc. Le logis que nous possédons ou louons, et dont nous avons en tout cas l'usufruit, est en effet d'un statut particulier du point de vue juridique en tant que « domicile », et comme « cocon » où s'exprime de manière habituelle

[244] P. SLOTERDIJK, *Bulles*, O. Mannoni (trad.), Paris (France), Pauvert, 2002, chap. « Penser l'espace intérieur » (p. 100-103)
[245] J.-F. STASZAK, « L'espace domestique : pour une géographie de l'intérieur », *Annales de géographie*, vol. 110, nº 620, 2001, p. 340-341 (en ligne : https://archive-ouverte.unige.ch/unige:76456 ; consulté le 29 décembre 2022)

et récurrente le registre spécifique des pratiques du ressourcement privé comme des micro-aménagements de l'espace.

I - *A MAN'S HOME IS HIS CASTLE* : ASPECTS JURIDIQUES

Dans les rapports du logis au privé, le premier point à évoquer est de nature juridique. En effet, au-delà des considérations sociales et historiques qui établissent bien cette évidence qu'il y a un rapport organique entre l'individu et cet espace personnel de restauration des forces et de vie quotidienne qu'est son domicile, le droit est le principal domaine dans lequel le domicile est défini explicitement comme un espace privé, et même comme l'espace privé individuel par excellence, à partir duquel sont éventuellement déclinées des variantes, comme l'espace de la voiture personnelle. Pour autant, voyons, au-delà de l'évidence terminologique, ce que recouvrent ces termes.

Définitions juridiques du domicile

C'est probablement dans la *common law*, le système juridique d'origine britannique, partagé par la majorité des pays du Commonwealth, et fondé sur la jurisprudence[246] que l'on trouve l'expression la plus vive de ce caractère privé du domicile. Warren et Brandeis le rappellent dans la fin de leur article historique sur la *privacy* : « La *common law* a toujours reconnu que la maison d'un homme était son château, impénétrable, le plus souvent, aux officiers mêmes chargés de son exécution »[247]. L'expression anglaise *A man's home is his castle*, est non seulement proverbiale, elle est aussi une des sources jurisprudentielles fondamentales de la *common law*. Elle apparaît dans l'écriture de la loi anglaise sous la plume d'Edward Coke dans *The Institutes of the Laws of England* en 1628 : « La maison d'un homme est son château, et son foyer est son plus sûr refuge »[248], sur la base d'un jugement qu'il avait rendu en 1604 à Londres dans le cas Peter Semayne contre Richard Gresham – Gresham conservant à son domicile des biens sur lesquels Semayne estimait avoir des droits après une succession, la question s'était posée de savoir si la police londonienne était en droit d'accéder au domicile de Gresham malgré son refus opposé à leur entrée chez lui. L'emploi du terme château est ici très

[246] Généralement opposée aux systèmes dits civilistes, hérités de la tradition juridique romaine antique, et fondés sur des codes de lois.
[247] « *The common law has always recognized a man's house as his castle, impregnable, often, even to its own officers engaged in the execution of its commands.* » S. WARREN et L. BRANDEIS, « The Right to Privacy », *op. cit.*, p. 220
[248] *« For a man's house is his castle, et domus sua cuique est tutissimum refugium [and each man's home is his safest refuge]* ».

fort, et signifie entre autres choses qu'un homme est tout en droit de défendre l'entrée de son domicile, y compris par la force, et quelle que soit la qualité de la personne se présentant à sa porte – la tradition ajoute souvent : fût-ce le roi d'Angleterre lui-même.

Les traditions juridiques civilistes n'en protègent bien sûr pas moins le domicile elles aussi. Dans le droit français en particulier, cette protection est explicitement garantie par l'article 226-4 du Code pénal qui dispose que « l'introduction ou le maintien dans le domicile d'autrui à l'aide de manœuvres, menaces, voies de fait ou contrainte, hors les cas où la loi le permet, est puni d'un an d'emprisonnement et de 15 000 euros d'amende » et, pour ce qui concerne le cas spécifique des agents publics, l'article 432-8 du même Code dispose que « le fait, par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, agissant dans l'exercice ou à l'occasion de l'exercice de ses fonctions ou de sa mission, de s'introduire ou de tenter de s'introduire dans le domicile d'autrui contre le gré de celui-ci hors les cas prévus par la loi est puni de deux ans d'emprisonnement et de 30 000 euros d'amende ». Le droit pénal s'applique cependant à des actes et à des comportements considérés comme d'une certaine gravité, relevant de la criminalité. Que dit le Code civil, d'application beaucoup plus large, et qui traite notamment de questions beaucoup plus communes telles que la propriété, la vie de famille, etc., à propos du domicile ? Étonnamment, rien, ou presque. D'après la thèse de doctorat en droit civil consacrée à la protection juridictionnelle du domicile d'Isabelle Gravelais, c'est en fait à travers l'article 9 de ce code, « chacun a droit au respect de sa vie privée » que « semble [être assurée] la sauvegarde implicite de ce principe » d'inviolabilité du domicile.[249] L'information est d'importance, puisque le fait que cet espace d'habitation usuelle soit le lieu privilégié d'expression de la « vie privée » des personnes est précisément ce qui justifie sa protection juridictionnelle, mais surtout ce qui le définit du point de vue du droit tel qu'il est écrit dans les codes. D'une certaine manière, c'est la vie privée qui est première, et la notion de domicile qui en découle. C'est donc la jurisprudence qui joue dans le droit français pour définir plus précisément le domicile, cette définition n'étant pas donnée par les Codes : « (…) la notion de domicile applicable en France n'a pas, même dans la langue du droit, une signification unique et invariable. C'est pourquoi, elle n'est pas définie par les textes. Sa définition est l'œuvre d'une construction jurisprudentielle. »[250] Cette absence de définition juridique universelle ne doit pas être vue comme une insuffisance du droit. Elle permet en fait d'assurer que le droit puisse évoluer pour définir, selon l'évolution des pratiques

[249] I. GRAVELAIS, *La protection juridictionnelle de l'inviolabilité du domicile*, thèse de doctorat en droit public, Dijon (France), université de Bourgogne, 2013, p. 23
[250] *Id.*

et des conceptions, le domicile de la façon la plus adéquate : « le droit (...) [étant] chose vivante (...) il est préférable de confier au juge la tâche d'assurer, avec la prudence nécessaire, l'adaptation progressive (...) [de la notion de domicile] aux nécessités de chaque époque »[251].

Régenter les pratiques dans le domicile : la question des mœurs

Cependant, l'histoire du droit quant au domicile ne se limite pas à la question de la définition du domicile comme terme juridique. Marcela Iacub en donne une éclatante démonstration dans son livre *Par le trou de la serrure*, qui fait une « histoire de la pudeur publique » du XIXe siècle à nos jours en liant tout à la fois les évolutions juridiques de la distinction entre espace public et espace privé à la question de la sexualité et de leurs régimes de visibilité. Iacub identifie notamment trois jalons dans l'histoire juridique de la sexualité qui ont contribué à faire évoluer les contours des notions d'espace privé, d'espace public, et de domicile :

- L'instauration du Code pénal par Napoléon Ier en 1810, qui contribue à ériger ce qu'elle décrit comme le « mur de la pudeur » : la sexualité est réprimée dans l'espace public, et doit être renvoyée derrière ce fameux mur, c'est-à-dire essentiellement dans l'espace domestique ou assimilé. Moins puritaine qu'on pourrait le croire, cette évolution juridique laisse en fait une grande liberté d'action aux personnes dans leur domicile, dans lequel l'État ne prétend pas s'immiscer pour y réguler les mœurs comme il continuait à le faire dans l'espace public ;

- L'arrêt Ponce en 1877[252], qui introduit une modification de l'article 330 du Code pénal et introduit, selon Iacub, la notion de « *publicité intérieure* »[253] dans l'espace privé : il ne suffit plus qu'un espace soit fermé et privé pour qu'aucune infraction d'outrage à la pudeur puisse être constituée. Il suffit qu'une personne assiste à une scène sans l'avoir expressément voulu pour que la pudeur publique s'en trouve outragée à travers les yeux de ce témoin. La jurisprudence évoluera

[251] R. MERLE et A. VITU, *Traité de droit criminel. Tome 1 - Problèmes généraux de la science criminelle, droit pénal général*, 7e éd., Paris (France), Cujas, 1997, p. 249, cité par I. GRAVELAIS, *La protection juridictionnelle de l'inviolabilité du domicile*, *op. cit.*, p. 25

[252] Il s'agit d'une jurisprudence faisant suite au jugement d'Eugène Ponce en 1877. L'homme avait agressé sexuellement une veuve puis sa fille, ouvrières agricoles dormant dans une étable. La tentative de viol n'a abouti, mais des attouchements ont été faits par Ponce. Son jugement fut donc fondé sur un outrage à la pudeur, qui aurait pu ne pas être jugé répréhensible, puisque les faits se sont déroulés dans un lieu privé fermé. Pour autant, il a été jugé que mère et fille avaient été alternativement témoins des attouchements subis par l'une et l'autre, et la vue de cette scène (plus que l'acte même de l'agression !) leur ayant été imposée.

[253] M. IACUB, *Par le trou de la serrure*, *op. cit.*, p. 107

sur la notion de témoin, mais l'important est de voir comment une évolution juridique a changé le rapport aux espaces : « la Cour n'a pas créé une nouvelle forme de publicité propre aux espaces clos. Elle a élargi la notion d'espace public à ces lieux, en posant une sorte de fiction selon laquelle l'un des témoins n'aurait pas été présent au début des faits, mais les aurait découverts en ouvrant une porte faisant communiquer l'intérieur et l'extérieur »[254] ;

- La dernière étape a des contours plus flous dans l'histoire juridique, mais correspond à la libération des mœurs dans les années 1970, qui fait entrer la société française dans ce que Iacub appelle « l'heure du Sexe »[255] (la majuscule signalant un concept spécifique développé par Iacub, distinct du sexe ou de la sexualité dans leurs sens communs). Cette lente évolution se cristallise dans la réforme pénale de 1992, qui sort les termes « mœurs » et « pudeur » du champ pénal au profit des « agressions, atteintes ou exhibitions sexuelles ».[256] Cette évolution acte la fin de près de deux siècles d'histoire juridique au cours de laquelle la limite entre l'espace privé et l'espace public aura été régenté par le régime de visibilité effective ou potentielle d'actes « impudiques », et de « spatialisation de la sexualité »[257].

C'est surtout dans la deuxième phase, avec l'arrêt Ponce puis ses descendants jurisprudentiels, que les effets spatiaux du droit sont les plus nets sur le domicile. Un domicile à une seule pièce ne pouvait par exemple plus être un espace privé pour une famille, il fallait nécessairement qu'il existât une deuxième pièce fermable pour pouvoir s'y isoler, par exemple de ses enfants, et constituer un espace privé en « [fermant] la porte à clé et en [obturant] la moindre brèche »[258]. On le voit, cela nécessitait en outre la présence d'une porte et de murs absolument aveugles – le titre de l'ouvrage *Par le trou de la serrure*, renvoyant à une anecdote de justice où il avait même été estimé qu'un couple n'avait pas assez protégé le public de la vue de ses ébats, puisqu'il avait suffi à des voyeurs de pousser le bout de chiffon calfeutrant la serrure pour pouvoir assister à la scène. Ainsi, « L'arrêt Ponce devint la matrice de production d'espaces nouveaux que les architectes durent prendre en considération pour penser la distribution interne des appartements, notamment la séparation des chambres à coucher des autres lieux. »[259]

[254] *Ibid.*, p. 112
[255] *Ibid.*, p. 237
[256] *Ibid.*, p. 239-240
[257] *Ibid.*, p. 130
[258] *Ibid.*, p. 115
[259] *Ibid.*, p. 116

Autrement dit, l'exemple donné par Iacub en matière de mœurs et de sexualité montre bien que non seulement l'usage mais jusqu'à l'agencement intérieur du lieu de résidence, du logis, doit être considéré sous l'angle juridique.

Le domicile au sens légal : une notion productive, mais insuffisante

Comme pour la protection de la vie privée, la réflexion juridique sur la privacité du domicile est très riche. Pour autant, on ne peut s'arrêter à la conception juridique pour traiter de la privacité du domicile, ni d'ailleurs pour traiter du domicile ou du logis tout court. Il suffit de rappeler que, dans le droit, le domicile est aussi et, sans doute, avant tout, une notion pragmatique. Pour le droit civil, Gravelais rappelle que le domicile sert d'abord à « déterminer la compétence territoriale des juridictions et le lieu d'accomplissement de certains actes juridiques »[260]. Le droit pénal s'intéresse plus directement au domicile comme lieu privilégié d'habitation : il est d'ailleurs patent que l'un des principaux critères déterminant la caractérisation d'un lieu comme domiciliaire soit « l'exigence d'une occupation effective et non d'un titre juridique [de location, de propriété, etc.] »[261]. Si le droit pénal est, d'une certaine manière plus ambitieux, et vise explicitement à garantir, à travers le domicile dûment identifié, les libertés individuelles, et notamment à prémunir les personnes contre l'arbitraire, il ne dit pas grand-chose d'autre de cette liberté ou de la vie privée qu'il contribue à protéger – et c'est sans doute heureux : il est difficile de ne pas voir comme un progrès la fin de l'immixtion de l'État dans l'espace domestique à travers la régulation des mœurs décrite par Iacub.

Ce flou se retrouve par exemple dans la distinction faite par E4 entre l'espace public et l'espace privé :

> « E4: Non mais c'est vrai que tu te dis que quand t'es à ton domicile, ben voilà, en principe t'es pas observé, pas écouté, et là c'est vraiment dans un cadre, voilà ! Alors que dès que tu mets un pied dehors, ben tout le monde t'observe, tu... enfin... » (entretien 1, 1 h 06 min)

Elle explique sa compréhension de ce qu'est la privacité du domicile : un lieu où « un cadre », sous-entendu légal ou réglementaire, prévient « en principe » l'immixtion d'yeux et d'oreilles tiers, contrairement à l'espace public (« dans la rue ») où elle conçoit parfaitement que cette observation soit possible. L'intérêt de cette remarque reste de montrer que cette enquêtée sent

[260] Notamment « le mariage ou l'adoption », « les significations d'actes de procédure » (l'adressage du courrier, en somme) ou de déterminer « le lieu d'exécution du paiement des dettes ». Voir I. GRAVELAIS, *La protection juridictionnelle de l'inviolabilité du domicile*, *op. cit.*, p. 31
[261] *Ibid.*, p. 45

que ses pratiques et son intimité sont protégées chez elle par la loi, qui conforte le fait que son domicile soit une forme de cocon protecteur (voir « Le logis comme cocon », p. 111).

*

Après avoir exploré la dimension légale de la protection de la vie privée au domicile, il nous faut donc maintenant revenir à ce qui fonde le domicile comme un espace social de pratiques particulières, et questionner ce qu'est le logis contemporain dans une approche plus anthropologique.

II - LE LOGIS COMME COCON

On l'a vu, tant l'histoire (« Évolution des contours de la notion de vie privée », p. 50) que le droit (« *A man's home is his castle* : aspects juridiques », p. 106) montrent la variabilité de la notion de domicile selon les époques et les sociétés, quand bien même le logis reste une constante anthropologique partout observée. Au-delà de la caractérisation juridique du domicile comme espace privé, qu'est-ce qui fait du logis contemporain un espace singulièrement privé pour ses habitants ? Qu'est-ce que cette « vie privée » s'épanouissant spécifiquement dans l'espace domestique, et qui a justifié que le droit estime nécessaire d'étayer dans le registre idéel les murs du logis ?

Du logis à la maison

Le logis est d'abord un lieu propre à la vie de la famille. En France, c'est dès le XIXe siècle et surtout au XIXe siècle que la norme jusqu'ici bourgeoise de la maison ou de l'appartement comme lieu clos et privé commence se diffuser au reste de la société française, après avoir longtemps été un lieu plus ouvert sur l'extérieur, et souvent d'ailleurs un lieu de travail, non seulement à la campagne, mais même en ville[262]. Cette évolution de la conception de l'espace domestique accompagne l'évolution déjà entamée des rapports familiaux. Dans *Les tyrannies de l'intimité*, Richard Sennett date du XVIIIe l'époque où la famille est de moins en moins conçue dans une logique patrimoniale, de protection réciproque ou de communauté de production économique : « La famille devient un refuge. On la considéra de moins en moins comme le centre d'un domaine particulier, non public, pour voir en elle un abri, un monde en soi, aux valeurs morales plus élevées que celles du domaine public. La vie de famille fut

[262] A. PROST, « Frontières et espaces du privé », dans G. Duby et P. Ariès (éd.), *Histoire de la vie privée - Tome 5 - De la première guerre mondiale à nos jours*, Paris (France), Seuil, 1987

idéalisée comme une vie dans laquelle l'ordre et l'autorité demeuraient incontestés, dans laquelle la sécurité de l'existence matérielle pouvait s'accompagner d'un véritable amour conjugal et dans laquelle, enfin, les relations entre les différents membres ne toléraient aucune ingérence extérieure »[263]. À cette opposition de plus en plus marquée de la distinction entre la vie de famille et la vie publique ou encore la vie professionnelle s'ajoute donc le renforcement d'une dimension affective : le logis devient le lieu de l'épanouissement des relations interindividuelles au sein de la famille ; et en cela il devient une maison au sens plein[264]. Dans *Habiter – Un monde à mon* image, Jean-Marc Besse abonde dans la définition primordiale de la « maison » autour de valeurs morales, de pratiques, et de relations sociales : « La maison est un concept qui permet de penser l'unité dans le temps et dans l'espace d'un ensemble d'activités très diverses, à la fois sur le plan technique (bâtir sans doute, mais aussi entretenir, réparer, cultiver, conserver, réemployer, etc.) et sur le plan humain (vivre avec les autres, avoir des repas en commun, dormir, mais aussi faire couple et le défaire, avoir des enfants et les élever, leur transmettre un langage, une culture, des valeurs, mourir, etc.) »[265]. Dans ce contexte, Besse insiste sur le fait que l'architecture ne doit pas être première dans la conception de la maison comme un des lieux privilégiés de l'habiter, quoique la maison soit un concept fondamental pour l'architecture elle-même – en particulier, l'opposition de la maison-pavillon avec la maison-appartement n'aura de sens pour nous qu'à la marge d'éventuelles différences de pratiques habitantes dans la suite du texte. Il ne s'agit pas ici de nier l'importance de la matérialité territoriale de l'espace de la maison. L'amélioration des conditions de vie s'accompagne par exemple de la possibilité croissante de diviser un espace domestique plus vaste en plusieurs sous-espaces, là encore selon le modèle bourgeois : certains espaces sont hybrides, plus ouverts sur l'extérieur (le salon, la salle à manger, où l'on reçoit plus facilement des visiteurs), d'autres sont dévolus à la vie familiale nucléaire, voire à la vie individuelle (la chambre, surtout quand elle est celle d'un individu ou d'un couple, étant le type d'espace le plus privé).

[263] R. SENNETT, *Les tyrannies de l'intimité*, *op. cit.*, p. 29 Cité par B. REY, *La vie privée à l'ère du numérique*, *op. cit.*, p. 29

[264] Dans le vocabulaire européen antique puis médiéval, la maison désigne d'ailleurs d'abord la famille, généralement noble, plus que son palais ou son château, et le lieu de rattachement de la lignée s'il est évidemment d'importance, est secondaire. On trouve aujourd'hui encore des manifestations de cette culture de maison par exemple au pays basque, où la famille gravite autour de l'*etxe* ; voir S. BRETOU, *De la mythologie basque à une construction identitaire militante : éthique de l'engagement au prisme de l'imaginaire collectif*, thèse de doctorat en sociologie, Montpellier (France), Montpellier 3, 2009

[265] J.-M. BESSE, *Habiter: un monde à mon image*, Paris (France), Flammarion, 2013, p. 8

COCON, n. m.

XVIIe siècle. Emprunté du provençal coucoun, « coque (d'un œuf) » et « cocon », dérivé de coco, « coque, coquille », du latin coccum.

☆1. ZOOL. Enveloppe soyeuse filée par de nombreuses larves de lépidoptères, et dans laquelle s'opère leur dernière mue. • Spécialt. Enveloppe qui renferme le ver à soie quand il a achevé de filer, et qu'on dévide pour obtenir la soie. Recueillir, trier les cocons. • Par anal. Petit sac soyeux dont les araignées enveloppent leurs œufs.

☆2. Fig. Milieu douillet où l'on est protégé des réalités, des difficultés de la vie. Vivre dans un cocon. Se retirer dans son cocon. Un enfant élevé dans un cocon.[266]

La thématique du logis comme un « cocon » me semble parfaitement résumer le point contemporain où nous ont menés le recentrage du logis autour de la vie privée et familiale, l'investissement émotionnel dans cet espace, et son aménagement toujours plus fin dans une logique décrite par Jean-Claude Kaufmann comme celle d'un « repli domestique »[267]. La définition du terme cocon par la 9e édition du *Dictionnaire de l'Académie* (voir ci-dessus) décrit bien la maison contemporaine : elle est à la fois le logis où l'on restaure ses forces (sens 1) et le lieu où s'épanouit « [douillettement] » la vie individuelle et familiale, où « l'on se retire », où l'on protège, éventuellement trop, un enfant (sens 2). Cocon a d'ailleurs donné l'anglicisme *cocooning* qui désigne la pratique de « (…) recherche de confort et de sécurité chez soi qui traduit le besoin de se protéger contre les réalités, perçues comme dures et imprévisibles, du monde extérieur » selon la psychosociologue Perla Serfaty-Garzon[268]. Serfaty-Garzon distingue *cocooning* et nidification, le premier terme impliquant selon elle une notion de défense contre l'extérieur qui n'est pas présente dans le deuxième. Si cette précision n'est pas sans intérêt ni justification (« cocon » aurait selon elle une étymologie militaire), je ne suis pas sûr que l'usage distingue réellement entre ces deux sens. Du reste, Serfaty-Garzon rappelle elle-

[266] « Cocon », dans *Dictionnaire de l'Académie française*, Paris (France), Centre national de ressources textuelles et lexicales, s. d. (en ligne : https://www.cnrtl.fr/definition/academie9/cocon)
[267] J.-C. KAUFMANN, *La chaleur du foyer. Analyse du repli domestique*, Paris (France), Klincksieck, 1988
[268] P. SERFATY-GARZON, « Cocooning », dans M. Segaud, J. Brun et J.-C. Driant (éd.), *Dictionnaire critique de l'habitat et du logement*, Paris (France), Armand Colin, 2003, p. 74-75 (en ligne : http://perlaserfaty.net/wp-content/uploads/2017/01/Cocooning-un-texte-de-Perla-Serfaty-Garzon.pdf)

même que l'émergence de cette thématique et le renforcement des pratiques associées dans les années 1980 résultent également d'un effort conscient du milieu du *marketing* : « Le terme *cocooning* vient des milieux du *marketing*. Forgé pour vendre les capacités marchandes et celles à « prévoir les tendances sociales » de spécialistes du marketing auprès de grandes compagnies productrices de biens de consommation, il saisit certes avec justesse un versant de l'intimité, celui de la tentation du repli domestique. Il a aussi pour vertu de rappeler que l'idéal du chez-soi entretient des liens intimes avec les comportements de consommation et d'acquisition de marchandises. »[269]. Si le terme *cocooning* a longtemps prévalu, le *marketing* a depuis poussé d'autres termes connexes, comme la notion danoise de *hygge* qui a eu un certain succès en 2016 et en 2017[270]. Au bout du compte, les différences terminologiques fines dans le domaine ne semblent pas refléter une réelle diversité sémantique. Elles reflètent dans tous les cas une tendance au repli sur l'espace domestique encouragée de longue date par le *marketing*, comme le montrait déjà Jean-François Staszak dans les premières lignes de son article « L'espace domestique : pour une géographie de l'intérieur » évoquant une publicité de 2000 pour la marque de meubles Roche-Bobois dont le slogan était « la vraie vie commence à l'intérieur ».[271]

Cette notion de cocon est spontanément évoquée par deux enquêtés. E20 explique ainsi qu'elle est devenue incapable de faire les boutiques, même pour une simple robe. Bien qu'elle ait 52 ans, elle est désormais habituée à commander sur Internet, et décrit une peur très forte de faire le mauvais achat dans une boutique physique, dans le sens où il pourrait toujours y avoir mieux ou moins cher ailleurs. Au moment, plus tard dans l'entretien, où elle décrit le processus de choix de l'enceinte qu'elle a acheté (une Amazon Echo), elle rapporte d'ailleurs avoir comparé des tests et pris des renseignements sur les enceintes connectées une semaine durant, essentiellement sur Internet. Cette anxiété éprouvée en magasin semble presque incapacitante pour elle, et ce n'est que dans le confort de son salon et sur Internet qu'elle effectue désormais la quasi-totalité de ses achats :

> « (…) Et donc je suis beaucoup plus à l'aise en ligne. Parce qu'en ligne, tu vois pas tout, et puis... tu es réconforté, t'es dans ton salon, dans ton cocon, dans ton endroit qui est à toi. Et donc je suis plus à l'aise, et là j'achète n'importe quoi, j'achète bien, j'achète même des trucs dont j'ai pas besoin, parce qu'Amazon CREE ce besoin. » (entretien 13 ; 13 min)

[269] *Id.*
[270] C. ARCE, « 5 tendances cocooning aussi cool que le hygge », *Le Huffington Post*, 11 février 2017 (en ligne : https://www.huffingtonpost.fr/2017/02/11/5-tendances-cocooning-aussi-cool-que-le-hygge_a_21659274/ ; consulté le 21 septembre 2021)
[271] J.-F. STASZAK, « L'espace domestique », *op. cit.*

Le dégoût qu'elle narre à se rendre en magasin fait un contraste étonnant avec le sentiment de liberté qu'elle éprouve dans le « cocon » de son salon, « [son] endroit [à elle] », qui la « [réconforte] ». Elle semble d'ailleurs avoir conscience de la force de cette opposition, puisqu'elle explique même pouvoir acheter « n'importe quoi » sur Amazon, y compris des choses inutiles : là où la difficulté à comparer les catalogues de boutiques physiques explique selon elle sa difficulté à y acheter des objets par crainte de la mauvaise affaire, l'achat sur Internet à domicile la met à l'aise au point qu'elle reconnaît simplement l'inutilité de certains des achats qu'elle fait alors – quand bien même elle reconnaît aussi la force de séduction de la force de vente d'Amazon.

E16 utilise lui aussi le mot cocon spontanément lorsque nous évoquons les dispositifs domotiques qui lui permettraient d'augmenter encore son espace domestique :

> « E16: Tu veux dire que je fasse confiance à une technologie... le fait de pouvoir fermer, contrôler, mon cocon, mon chez-moi, heu, mon petit, mon petit brin de liberté où je peux faire pousser (rapport à la conversation sur Linky et les producteurs de cannabis, je pouffe) .» (entretien 10 ; 46 min 55 s)

Le vocabulaire utilisé pour décrire son espace domestique est très possessif (« mon » répété quatre fois), intimiste (le « chez-moi », le « cocon ») et mélioratif (« brin de liberté »). L'évocation de la possibilité d'y faire pousser du cannabis est une boutade relative à une séquence plus tôt dans l'entretien où ont été évoqués les compteurs Linky, mais elle fait écho à la notion de liberté qu'il évoque, à savoir la liberté y compris de pratiques culturales illégales – Linky restreignant encore la possibilité de faire pousser du cannabis sous lampe sans être trahi par sa consommation électrique. Comment souvent avec E16, il rappelle que son handicap moteur explique aussi son attachement à cet espace de liberté qu'est pour lui son domicile, où il peut minimiser les contraintes de sa vie quotidienne et donc maximiser le temps non contraint qu'il peut consacrer à des activités autres que la gestion de son corps. Quand je lui propose de me donner sa définition de la vie privée une dizaine de minutes plus tard, il revient là encore sur la notion de cocon avec ce vocabulaire très mélioratif :

> « E16: C'est partager certains endroits, avec certaines personnes, pas forcément une information. Mais... on va avoir un bar préféré avec, heu, des amis, moi j'ai maintenant mon petit chez moi, qui me permet qu'on puisse discuter, même pour inviter des gens, etc., chose que je n'avais pas avant. J'étais dans une chambre, chez mon père, et j'avais pas ce côté... petit cocon, pour moi.
> JF: (acquiesce)
> E16: J'étais, entre guillemets, en mode survie, dans une chambre, pendant deux

ans... J'avais PAS ce lieu. Donc l'information, mais aussi ce lieu privé, cette intimité, par le cocon, heu...»
(entretien 10 ; 58 min 10 s)

Trois autres enquêtés réagissent positivement au terme cocon quand je l'évoque moi-même pour prolonger leur propos, à l'instar d'E18 et E19 :

« JF: ...mais finalement non. C'est-à-dire qu'il y a des gens qui ont... qui ont besoin d'être chez eux bien dans leur cocon, qui ont besoin de solitude, en fait.
E19: Oui oui oui oui !
E18: Ouais.
E19: D'un certain isolement, ouais.»
(entretien 12, 1 h 10 min)

Sans avoir eux-mêmes employé le terme spontanément, ils souscrivent sans problème à l'idée, qu'E19 prolonge même par l'idée que le chez-soi permet un certain isolement individuel.

Finalement, seul un enquêté, E17, réagit négativement à mon évocation directe du terme cocon appliqué à son espace domestique :

« E17: Enfin, je vois pas la différence... J'aimerais pas qu'on me filme pendant que je dors ou pendant que je me lave, mais bon, je vais pas faire un selfie de moi dans la salle de bain, à poil ou des trucs comme ça, non. Voilà.
JF: Après, oui, de temps en temps... Ça peut être des trucs comme s'habiller plus confortablement chez soi, des trucs comme ça ?
E17: Oui, avoir la paix, mais la paix je peux l'avoir dans des bibliothèques et tout ça.
JF: Oui, vous n'avez pas de... fétichisme du chez-soi comme un cocon, ou des choses comme ça ?
E17: Non, heu...
JF: Enfin, fétichisme...
E17: Non, c'est juste pour dormir, ou pour travailler au calme, mais il peut y avoir d'autres endroits. Oui, si, il y a mes documents, ma documentation. »
(entretien 11 ; 2 h 40 min)

La suggestion ne lui convient manifestement pas du tout, de près ou de loin : son appartement n'est pas un cocon, et il marque étonnamment peu (voire pas) la différence entre l'espace public et l'espace privé. Il résume son appartement au logis le plus élémentaire, réduit à sa fonction de lieu de sommeil ou d'hygiène. Ancien journaliste, il concède à la rigueur que la présence de sa « documentation » est ce qui spécifie le plus son appartement comme étant le sien. Il affirme pouvoir se sentir « en paix » dans une bibliothèque aussi bien que chez lui, ce qui laisse entendre que son logis n'est pas un lieu plus protecteur ou reposant qu'un autre. Il faut préciser ici qu'E17 est un cas singulier parmi les enquêtés. Au premier degré, on pourrait croire qu'il est

simplement très à l'aise dans les lieux publics, ou qu'il affecte le détachement par rapport aux contingences ou aux attachements matériels. En réalité, deux éléments expliquent ce rapport singulier à l'espace domestique, par ailleurs unique dans mon matériel d'enquête. D'une part, comme ancien journaliste, il est habitué à travailler de chez lui et sans compter ses heures, les sphères privée et professionnelle ont longtemps été confondues pour lui. D'autre part, il n'est pas tant à l'aise dans l'espace public comme il l'est dans son espace privé qu'il n'est autant sur ses gardes chez lui qu'il l'est dans l'espace public. Un élément traumatique de son histoire familiale l'explique, qu'il me livre au bout de deux heures d'entretien : ses parents ont fui une dictature d'Europe centrale, dans laquelle une partie de sa famille a continué de vivre. Aussi, et depuis son plus jeune âge, lui était-il intimé de faire très attention à ce qu'il pouvait dire au téléphone, présenté comme toujours sous écoute potentielle. En somme, et malgré le passage du temps, E17 estime nécessaire de garder un masque dans presque toutes les circonstances, et ce jusque dans l'intimité familiale – ce qui explique également sa réticence à l'utilisation d'une enceinte connectée.

Pour finir cette évocation du rapport au logis comme cocon au cours des entretiens, précisons que d'autres enquêtés s'inscrivent quant à eux dans la description possessive de leur appartement, sans forcément évoquer le terme de cocon, comme c'est le cas d'E7 :

> « E7: Après c'est juste le côté un peu moral (sur un air d'énumération d'évidences) , c'est quand même dans MA maison, heu...
> E6: Oui !
> E7: C'est l'endroit où je suis censé être chez moi. Et il y a un truc qui m'écoute et qui m'observe.
> E6: Après c'est un peu consenti parce que...
> E7: (l'interrompant) Oui on a consenti, on l'a acheté, on l'a branché, bien sûr ! » (entretien 3 ; 30 min 30 s)

Ce dernier exemple n'est pas choisi au hasard : E7 souscrit à la conception du logis comme un cocon (« c'est quand même dans MA maison »), insiste vocalement sur le possessif « ma », et parle de « maison » pour décrire son appartement – dans lequel elle est une locataire récente. Son attachement à la figure de l'espace domestique comme étant un lieu éminemment personnel est criant. Pour autant, cette affirmation d'un rapport très territorial[272] à son domicile est faite précisément en réaction à l'évocation d'une possible transgression de l'immunité de ce territoire par un dispositif, l'enceinte connectée, qui contribue à la porosité de la frontière entre son

[272] Le territoire étant ici à lire dans l'un de ses sens les plus classiques en géographie, à savoir un espace circonscrit approprié par un individu ou un groupe.

espace domestique et l'extérieur. La tension est ici manifeste dans la contradiction entre ce discours territorial affirmé et la possession effective d'un objet dont elle a accepté (« Oui on a consenti, on l'a acheté, on l'a branché, bien sûr ! ») qu'il vienne concurrencer son appropriation de son espace domestique. Il faut préciser que cette tension est interne à E7, qui n'aurait probablement pas acquis seule une enceinte connectée, mais n'a pas opposé de véto à l'achat de ce qu'E6 considère lui-même comme un « gadget », et qu'elle utilise par ailleurs volontiers.

*

Comme nous l'avons vu jusqu'ici, la définition de la vie privée pose de redoutables problèmes de définition, *a fortiori* à l'ère numérique, et plus encore dans la mesure où la littérature liant ces sujets fait très peu explicitement cas des questions d'espace et de spatialités – pourtant jugées fondamentales par les auteurs de l'*Histoire de la vie privée* sur les deux millénaires précédant l'émergence des technologies numériques. Malgré l'intérêt d'approches sectorielles, en particulier sociologiques ou juridiques, pour comprendre les liens entre vie privée et technologies numériques, il nous manque à ce stade un recul suffisant pour identifier des transversalités fortes qui nous permettraient de saisir spatialement la vie privée à l'ère numérique. À travers sa métaphore des bulles et de l'écume du social, Peter Sloterdijk me semble fournir l'outillage mental adéquat à une compréhension plus englobante et spatialisée de la vie privée contemporaine comme un mécanisme immunitaire d'individus pris dans des relations et des espaces aussi complexes que changeants et multiscalaires.

Chapitre 4 - BULLES ET ECUMES DU PRIVE

I - LA « SPHEROLOGIE » DE PETER SLOTERDIJK

Le philosophe allemand Peter Sloterdijk propose une grille de lecture particulièrement stimulante pour penser spatialement les notions d'intimité et de privé à l'ère numérique à travers sa sphérologie et la métaphore des écumes.

Dans le premier tome de sa trilogie *Sphères* publiée entre 1998 et 2004, Sloterdijk s'intéresse aux « microsphères » de l'expérience humaine, à savoir un « système immunitaire de l'espace psychique »[273] que les individus constituent *in utero* par l'expérience du son, du toucher et des émotions. Sloterdijk prend notamment le contre-pied de Lacan, pour qui la conscience individuelle se forme au « stade du miroir », quand le nourrisson découvre l'unicité de son être dans le reflet que lui renvoie le miroir[274]. La bulle définit un intérieur et un extérieur, dont elle constitue une limite poreuse, et nécessairement « dyadique » : elle naît d'abord dans la relation utérine du couple mère-enfant, prolongée ultérieurement dans la relation à autrui et au monde, qui sont autant d'autres « sphères »[275]. La théorie du social de Sloterdijk consiste à interroger la coexistence, l'imbrication et l'interaction entre la multiplicité des sphères dans lesquelles évoluent les êtres, et qu'il nomme « sphérologie » : « L'idée que la vie est une affaire de forme - voilà ce que nous associons à la vieille et respectable expression de *sphère*, empruntée aux philosophes et aux géomètres. Elle suggère que la vie, la constitution de sphère et la pensée sont des expressions différentes pour désigner une seule et même chose. Dans cette mesure, la référence à une géométrie sphérique vitale n'a de sens que si l'on admet l'existence d'une sorte de théorie qui en sait plus sur la vie que la vie elle-même - et que partout où l'on trouve de la vie humaine, qu'elle soit nomade ou sédentaire, naissent des globes habités, itinérants ou fixes (…) »[276]. Sloterdijk poursuit une quinzaine de pages plus loin en affirmant qu'« (…) habiter signifie toujours constituer des sphères, en petit comme en grand, [et que] les hommes sont les créatures qui établissent des mondes circulaires et regardent toujours vers

[273] P. SLOTERDIJK, *Écumes - Sphérologie plurielle*, O. Mannoni (trad.), Paris (France), Hachette Littératures, 2006, p. 9
[274] P. SLOTERDIJK, *Bulles*, *op. cit.*, chap. Digression IX
[275] Bien que la filiation avec Leibniz soit assumée chez Sloterdijk, la bulle n'est pas tout à fait ou pas uniquement une monade. « La théorie de l'écume, elle ne s'en cache pas, a indiscutablement une orientation néomonadologique: mais ses monades ont la forme fondamentale de dyades ou de structures plus complexes, relevant de l'espace spirituel, de la paroisse et de l'équipe. » P. SLOTERDIJK, *Écumes*, *op. cit.*, p. 53
[276] P. SLOTERDIJK, *Bulles*, *op. cit.*, p. 13

l'extérieur, vers l'horizon »[277]. Il établit donc le point de vue, le regard individuel comme la base de sa pensée du social, ce qui est, pour ainsi dire, géométriquement cohérent avec une approche de la vie privée partant de la mise en tension de problématiques fondamentalement individuelles – quoique leur agrégation ne soit pas sans effet collectif, comme le signale Daniel Solove[278]. Sloterdijk poursuit d'ailleurs immédiatement en expliquant qu'une telle sphère est un construit qui ne résume pas l'identité individuelle, et qui n'est pas plus fermée sur elle-même qu'elle ne tire son principe exclusivement d'elle-même : « Vivre dans des sphères, cela signifie produire de la dimension dans laquelle les hommes peuvent être contenus. Les sphères sont des créations d'espaces dotés d'un effet immuno-systémique pour des créatures extatiques travaillées par l'extérieur »[279].

En première hypothèse, on pourrait ramener la pensée sphérologique de Sloterdijk à celle des « coquilles » de la *Psychosociologie de l'espace* d'Abraham Moles et d'Elisabeth Rohmer[280]. Cela plus particulièrement en ce qui touche à des questions de limites et d'échelles liées à la vie (pas seulement privée) de l'individu, dans l'approche plus phénoménologique ou égo-centrée que ces deux auteurs proposent. Les trois premières coquilles, qui vont de l'échelle du corps à celle de la pièce puis du logis couvrent l'essentiel des types spatiaux étudiés dans cette thèse. Pour autant, la pensée de Sloterdijk dépasse largement ce premier cadre scalaire et phénoménologique. Selon Lussault, « Sloterdijk pose les fondements d'une véritable philosophie de l'espace – très au-delà de la conception statique classique – systémique, relativiste et hyper-relationnelle.[281] » Cette philosophie de l'espace permet notamment la prise en compte d'interspatialités devenues beaucoup plus variées et d'interactions multi-acteurs devenues infiniment plus complexes à l'ère numérique.

Filant la métaphore de la bulle, Sloterdijk propose dans le dernier ouvrage de sa trilogie d'envisager la société et ses espaces comme une « écume ». Cette écume est composée d'une grande variété de bulles, caractérisées par le volume d'air qu'elles enclosent et par leur paroi, tenant en un fragile équilibre entre leur pression interne et leur tension de surface. Un aspect important de la pensée de l'écume est en effet que toute sphère partage sa paroi avec une ou plusieurs autres sphères. Les bulles vivent, croissent, éclatent, et leur éclatement leur fait partager leur volume d'air avec leurs voisines, qui à leur tour grandissent ou éclatent selon les

[277] *Ibid.*, p. 30
[278] D. J. SOLOVE, *« I've Got Nothing to Hide » and Other Misunderstandings of Privacy*, *op. cit.*
[279] P. SLOTERDIJK, *Bulles*, *op. cit.*, p. 30
[280] A. A. MOLES et E. ROHMER-MOLES, *Psychosociologie de l'espace*, *op. cit.*
[281] M. LUSSAULT, *L'homme spatial: la construction sociale de l'espace humain*, Paris (France), Seuil, 2007, p. 37

forces de tension de surface qui les maintiennent plus ou moins longtemps, et plus ou moins indépendantes. Cet aspect de la métaphore est important en cela qu'il explique ou rend possible l'historicité de l'écume, et qu'il éclaire sur ses évolutions. Ce sont ainsi les bulles les plus anciennes qui sont les plus vastes, ou encore celles qui se sont nourries de l'éclatement du plus grand nombre de bulles en elles-mêmes. Dans cette logique, d'un grand nombre de microsphères individuelles éclosent ainsi des macrosphères très englobantes, constituant par exemple des cultures voire des civilisations.

Dans cette perspective fondamentalement relationnelle d'un espace privé d'un centre et donc d'un référentiel de spatialisation absolus, le parallèle semble tout à fait pertinent avec l'opposition entre la topographie et la topologie, ou plus exactement entre « les agencements topographiques du réel [qui] ne sont que des généralisations topologiques, qui consistent en l'appréhension de l'ensemble des relations coexistentielles qui prévalent pour un ensemble d'éléments considérés », selon Beaude et Nova[282]. Ils poursuivent : « Aussi, l'illusion topographique tiendrait essentiellement à la stabilité relative des relations entre les entités considérées. Une place, un immeuble, une rue et plus encore une ville ne sont, in fine, que des agencements relativement stables d'entités dont le mouvement relatif est tellement négligeable que l'on s'autorise à ne plus le penser d'un point de vue relationnel. »[283] Dans la terminologie de Sloterdijk, cette plus ou moins grande stabilité des agencements sociaux est rendue par l'opposition entre « l'écume » et « la mousse », qui diffèrent au sens physique par leur niveau de stabilité tout en n'étant pas fondamentalement différentes : la mousse est une forme stabilisée de l'écume, qui n'en conserve pas moins un minimum de malléabilité. De ce point de vue, la mousse serait peu ou prou à l'écume ce que la topographie est à la topologie, et la métaphore de Sloterdijk présente l'intérêt de nous prémunir mentalement de l'exacerbation de l'opposition entre topographie et topologie.

Malgré tout, ce dernier parallèle reste encore insuffisant si l'on veut, pour ainsi dire, importer la pensée de Sloterdijk dans le champ géographique : il lui manque une pensée de l'acteur et de l'action spatiale ou, autrement dit , « il lui manque d'insister sur un point pour être complètement pertinent[e] (…) : le versant pragmatique. »[284]

[282] B. BEAUDE et N. NOVA, « Topographies réticulaires », *Réseaux*, nº 195, 24 mars 2016, p. 56 (en ligne : http://www.cairn.info/resume.php?ID_ARTICLE=RES_195_0053 ; consulté le 22 septembre 2016)
[283] *Id.*
[284] M. LUSSAULT, *L'homme spatial*, *op. cit.*, p. 37

II - SPATIALITES DE L'ECUME

La sphérologie de Sloterdijk n'est pas figée : elle questionne même, justement et au contraire, les conséquences pour l'humanité de la fin des grands modèles cosmologiques figés tels que le géocentrisme d'un Claude Ptolémée. Que cette fin soit intellectuellement actée ne signifie pas pour autant que les schémas mentaux associés se soient évanouis. Pour Sloterdijk, même la Modernité conserve un projet sphérologique, elle cherche à recréer des sphères, le sentiment d'être, pour ainsi dire, *contenus* ou immunisés, après la perte de l'illusion cosmologique antérieure : « Au gel cosmique qui pénètre dans la sphère humaine par les fenêtres grandes ouvertes des Lumières, l'humanité des temps modernes oppose un effet de serre volontaire : elle entreprend une manœuvre pour compenser par un monde artificiel et civilisé son absence d'enveloppe dans l'espace, due à la cassure des vases célestes »[285]. La sphérologie est donc aujourd'hui moins une description statique du monde qu'une activité fondamentale, et qui fournit le canevas de l'habitation du monde pour les Modernes. Le terme d'habitation du monde est à prendre en un sens très large, puisqu'elle inclut selon l'auteur des projets comme la mondialisation commerciale ou l'État-providence en cela qu'ils visent à restaurer notre immunité primordiale. Sloterdijk poursuit à la page suivante en incluant explicitement les pratiques numériques dans ce même mouvement de fond, en dépit de leur intangibilité : « Avec une peau médiatique électronique, le corps de l'humanité veut se créer une nouvelle constitution immunitaire »[286].

Si Sloterdijk tend à partir de la cosmologie antérieure pour justifier les formes modernes de l'habitation du monde, et donc du résultat recherché pour expliquer l'action qui y mène, Lussault insiste davantage sur le primat de l'action elle-même dans la construction des espaces, qui résultent des spatialités au moins autant qu'ils les conditionnent : « (…) en sus de ce que les intuitions de Sloterdijk révèlent, j'écrirais que l'espace est (en) action(s), car il manifeste (…) l'indispensable et inlassable activité des êtres humains avec la distance et les places. Sloterdijk se focalise dans son travail sur l'organisation de l'espace, ce qui est nécessaire, mais pas assez sur celle de la spatialité, c'est-à-dire l'action spatiale des opérateurs sociaux. »[287]. Il nous faut donc reprendre la sphérologie et la métaphore de l'écume en enrichissant cette dernière du « pan pragmatique » des spatialités, qui permet d'appréhender finement les phénomènes spatiaux à l'œuvre à l'échelle micro du domicile, et ce, en interspatialité avec des

[285] P. SLOTERDIJK, *Bulles*, *op. cit.*, p. 27
[286] *Ibid.*, p. 28
[287] M. LUSSAULT, *L'homme spatial*, *op. cit.*, p. 37

phénomènes d'échelle beaucoup plus large et de métrique topologique. Cela permet d'aller au bout d'une réflexion géographique envisageant les « (…) les espaces, ces arrangements de matières et d'idées, [comme] les réponses apportées par les individus et les groupes pour satisfaire aux différentes exigences des innombrables (inter)spatialités des opérateurs sociaux. Ces réponses se sédimentent avec le temps et forment des espaces organisés, structurés, qui s'enrichissent de chaque acte nouveau et qui proposent des substrats aux spatialités à venir »[288]. Dans la terminologie de Sloterdijk, il faudrait en somme envisager ce qui fait écumer les sphères, et se garder de ne considérer que la mousse qui parfois en résulte.

Dans cette perspective, j'étendrais la métaphore de l'écume aux actes et non seulement aux individus et aux espaces qu'ils construisent et dans lesquels ils évoluent. Ces actes constituent autant de microsphères extrêmement fragiles, fugaces, qui n'en ont pas moins d'effet sur les sphères au sein desquelles d'autres actes seront effectués, et qui contribuent donc à l'agencement du monde. C'est ce que propose sur un mode mineur Sloterdijk lui-même dans l'introduction de son deuxième tome en parlant du souffle par lequel l'enfant forme des bulles par jeu, et qui me semble constituer une image de deuxième niveau intéressante pour intégrer l'action dans l'édifice métaphorique de l'auteur.

III - LA VIE PRIVEE CONTEMPORAINE COMME MECANISME IMMUNITAIRE

Si l'on s'appuie sur la pensée de Sloterdijk pour penser la question de la vie privée, alors on peut définir le privé comme la limite de l'extension de soi dans le monde, et la vie privée comme l'activité immunitaire qui consiste à gérer cette limite. En cela, la vie privée est un problème fondamentalement spatial, consubstantiel à l'habitation du monde. Je m'inscris en cela à la suite de Jean-Marc Besse, pour qui « Habiter (…), c'est fabriquer des sphères ou des cellules immunitaires (P. Sloterdijk), des bulle (A. Moles), des enveloppes (D. Anzieu), des milieux métaboliques à l'intérieur desquels les habitant façonnent leur intimité »[289]. Nous verrons dans la partie suivante selon quelles modalités spécifiques habiter le monde à l'ère numérique à travers le concept d'habitèle.

Bénédicte Rey partage cette conception du privée à partir d'autres références : elle cite Altman pour dire que le privé est la question du maintien d'une limite, en tension permanente :

[288] M. LUSSAULT, *L'avènement du Monde: essai sur l'habitation humaine de la Terre*, Paris (France), Seuil, 2013, p. 53
[289] J.-M. BESSE, *Habiter*, *op. cit.*, p. 55

« Une définition de ce qui relève du privé peut alors se concevoir non pas comme un ensemble d'éléments identifiables une fois pour toutes, mais plutôt comme un ensemble qui se définit par son contraire, par sa négation. C'est en cherchant à voir ce qui se joue lorsque les frontières du privé sont en question que l'on saura le mieux en identifier les contours mouvants. C'est en ce sens que nous approchons la question du privé moins comme un état que comme un processus de maintien d'une limite (Altman, 1977). Ce processus semble donc pouvoir être caractérisé au mieux en situation, lorsqu'il y a tension. »[290]

Si l'on reprend ici la métaphore de Sloterdijk comme grille de lecture, la vie privée consiste à gérer la « tension » de surface d'une des bulles d'écume dans laquelle nous habitons chacun de nos actes, tension qui résulte d'une forme de différentiel entre l'individu et son environnement. Cette acception du terme d'immunité correspond aussi à la définition donnée par Duby que nous avons cité plus longuement en exergue de la partie « La vie privée : une notion à historiciser », p. 50, et qui consiste à défendre la « part de l'existence que tous les langages disent privée, une zone d'immunité offerte au repli, à la retraite, où chacun peut abandonner les armes et les défenses dont il lui convient d'être muni lorsqu'il se risque dans l'espace public ».

Cette approche du privé comme une « zone » à l'intérieur de laquelle « les armes et les défenses » n'ont plus à être mises en œuvre par les individus laisse néanmoins entendre qu'elles sont nécessaires dans ou contre l'espace public, autrement dit pour nous en *bordure* de cette zone, à l'interface entre les espaces du privé et du public. Elle est également adoptée par le géographe Francisco Klauser, qui en fait une grille de lecture des espaces urbains contemporains de plus en plus surveillés. Il inclut ici notamment les communautés fermées (« *gated communities* »), les centres commerciaux, gares et aéroports, mais aussi dans une moindre mesure les domiciles[291]. Il propose de « conceptualiser les efforts sécuritaires contemporains non seulement comme des pratiques et techniques de surveillance et de séparation articulées par l'espace, mais aussi comme des forces générant des (atmo)sphères au sens plein ». Il assume cet emploi de la métaphore spatiale de la sphérologie en s'appuyant sur la pensée de Sloterdijk : « J'utilise ici le terme « (atmo)sphère » non dans un sens physique mais dans une acception

[290] B. REY, *La vie privée à l'ère du numérique*, *op. cit.*, p. 16

[291] F. KLAUSER, « Splintering Spheres of Security: Peter Sloterdijk and the Contemporary Fortress City », *Environment and Planning D: Society and Space*, vol. 28, nº 2, avril 2010, p. 332 (en ligne : http://journals.sagepub.com/doi/10.1068/d14608)

psychopolitique, à la manière de Sloterdijk »[292]. Si le concept d'(atmo)sphère de Klauser peut être utile pour penser l'espace domestique, il traite davantage de la question de la sécurité ou du sentiment de sécurité perçu dans un espace que de l'activité immunitaire spécifique à l'œuvre pour les habitants d'un espace privé domestique. La transposition n'est donc pas totale, et concerne avant tout la dimension « psychopolitique » de la production d'espace, que ce soit sous l'angle de l'immunité sécuritaire ou de l'immunité du privé. À une échelle plus fine (ou plus *écumante*) que ce que propose Klauser dans l'espace urbain, il est donc tout à fait pertinent d'investiguer les « micro-échelles » et les effets sur les « individus » de l'activité immunitaire dans la production de l'espace[293].

La montée en généralité pour ainsi dire anthropologique que nous avons appuyée sur la pensée de Sloterdijk présente un double intérêt, théorique et méthodologique. D'abord, elle permet de mesurer l'importance de la question de la vie privée, bien au-delà des nouvelles modalités de sa mise en tension à l'ère numérique, mais sans pour autant la fétichiser outre-mesure. Cela permet d'éviter toute « tentation panique »[294], comme le préconisent du reste Gary T. Marx et David Lyon, deux auteurs pourtant fondateurs des *surveillance studies*[295], de même que tout jugement technique trop détaché[296] sur la pertinence ou non des réactions souvent *épidermiques* des enquêtés quant à leur vie privée. Cette montée en généralité offre ensuite une grande souplesse et une grande finesse méthodologique, qui permettent de considérer tout l'éventail des espaces et des spatialités possibles de la vie privée à l'ère numérique. Elle nous évite notamment l'écueil de l'opposition simpliste entre espace privé et espace public, en nous invitant plutôt à des allers-retours dans la co-construction des espaces et des spatialités. Ainsi, bien que la question du logis soit évidemment centrale pour traiter d'objets, les enceintes et objets connectés, dont la vocation domotique est une dimension essentielle,

[292] « *to conceptualise contemporary security efforts not only as an ensemble of spatially articulated practices and techniques of surveillance and separation but also as (atmo)sphere-creating forces in their own right. I hereby use the term `(atmo)sphere' not in its physical sense but in its psychopolitical meaning, as developed by Sloterdijk* » (trad. pers.) *in Ibid.*, p. 327

[293] « *very few academics have provided detailed empirical accounts of the qualitative, microscale implications of these developments in terms of individual experiences of the city* » (trad. pers.) *in Ibid.*, p. 338

[294] O. Aïm, « Introduction », dans *Les théories de la surveillance - Du panoptique aux Surveillance Studies*, Paris (France), Armand Colin, 2020, § 6

[295] « Dès la fin des années 1990, David Lyon et Gary T. Marx prennent conscience de la tension en jeu : l'inflation des questions liées à la surveillance, d'une part, et la nécessité d'un cadre théorique solide pour l'analyser et la penser, d'autre part. Il ne s'agit pas d'invalider les approches précédentes. Mais il s'agit de faire rupture avec les modèles trop généraux auxquels elles ont donné lieu. « Le Panoptique et au-delà » (« *Panopticon and Beyond* ») : tel est le mot d'ordre que proclame, dès 2002 de manière emblématique, la revue qu'ils fondent sous le titre de *Surveillance & Society*. » *in Ibid.*, § 9

[296] En particulier, des réflexions sur l'effectivité ou non de la seule circulation des données personnelles, qui cristallise bien souvent les débats contemporains.

nous ne nous y enfermerons pas. Si le domicile relève davantage de la mousse que de l'écume, la sphérologie permet d'embrasser à la fois la stabilité et la subtilité mouvante des arrangements domestiques autour de la vie privée des individus dans leur habitat.

CONCLUSION PARTIELLE

> *« La nouvelle constellation est donc la suivante : le sérieux et le fragile, ou encore (pour installer le tournant des rapports de sérieux sur la pointe où il devra désormais se tenir) l'écume et la fécondité. L'aphrologie - du grec* aphros, *l'écume - est la théorie des systèmes affectés d'une co-fragilité. Si l'on parvenait à démontrer que ce qui relève de l'écume peut en même temps être ce qui porte l'avenir, qu'il est, dans certaines conditions, fertile et capable de procréer, on couperait l'herbe sous le pied du préjugé substantialiste. C'est précisément ce que l'on entreprend ci-dessous. Ce que l'on a rendu méprisable pendant une ère entière, l'apparemment frivole, ce qui n'existe qu'en allant vers son implosion, reconquerrait alors sa part dans la définition du réel. On le comprend alors : il faut reconnaître ce qui vole en suspension comme un élément fondateur d'une nature particulière ; le creux doit être décrit de nouveau comme une entité emplie fonctionnant selon ses propres lois; le fragile doit être pensé comme le lieu et le mode de ce qui est le plus réel. Il faut montrer que ce qui ne se répète pas est un phénomène plus élevé que le sériel. »*[297]

L'intérêt heuristique de Sloterdijk vient de ce que la subtilité de son approche et la fragilité des bulles et des sphères qu'il décrit permet une meilleure prise en compte de la grande variabilité conceptuelle et individuellement perçue et mise en œuvre d'une notion comme la vie privée. Il ne s'agit définitivement plus de souscrire à un « préjugé substantialiste » et encore moins métaphysique consistant à chercher un « plus petit dénominateur commun »[298], une essence au concept de vie privée, dépassement auquel nous invitait Daniel Solove. Il ne s'agit pas non plus seulement de déterminer des limites au privé, qu'elles soient informées par une norme légale, ou même par une norme « d'intégrité contextuelle » construite par chaque société. Il s'agit en fait de voir que le privé caractérise fondamentalement la « sphère » du soi dans le monde telle qu'elle est éprouvée, insufflée et négociée par les individus. De même, l'écumante fugacité de tout acte, la vacuité de ce qui le fonde, qui le souffle, ne doit nous pousser à minimiser ni sa réalité, ni sa propension à grandir et à faire grandir d'autres actes, matériels ou idéels, notamment dans l'agencement et l'arrangement des espaces. La métaphore de l'écume développée par Sloterdijk, partie de la constitution de l'espace humain, et étendue aux pratiques spatiales, nous permet de mieux penser les immunités individuelles et collectives, les fragiles

[297] P. SLOTERDIJK, *Écumes*, *op. cit.*, p. 34
[298] D. J. SOLOVE, *Understanding privacy*, *op. cit.*

limites du privé à l’ère numérique, ainsi que la logique immunitaire qui est ce qui est réellement mis en jeu quand sont exprimées des « tensions » liées à la vie privée.

Partie 2 - L'HABITELE, OU LA LOGIQUE IMMUNITAIRE DU PRIVE BOUSCULEE PAR LES NOUVELLES SPATIALITES NUMERIQUES

Si la sphérologie développée par Peter Sloterdijk éclaire notre *rapport* à l'espace et particulièrement à l'espace domestique, elle ne décrit pas à elle seule la *manière* dont nous habitons au quotidien ces espaces, et ce, plus particulièrement à l'ère numérique. Il faut donc désormais partir de l'idée que nous habitons autant les bulles d'espace que nous nous construisons que nous habitons nos actes et nos pratiques quotidiennes. Ces pratiques se trouvent être toujours plus médiées par le numérique, et il est donc inévitable que nous construisions désormais notre habitat à travers elles, voire pour elles (chapitre 1). Il peut paraître paradoxal que des êtres aussi soucieux de se constituer des sphères immunitaires contribuent par leurs pratiques à fragiliser l'immunité de cet habitat, danger qu'ils perçoivent pourtant déjà à travers le principal dispositif de rupture de l'ère numérique, le smartphone (chapitre 2). Les espaces domestiques, après avoir longtemps cristallisé l'activité immunitaire, sont désormais directement mis à l'épreuve de nouvelles médiations numériques à travers l'émergence des enceintes connectées et de la domotique – ou, *in fine*, de la *smart home* (chapitre 3).

Chapitre 1 - HABITER LE / AVEC LE NUMERIQUE

Avec l'émergence du concept d'habiter, nous avons paradoxalement assisté à un mouvement de sortie de la notion d'habitat hors du simple géotype du domicile : « La spatialité humaine consiste pour tout un chacun, à partir de l'utilisation de l'espace-ressource, à organiser un *habitat*. Ce mot ne renvoie pas, dans ce cadre d'analyse, au seul logement : la demeure fait partie de l'habitat, mais celui-ci ne s'y réduit pas. »[299] L'habitant nomade et/ou « poly-topique »[300] contemporain, pouvant s'appuyer notamment sur des prothèses numériques pour se repérer dans tout espace, voire pour faire sien presque tout lieu, est un personnage-type de cette tendance. Ce constat de la dissociation croissante entre l'habitat comme lieu, le domicile au premier chef, et l'habiter qui se joue désormais dans une diversité d'espaces beaucoup plus importante et de métrique topologique, crée néanmoins un hiatus conceptuel : comment les individus s'approprient ces nouveaux espaces ? Comment décrire les spatialités de l'habiter hors de l'habitat ? Pour Dominique Boullier, « (…) les notions " d'habitat " ne permettent pas de saisir la mise en forme technique d'une autre forme d'appropriation, de création de frontières, celle qui se fait à travers les réseaux techniques »[301]. C'est pourquoi il a proposé la notion d'*habitèle* pour décrire comment habiter l'espace urbain contemporain, et notamment l'espace hors domicile, avec des outils de gestion de la mobilité et des passages (de la simple clé de porte au passe de transports en commun).

C'est dans un essai sur *L'urbanité numérique* et la notion de « troisième ville » que Boullier a proposé en 1999 le terme d'habitèle[302]. Le terme s'inscrit dans l'idée que nous serions entrés dans une troisième ère urbaine, faisant suite à la logique urbaine de la ville comme « place forte » enclose en ses murs jusqu'au Moyen-âge, puis de la ville marchande dévolue aux échanges de biens dans un contexte d'accroissement des « modes de transport et infrastructures de déplacement » jusqu'à nos jours[303]. La troisième ville serait celle de la logique réticulaire préfigurée d'abord à travers des réseaux techniques de plus en plus complexes (dans le transport, mais aussi les « fluides » comme l'eau ou l'électricité), puis

[299] M. LUSSAULT, *L'homme spatial*, *op. cit.*, p. 348
[300] M. STOCK, « L'hypothèse de l'habiter poly-topique : pratiquer les lieux géographiques dans les sociétés à individus mobiles. », *EspacesTemps.net*, Association Espaces Temps.net, 1er février 2006 (en ligne : http://www.espacestemps.net/document1853.html)
[301] D. BOULLIER, *L'urbanité numérique. Essai sur la troisième ville en 2100*, Paris (France), L'Harmattan, 1999, p. 44
[302] *Ibid.*, p. 43
[303] *Ibid.*, p. 9

complètement actée par l'avènement des technologies numériques. Le propre de l'habiter dans la troisième ville est que l'individu doit maîtriser des compétences réticulaires de plus en plus complexes : « Notre inscription dans le réseau, notre statut de consommateur de flux techniques, vaut preuve juridique de notre appartenance spatiale. Nous sommes humainement définis comme membre de multiples réseaux. »[304] Même en en restant aux réseaux techniques ou matériels, Boullier évoque par exemple la notion d'adresse (nécessaire, d'abord et avant tout, pour l'adressage du courrier) ou de justificatif de domicile (lié pour l'essentiel au lieu où nous réglons la facture des flux consommés au dit domicile).

I - HABITELE, SENS 1 : LES MOYENS DE L'IDENTIFICATION

Dans ce contexte, un premier sens de l'habitèle désigne les dispositifs techniques individuels permettant d'évoluer parmi « [ces] affiliations ne repos[a]nt pas uniquement sur nos téléphones mobiles, mais également sur d'autres dispositifs d'accès physique ou virtuels, comme les cartes de crédit, les clés, des applications dédiées, des badges de toutes sortes, qui tendent à être concentrés dans les téléphones mobiles sans que le processus soit achevé »[305]. Autrement dit, l'habitèle renvoie à l'ensemble des dispositifs qui, associés aux compétences spatiales des individus, leur permettent de pratiquer, d'habiter les réseaux urbains. Boullier propose « (…) de prolonger alors la lignée terminologique construite sur "habere" pour désigner notre forme d'appropriation d'un espace de réseau en forgeant le néologisme de " habitèle ", composé avec tèle qui traduit le Web en toile (latin : *tela*) et proche d'étoile (latin : *stella*) qui est une forme classique de représentation des réseaux »[306]. Le rapprochement homophonique avec « télé », désignant l'activation à distance, n'est pas dénié, mais n'est pas au cœur de la proposition. Le cas de la clé, évoquée par l'auteur dans son énumération, est sans doute éclairant à ce titre : on ne peut pas faire moins distant que la clé qui entre littéralement dans la porte qu'elle est censée ouvrir. En revanche, le trousseau de clé dont chacun dispose dessine le réseau presque toujours unique des lieux auxquels il peut accéder. Boullier associe donc plutôt le suffixe « tèle » à « une lignée de composition terminologique déjà créée par " parentèle " et " clientèle " qui ont exactement cette [p. 45] construction et renvoient à la même

[304] *Ibid.*, p. 44

[305] « *These affiliations may rely not only on mobile phones per se but also on other physical and virtual service access devices such as credit cards, keys, dedicated applications, credentials of various kinds, which tend to assemble in the mobile phones, but have not yet fully converged.* » (traduction personnelle). Voir D. BOULLIER, « Habitele: mobile technologies reshaping urban life », *URBE*, vol. 6, nº 1, avril 2014, p. 13 (en ligne : https://www.boullier.bzh/articles/boullier-dominique-habitele-mobile-technologies-reshaping-urban-life/ ; consulté le 29 septembre 2020)

signification de réseau. »[306] Dans un texte ultérieur, l'habitèle de sens 1 est définie dans une formule plus synthétique de « portabilité de nos appartenances », et désigne « notre capacité générale d'appareiller notre identité sociale, notre statut de sujet »[307], à travers le téléphone, mais déjà auparavant, donc, avec des dispositifs plus classiques : « [la] portabilité de nos marqueurs d'appartenances était (…) présente dans d'autres dispositifs beaucoup plus anciens (papiers d'identité) mais aussi en développement à travers les cartes (numériques ou non) et autres dispositifs d'accès, porteurs d'information personnalisées »[308].

Dans un autre texte de 2014, Boullier insiste plus directement sur la parenté et la distinction notionnelle avec l'habitat, introduite avec la notion d'habitèle : « L'habitat, qui ne recouvre pas seulement un sens écologique, mais désigne aussi "le logis" ou "le lieu d'établissement" pour peu qu'ils soient appropriés, était le principal concept à traiter. D'Heidegger (2001) à Radlowski (2002) et Latour (2005), penser l'habitat aide à penser le processus même de couplage entre l'humain et son environnement, l'humain et la technologie, dans la mesure où ces abris sont des entités tangibles et qui, dans le même temps, encapsulent pléthore de traits intangibles, très signifiants pour ceux qui les habitent, qui en viennent à s'y sentir à l'aise, "à la maison". Tant la partie humaine que la partie non-humaine sont affectées par l'expérience de l'habiter. »[309] Dans cette première opposition, l'habitèle désigne encore l'ensemble des outils matériels ou logiciels qui nous identifient comme individus, qui nous sont à la fois nécessaires, généralement proches, et plutôt rassurants : cela explique qu'ils soient presque toujours dans nos portefeuilles, poches et autres sacs, à portée de main, dans la deuxième « coquille » décrite par Moles et Rohmer, juste après la peau elle-même. Ils sont la manifestation concrète de nos « affiliations » sociales autant que, bien souvent, les moyens de s'en prévaloir, comme lorsque nous justifions de notre état-civil à l'aide de papiers d'identité, ou que nous utilisons un badge pour passer le portique d'accès d'un réseau de transports en commun auquel on est abonné. L'habitat est quant à lui renvoyé à son sens habituel, le logis,

[306] D. BOULLIER, *L'urbanité numérique*, *op. cit.*, p. 45-46
[307] D. BOULLIER, « La portabilité des réseaux d'appartenance. Pour une théorie de l'habitèle », dans É. Bajolet, J.-M. Rennes et M.-F. Mattéi (éd.), *Quatre ans de recherche urbaine 2001-2004. Volume I : Action concertée incitative Ville. Ministère de la Recherche*, Tours, Presses universitaires François-Rabelais, 2013, § 4
[308] *Ibid.*, § 6
[309] « *Habitat, which is not only an ecological term but may encompass "lodging" and "settlement" as long as they are appropriated, was the main concept to be addressed. From Heidegger (2001) to Radkowski (2002) and Latour (2005), thinking about habitat helps us understand the very process of coupling human and environment, human and technology, since these shelters are tangible entities and, at the same time, encapsulate so many intangible features, very significant for the humans who inhabit them, who come to feel comfortable within, to feel "at home". Both human and non human sides are affected by the experience of inhabiting. Settling down and lodging do not account for the process of habitat, where a deep and lasting mark is left on each of the terms of the relationship.* » Traduction personnelle. Voir D. BOULLIER, « Habitele: mobile technologies reshaping urban life », *op. cit.*, p. 14

quoique l'auteur ne dénie pas la co-construction, le « couplage » à l'œuvre entre l'habitant et son habitat à travers la pratique de l'habiter.

Les deux termes d'habitat et d'habitèle sont en fait deux manifestations de l'habiter : l'une cristallisée dans l'espace topographique du logis, l'autre plus labile, renvoyant à la fugacité des spatialités, entendues comme pratiques spatiales. De fait, si l'on se réfère à la définition de Jean-Marc Basse dans *Habiter – Un monde à mon image*, l'habiter ne se limite clairement pas à son versant architectural (ou spatial) : « Habiter recouvre un vaste ensemble d'activités et d'expériences qui dépassent de loin, dans leurs contenus et leurs échelles, le domaine de l'architecture, du moins si l'on restreint cette dernière à la seule conception et à l'édification des bâtiments. Habiter, c'est un [p. 8] destin collectif et une expérience individuelle qui renvoient au bout du compte à l'organisation, parfois conflictuelle, de la vie, c'est-à-dire à la définition d'un temps, à la mesure d'un espace et à leur orientation générale. »[310] Si le couplage, l'influence réciproque entre l'habitant et son habitat est admise, et que l'habitat n'épuise pas l'habiter, comment la notion d'habitèle permet-elle de compléter cette notion d'habiter, et que dire du rapport de l'habitant à son habitèle ? Si, comme on le propose ici, l'habitat doit être entendu comme l'espace de l'habiter, et l'habitèle comme la spatialité de l'habiter, comment dépasser le premier sens du terme restreint à des dispositifs d'identification ?

II - HABITELE, SENS 2 : HABITER LES RESEAUX NUMERIQUES

Dans ses travaux les plus récents, et notamment lors d'un colloque à Cerisy en 2019, Dominique Boullier semble avoir élargi la portée de sa notion d'habitèle. Si l'habitèle de sens 1 convoyait nombre d'intuitions utiles à partir de la question de l'identification individuelle et des mobilités, ce n'est que récemment qu'elle semble avoir acquis pleinement un caractère plus général.

Déjà dans sa première proposition en 1999, Boullier concluait sa définition sur l'idée que la réflexion sur l'habitèle de sens 1 nous informait sur « notre façon d'appareiller le sujet que nous sommes, de nous constituer des peaux artificielles pour en faire de l'intérieur »[311], en résonnance avec la théorie de l'espace de Peter Sloterdijk qu'il cite abondamment. Au cours des vingt années suivantes, deux directions de recherche ont principalement contribué à l'évolution de la notion vers un approfondissement de cette intuition initiale. D'abord, la prise

[310] J.-M. BESSE, *Habiter*, *op. cit.*, p. 8-9
[311] D. BOULLIER, *L'urbanité numérique*, *op. cit.*, p. 46

en compte de la convergence et de la concentration des moyens de l'habitèle de sens 1 au sein d'un objet singulier, le téléphone, puis surtout le *smartphone*, ou, à terme, tout dispositif équivalent relevant de l'informatique ambiante. L'avènement de l'ère numérique a pour ainsi dire parachevé la perception que nous pouvions avoir de l'artificialité des dispositifs de l'habitèle en mettant en évidence jusqu'à leur potentielle immatérialité : la quasi-totalité des actions permises est aujourd'hui possible sans recourir à un objet tangible dédié, telle qu'une clé (voir « La serrure connectée : une réticence provisoire ? », p. 359). Ensuite, l'intérêt pour les dispositifs de l'habitèle de sens 1 mis en œuvre dans le cadre de pratiques spatiales hybrides, territoriales et/ou réticulaires[312], par exemple dans un numéro de la *Revista Brasileira de Gestão Urbana* introduit par Boullier en 2014, et dont les articles traitent de l'analyse des mobilités en Inde et à Sao Polo à partir de données téléphoniques, de la mise en relation de marchands et de leurs fournisseurs à Durban (Afrique du Sud), du service de vélos en libre-service parisien Vélib, ou encore du *marketing* direct via les réseaux sociaux en direction de consommateurs « locaux ».

Au bout du compte, Boullier finit par définir l'habitèle en 2019 comme « la dimension numérique de l'habitat, l'appropriation des réseaux pour en faire des enveloppes vivables »[313], ce que je retiens comme étant l'habitèle de sens 2. On voit bien ici que le sens 1 est dépassé par le sens 2, en ne se limitant plus aux dispositifs de nos appartenances ou de nos affiliations sociales, pour exprimer dans l'habitèle la manière dont nous habitons individuellement ces dispositifs, dont nous nous approprions / habitons le monde à travers ces médiations. L'habitèle de sens 2 a une dimension beaucoup plus existentielle, et s'inscrit dans une perspective plus profondément « anthropologique », « sociale et spatiale » esquissée dans les textes précédents : « [cette] habitèle n'est plus seulement une extension de la personne au-delà d'un territoire et d'appartenances de référence (…), elle devient la condition même du maintien du statut de personne, notamment lorsque l'habitat est trop précaire pour constituer la base subjective d'un centre. »[314]

Un autre aspect intéressant de la notion est qu'elle renvoie aux dimensions d'appropriation des réseaux, et singulièrement des technologies numériques augmentant l'espace urbain. Dans son premier texte de 1999, Boullier affirmait déjà : « Ici, point d'alerte à

[312] « *This issue of urbe will investigate all these stakes of habitele in the city through a number of case studies that have in common the crossing of boundaries between what is supposed to be urban and what is supposed to be online activity.* » Voir D. BOULLIER, « Habitele: mobile technologies reshaping urban life », *op. cit.*, p. 15
[313] D. BOULLIER, « Rendre le numérique habitable : l'habitèle », dans Y. Calbérac *et al.* (éd.), *Les colloques de Cerisy*, Paris (France), Hermann, 2019, p. 6 (en ligne : https://drive.google.com/file/d/1TCcu8tzQwgzc3Afh_jdN7RY8QBL-Yy6a/view ; consulté le 29 septembre 2020)
[314] D. BOULLIER, « La portabilité des réseaux d'appartenance. Pour une théorie de l'habitèle », *op. cit.*, § 11

la catastrophe imminente, pour ceux qui font métier de prophète. »[315] On peut penser que la critique s'adressait aux approches plus pessimistes du numérique, se focalisant sur la surveillance par exemple. De fait, il y a bien une réification des individus par ces dispositifs surveillants, qui en font des objets plutôt que des sujets. Pour autant, avec la racine *habere*, l'auteur veut aussi signaler qu'une appropriation des réseaux est possible, et ne doit pas être négligée. À travers son habitèle, l'individu est également un acteur des réseaux numériques, avec lesquels il peut composer en fonction de ce qu'il *a*, et donc les habiter, pour y *être*. Le parallèle fonctionne ici très bien avec l'habitat, qui est aussi pris selon Boullier dans une relation de co-construction avec l'habitant. De ce point de vue, un enjeu théorique de l'habitèle semble être de ne pas limiter la pensée critique des réseaux a une relation réifiant les individus qui les habitent.

III - LES DIMENSIONS DE L'HABITELE

Fort de ce constat, Boullier identifie trois dimensions de l'habitèle comme habiter numérique : le « lestage », « l'accès » et le « climat ».

Le lestage, d'abord, rappelle que tout mobiles que nous soyons, notre identité nous accompagne et que nous ne sommes pas sans attache, pérennité ou pesanteur. Le terme est « hérité du monde maritime et (…) permet de créer la verticalité nécessaire, sans pour autant empêcher la mobilité. (…) Cet héritage que nous portons avec nous quand bien même nous nous déplaçons (…) et vaudra programme pour toutes nos activités en ligne, portables mais demandant elles aussi un lestage, des repères, un au-delà d'elles-mêmes pour prendre sens. » L'auteur propose un parallèle intéressant : « Le mât des nomades remplissait d'ailleurs la même double fonction »[316], ce qui renvoie également à l'idée que de disposer de points de repères fixes, et éventuellement personnels, est une condition de l'extrême mobilité rendue par l'idéal-type du nomadisme agraire. L'essentiel de ce lestage est sans doute, de manière moins paradoxale qu'il n'y paraît, proprement réticulaire, en particulier depuis l'émergence du web social ou 2.0 : il n'est plus besoin de compétences particulières pour disposer d'un lieu à soi sur Internet, telles que des bases de *web design* pour entretenir un blog. Les réseaux sociaux, et Facebook au premier chef (historiquement et de manière presque universelle) ont doté tout un chacun d'un lieu unique ou être contacté, sollicité, et duquel partir vers d'autres pages web ou

[315] D. BOULLIER, *L'urbanité numérique*, *op. cit.*, p. 7
[316] D. BOULLIER, « Rendre le numérique habitable : l'habitèle », *op. cit.*, p. 8

communiquer soi-même avec d'autres, un lieu certes plutôt public en tant qu'il est ouvert et dédié à l'interaction, mais fondamentalement personnel[317]. Du fait de l'extrême diffusion de leurs services liée à leur hypercentralité, Facebook et Google ont également réussi à s'imposer comme de nouveaux trousseaux de clés et papiers d'identité numérique, revivifiant la notion d'habitèle de sens 1 avec *Google Connect* et *Facebook Login*, qui permettent la connexion voire l'inscription automatisée à une multitude de services tiers à partir des informations des profils-utilisateurs. Tout site peut utiliser les API afférentes de Google ou Facebook pour leur déléguer tout ou partie de l'identification des personnes souhaitant se connecter à leurs services. En somme, presque où que l'on soit sur Internet, une forme de « verticalité » transcende par ce biais nos positions en ligne instantanées, horizontales.

L'accès, ensuite, couvre la question du passage d'un espace à un autre. L'habitèle de sens 1 faisait déjà la part belle à cette dimension des spatialités, que ce soit à travers les dispositifs physiques (comme les clés) ou hybrides (comme les badges d'accès RFID). Elle se prolonge facilement dans l'habitèle de sens 2 en cela que le passage de frontières de natures diverses est évidemment une pratique courante des spatialités de l'habiter, en particulier des limites des espaces auxquels chacun dispose d'un accès particulier – domicile et autres espaces personnels même non-possédés. L'accès à des espaces plus strictement réticulaires sont également pleinement inclus dans cette dimension de l'habitèle : le recours au couple identifiant / mot de passe pour gérer les accès ou la gradation des privilèges[318] dans un espace numérique donné manifeste clairement le rapport entre l'habitant et son habitat. La personne qui ne dispose que d'un droit de consultation des données est ainsi traitée en visiteuse, celle qui dispose du droit de modification des données en dispose en revanche à sa guise – bien que des normes puissent bien sûr régir la modification de données partagées avec autrui. Il ne s'agit pas de dire ici que l'employé ayant pouvoir de modification sur la base de données clients de son entreprise, par exemple, puisse sans conséquence la supprimer comme il disposerait de ses biens propres. Un dernier niveau de privilège serait enfin celui de l'administrateur-système, qui dispose lui de droits de modification jusque sur l'infrastructure logicielle (et parfois matérielle), dont il est en quelque sort un architecte et un gestionnaire permanent. Dans l'espace territorial, les contraintes physiques limitaient la production de lieux à habiter pleinement, à savoir surtout le domicile, parfois certains espaces professionnels, auxquels adjoindre dans une moindre

[317] J. BURKELL *et al.*, « Facebook: public space, or private space? », *Information, Communication & Society*, vol. 17, nº 8, 14 septembre 2014, p. 974-985 (en ligne : http://www.tandfonline.com/doi/citedby/10.1080/1369118X.2013.870591 ; consulté le 23 janvier 2018)
[318] Privilège compris dans son sens en informatique, à savoir les droits accordés ou non de consulter ou de modifier des données.

mesure certains lieux appropriés sur un mode mineur du fait de leur fréquentation régulière, mais également accessibles à d'autres personnes avec lesquelles leur partage s'impose : un parc en bas de chez soi, un café où l'on a ses habitudes, le *club house* de son association sportive… Dans les espaces réticulaires où la contrainte physique à l'agencement d'espaces est presque nulle, la principale limite à l'habitation du monde devient finalement le temps. Les médiations numériques enrichissent donc considérablement le nombre et la variété des espaces habitables : « (…) ce sont désormais des multitudes d'intérieurs que nous produisons par la démultiplication des mondes d'appartenance, plus ou moins éphémères, et qui sont affectés les uns les autres. »[319] Plus encore, l'augmentation numérique des procédures d'accès à des espaces physiques et à leurs équipements enrichit et transforme notre rapport aux espaces existants. On verra plus particulièrement que la domotique permet des formes d'appropriation nouvelles et plus intenses des espaces domiciliaires, que l'on peut désormais contrôler ou activer à distance. Du point de vue de l'accès, l'émergence en cours des serrures connectées est un cas paroxystique sur lequel nous nous attarderons plus particulièrement. Au bout du compte, « (…) ce décentrement de l'idée de frontière, de tout, rappelle le précédent décentrement vis-à-vis d'un ancrage unique et nous permet de faire émerger un chemin vers « habiter le numérique » dans le mouvement même de la redéfinition de l'habiter. »[320]

Le climat, enfin, désigne la perception et le rapport individuels aux espaces habités : « habiter génère un couplage entre centralité et accessibilité, entre ancrage et accès : cet espace entre-deux, produit un climat, une atmosphère, une respiration, un souffle, une vibration ou pour Sloterdijk, une "tension dans la chambre intérieure". Habiter constitue une expérience très différente selon les réglages fins composant avec les ancrages et les accès : toute une théorie de l'hospitalité (Derrida, 1997) a été construite pour penser cette tension. »[321] En somme, le climat d'un lieu est la résultante de ce couplage de l'ancrage et de l'accès telle qu'elle est vécue par les individus habitant plus ou moins intensément ce lieu. Il ne désigne pas seulement une habitabilité générique, potentielle, qui relève plutôt du champ notionnel de l'aménité, mais bien le rapport individuel effectif, si ce n'est affectif, au lieu. Du point de vue plus strictement spatial, cette notion de climat est d'autant plus intéressante qu'elle participe à un dépassement épistémologique en cours relatif à l'opposition trop binaire entre métriques topologique et topographique. « (…) Le concept de coïsolation dans l'écume permet de corriger la mauvaise trajectoire dans la métaphore outrancière du réseau, dont trop d'auteurs se sont promis trop de

[319] D. BOULLIER, « Rendre le numérique habitable : l'habitèle », *op. cit.*, p. 8
[320] *Id.*
[321] *Id.*

choses - le plus souvent sans remarquer qu'avec ce discours de la mise en réseau, ils font des emprunts à un graphisme erroné et à une géométrie démesurément réductrice : au lieu de souligner le fait que les communicateurs à mettre en relation mutuelle disposent de leur espace propre, l'image du réseau suggère une conception fondée sur des points sans étendue que des lignes rassembleraient sur des interfaces - un univers pour pêcheurs de données et anorexiques. (…) Le discours des écumes souligne en revanche les volumes spécifiques des unités communicantes. »[322] Lussault fait également sienne cette critique en hybridité de métriques trop généralement opposées dans son *Homme spatial* : « De ce point de vue, je souscris à la critique de Sloterdijk qui reproche aux tenants du concept de réseau d'omettre que les points d'un réseau sont des espaces propres, tout comme les lignes au demeurant »[323]. La notion de climat proposée par Boullier permet le dépassement de cette opposition ou, à tout le moins, fournit un premier terme qui permette de nommer la nécessité de ce dépassement en redonnant du volume aux points des réseaux parcourus par les individus.

Les enceintes connectées, ou les dispositifs à venir qui en prolongeront le principe, semblent un cas d'autant plus intéressant du point de vue de l'ancrage qu'elles sont conçues pour être de nouveaux *hubs* dans la relation au « foyer » (ou à l'*oikos* que Boullier évoque comme « principe situant »). Ces nouvelles médiations numériques activent puissamment la relation à distance au foyer dans un registre inédit, sauf peut-être pour de rares précurseurs en matière de domotique, et sans parler des représentations déjà proposées par la science-fiction. Toutes les dimensions de l'habitèle de sens 2 sont mobilisables pour traiter des enceintes connectées. Comme *hubs* domotiques, elles constituent un point d'ancrage pour une grande partie des appareils connectés du domicile, autant qu'un point d'accès vers eux depuis l'extérieur. Mais ces relations réticulaires n'en ont pas moins des effets topographiques sur le lieu qu'est le domicile, des effets « climatiques ». Leur utilisation implique par exemple des habitants une réflexion sur la zone couverte par les antennes Wi-Fi et Bluetooth de leurs appareils, à l'extension de la zone de captation et/ou de diffusion audio de leur enceinte, et aux aménagements tout à fait matériels à opérer en conséquence – où installer le modem ? où installer une ou des enceintes connectées ? etc. Le sens climatique est parfois même à prendre au sens propre quand il s'agit de régler ou déléguer à un algorithme la gestion du thermostat ou encore d'automatiser ses volets roulants avec des conséquences sensibles sur l'air ou la luminosité intérieure du logement. Quant à leur fonction comme point d'accès, elle est assez

[322] P. SLOTERDIJK, *Écumes*, *op. cit.*, p. 226
[323] M. LUSSAULT, *L'homme spatial*, *op. cit.*, p. 134

classiquement celle des dispositifs numériques, personnels ou partagées dans un groupe social restreint, quand ils sont connectés à Internet.

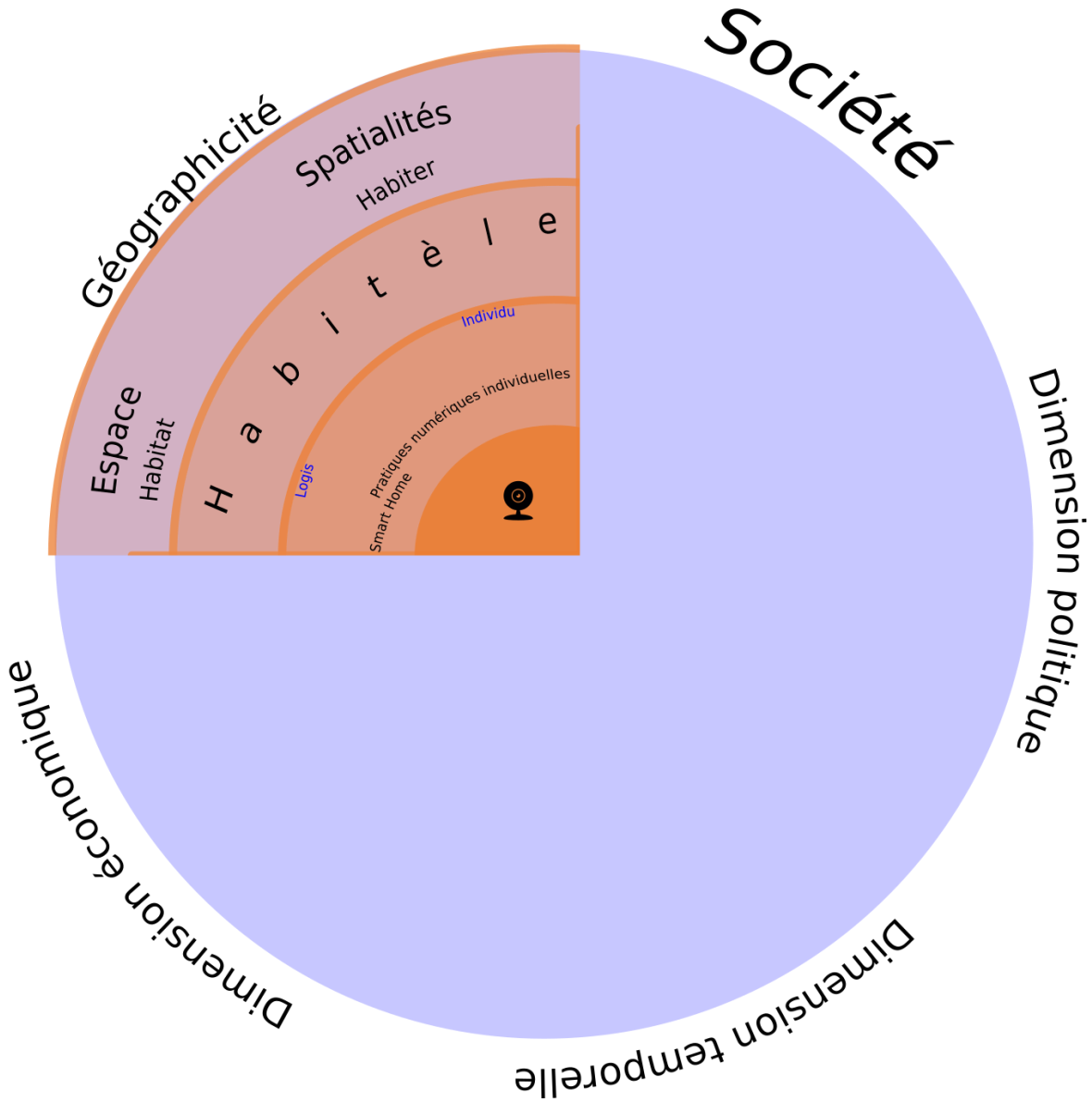


Figure 10 - L'approche géographique de l'enceinte connectée à travers la notion d'habitèle (JFP)

In fine, la notion d'habitèle permet de fonder l'approche géographique de l'ensemble des dispositifs domotiques en interaction avec les pratiques numériques individuelles qui en sont faites (voir Figure 10). Elle invite à une approche dynamique de ces dispositifs, des espaces dans lesquels ils s'insèrent et qu'ils concourent à produire à travers les nouvelles modalités de l'habiter introduites par les médiations numériques. Si l'habitèle est le pivot d'une approche spécifiquement spatiale de ces dispositifs, il ne s'agit pour autant pas de méconnaître d'autres

approches complémentaires du sujet, qui peut (et doit) bien sûr être également abordé dans ses dimensions politique, économique et temporelle.

Chapitre 2 - LA RUPTURE HISTORIQUE DU SMARTPHONE

D'un point de vue historique, il faut signaler que le cas et les usages du *smartphone* anticipent presque parfaitement le retournement provoqué par l'émergence de la *smart home*. Outil par excellence de l'habitant nomade et/ou polytopique ainsi que des spatialités de métrique (plutôt) topologique, il constitue la rupture technologique la plus forte de ces dernières décennies en synthétisant l'ensemble des apports d'une informatique miniaturisée, multimédia, connectée et sans fil. On parle parfois d'informatique ambiante ou *pervasive* (en anglais) pour rendre compte de cette omniprésence des terminaux et des réseaux dans l'espace. C'est plus particulièrement à travers le *smartphone* que le numérique a fait, pour ainsi dire, *écumer* le social au point de brouiller la limite entre espace privé et espace public. Les possibles ouverts par le dispositif *smartphone* dépassent même largement ceux de la *smart home*, même si cette dernière a quelques spécificités propres.

I - LE SMARTPHONE EST LE PRINCIPAL DISPOSITIF DE RUPTURE DE L'INFORMATIQUE AMBIANTE

Dans l'ouvrage tiré de sa thèse, *Smartphone*, Nicolas Nova adopte lui aussi une approche historique des usages progressivement permis ou condensés dans le *smartphone* (voir Figure 11). Il en propose une lecture « anthropologique » à travers une série de quatre « transversalités », et en le décrivant notamment comme un objet à la fois « protéiforme » et « total ». [324] L'évolution du téléphone portable au *smartphone* a mené à la convergence de fonctions de plus en plus nombreuses depuis la téléphonie jusqu'au paiement par carte (voir

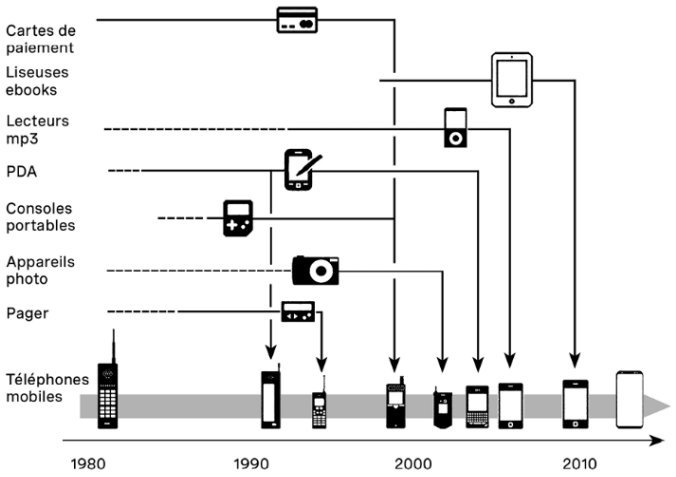


Figure 11 - Évolution de la convergence des services numériques sur le smartphone, avec une représentation à l'échelle des terminaux (Source:N.Nova, 2020)

[324] N. NOVA, *Smartphones: une enquête anthropologique*, Genève (Suisse), MétisPresses, 2020, chap. Conclusion

Figure 11) et, désormais, la télécommande pour la domotique. L'informaticien Stéphane Bortzmeyer reprend d'ailleurs volontiers la traduction peu usitée « ordiphone », et décrit cet appareil comme « Un ordinateur complet, avec les avantages et les inconvénients d'un ordinateur, mais qui est souvent appelé « téléphone » alors que ce n'est qu'une de ses fonctions, qui n'est parfois même plus utilisée »[325]. Cette convergence fonctionnelle a fait du *smartphone* beaucoup plus qu'un dispositif numérique parmi d'autres. Il est sans aucun doute l'objet le plus couramment et le plus longuement manipulé au quotidien par la plupart des personnes qui en disposent. Souvent activé/déverrouillé jusqu'à plusieurs dizaines de fois par jour, plus de la moitié des personnes âgées de 50 ans ou moins déclaraient lui consacrer plus d'une heure par jour, et même plus de quatre heures par jour pour près d'un tiers (28 %) des jeunes de 15 à 17 ans (voir Figure 12). Parmi les terminaux d'accès au Web, le *smartphone* est aujourd'hui dominant : sa part dans le trafic mondial est systématiquement supérieur à 50 % depuis le troisième trimestre 2019, et a culminé à 55,78 % au troisième trimestre 2021[326].

[325] S. BORTZMEYER, *Cyberstructure: l'internet, un espace politique*, Caen (France), C & F Éditions, 2018, p. 30
[326] StatCounter (12/I/2022). « Percentage of mobile device website traffic worldwide from 1st quarter 2015 to 4th quarter 2021 [Graph] ». In *Statista*. Consulté le 19/I/2022 : https://www-statista-com.ezproxy.u-pec.fr/statistics/277125/share-of-website-traffic-coming-from-mobile-devices/

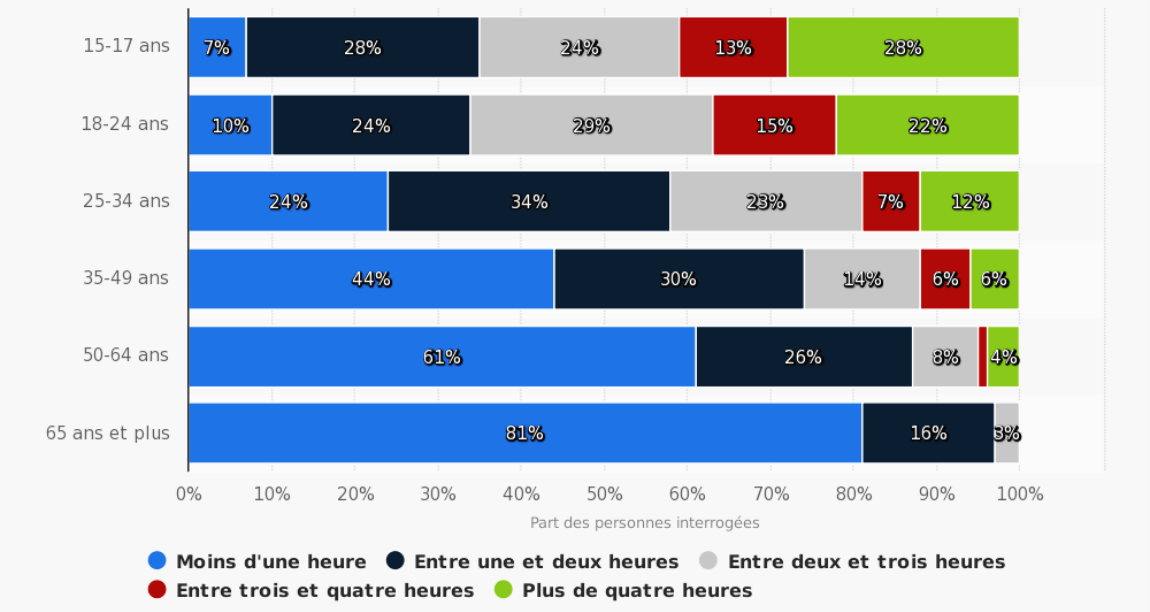


Figure 12 - Répartition des possesseurs de téléphone mobile en France en 2017, selon l'âge et la durée d'utilisation par jour

Détails : France; IFOP; 9 - 15 février 2017; 1.202 personnes interrogées; 15 ans et plus; possesseurs d'un téléphone mobile permettant d'écouter de la musique, soit 88 % de l'échantillon; Questionnaire auto-administré en ligne (CAWI)

Cette prégnance de l'utilisation du *smartphone* dans les budgets-temps quotidiens est l'une des raisons qui poussent Nicolas Nova, reprenant les termes d'une de ses enquêtées, à parler entre autres choses de cet objet comme d'une « laisse ». Le terme est particulièrement intéressant en cela qu'il signale à la fois très littéralement l'attachement physique, mais suggère aussi la mobilité. L'écho sémantique est partiel, mais signifiant, avec le « lestage » et le « mât des nomades » décrit par Boullier. Le *smartphone* est un lien (au sens de ligature), mais un lien mobile, et c'est là que réside son intérêt majeur comme technologie spatiale. En effet, là où les architectes, urbanistes et designers anticipaient dans les années 1990 l'informatisation et la connexion du / dans le / par les surfaces des murs et le bâti en général (voir « *Smart home* : l'augmentation de l'espace privé par la domotique », p. 156), le premier succès commercial des *smartphones* avec l'iPhone d'Apple sorti en 2007 a radicalement changé la donne en n'attachant plus son utilisateur à une interface peu mobile, voire ancrée, comme une borne numérique ou une tour d'ordinateur personnel – et l'infrastructure physique de câbles afférente. Le *smartphone* en tant que terminal informatique n'est pas en soi révolutionnaire : il accentue et prolonge des logiques déjà à l'œuvre dans l'informatique personnelle, comme la miniaturisation des composants, le fonctionnement sur batterie, ou l'interface tactile. Ce qui différencie le *smartphone* de l'ordinateur portable ou du PDA (*Personal Digital Assistant*), c'est avant tout

sa connectivité aux réseaux de téléphonie mobile, et à travers eux à Internet, au sein de vastes cellules qui rendent cette connexion aisée et quasi permanente[327], ou encore *ambiante*.

En somme, c'est le fait que la « laisse » soit aussi un lien continu aux réseaux téléphoniques et de données qui a permis au *smartphone* de s'intégrer aussi finement dans nos vies quotidiennes. D'une part, il est toujours à disposition pour des usages actifs : il suffit de le sortir de la poche pour trouver son chemin, réserver une place de train ou regarder une vidéo. D'autre part, il est toujours passivement présent pour nous solliciter afin de répondre à un appel, nous prévenir de l'arrivée d'un message ou d'une notification. Il était déjà techniquement possible d'être connecté en quasi-permanence *via* un terminal informatique plus classique et peu mobile de type ordinateur personnel avec l'arrivée des technologies DSL à la toute fin des années 1990[328]. Mais cette expérience a été généralisée à la vaste majorité de la population[329], plus particulièrement à l'arrivée des réseaux 3G (fin 2004 pour la France), au point que les utilisateurs de *smartphones* sont connectés partout et par défaut, et que la déconnexion relève de la démarche active, du droit revendiqué, ou de l'accident plus que de la norme. En France, 84 % de la population de plus de 12 ans possède un *smartphone* en 2020, et 94 % un téléphone mobile en général[330]. Par ailleurs, le *smartphone* est devenu le terminal informatique le plus commun depuis 2019, avec un taux d'équipement de 77 %, devant l'ordinateur à domicile (76 % en 2019, en chute à 61 % en 2020)[331].

L'infrastructure qui rend possible cet usage du *smartphone* se rappelle tout de même à l'utilisateur de smartphone éloigné d'une antenne-relais ou d'une borne Wi-Fi – le cas étant de plus en plus rare. La question de

[327] Cellule étant à comprendre comme la zone couverte par une antenne-relais de téléphonie mobile, auquel se réfère la langue anglais avec *cell phone*. Il est à noter que la première norme de téléphonie cellulaire ne permettait que la communication vocale par la transmission d'un signal analogique, comme celui d'un talkie-walkie. C'est avec la norme *Global System for Mobile Communications* (GSM, ou 2G) que le signal utilisé est désormais numérique. Les extensions « 2,5G » à la norme GSM que sont GPRS (*General Packet Radio Services*) puis EDGE (*Enhanced Data rates for GSM Evolution*) ont par la suite permis la généralisation de la transmission de données par paquets et donc l'usage de l'Internet mobile à un prix accessible.

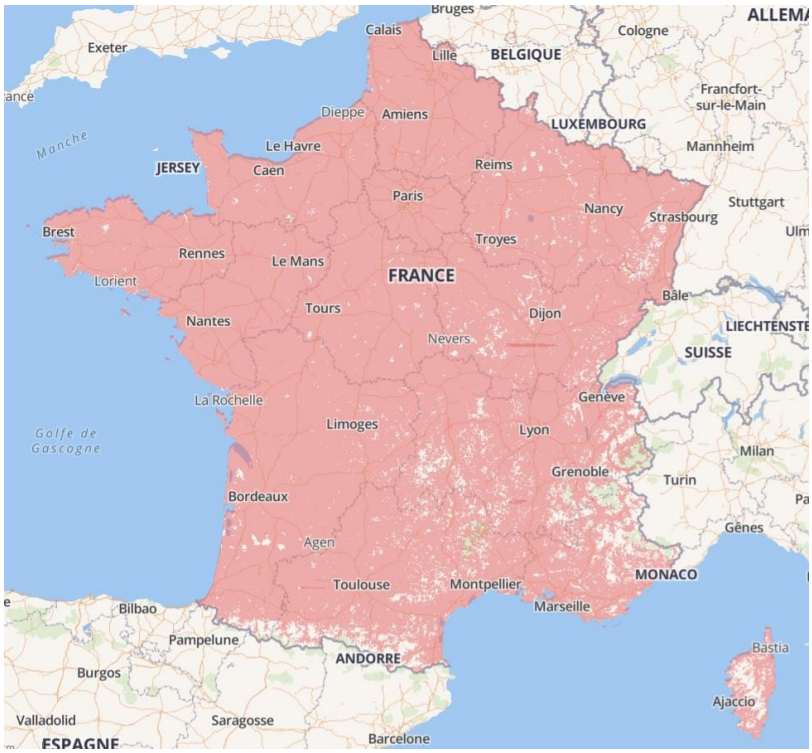
[328] Les technologies DSL (dont l'ADSL) ont inauguré la possibilité pour l'usager d'être connecté au réseau Internet sans monopoliser sa ligne téléphonique physique, comme GPRS et EDGE pour la téléphonie mobile. Elles ont aussi permis l'augmentation de la capacité des connexions en utilisant un plus large spectre de fréquence sur la ligne téléphonique en cuivre que celle auparavant utilisée à la seule fin de transmettre la voix.

[329] La moitié de la population mondiale dispose d'un accès à l'Internet mobile depuis 2020 (J. SSALI, « Infographic: Half the global population are now using the mobile internet », sur *GSMA Intelligence*, février 2020 (en ligne : https://data.gsmaintelligence.com/research/research/research-2020/infographic-half-the-global-population-are-now-using-the-mobile-internet ; consulté le 15 février 2022)). Pour la France, les possesseurs de *smartphone* dans la population en France âgée de 12 ans ou plus est passée de 46 % en 2014 à 58 % en 2015 (*Baromètre du numérique 2021 - Enquête sur la diffusion des technologies de l'information et de la communication dans la société française*, Paris (France), CRÉDOC, 2021, p. 27)

[330] *Baromètre du numérique 2021*, *op. cit.*, p. 27

[331] *Ibid.*, p. 46

la « fracture numérique » a longtemps été un enjeu territorial (voir « L'approche territoriale d'Internet », p. 8), mais la résorption des « zones blanches » (voir « Internet et la « fin de l'espace » », p. 72) est très avancée aujourd'hui, comme en témoigne la Carte 1. On observe que les zones non couvertes en 4G fin 2021 sont rares et concernent essentiellement des territoires de montagne très peu densément peuplés : Massif central, parc national des Écrins, parc naturel régional (PNR) du Vercors, Pyrénées, montagne Noire… et quelques rares espaces en plaine : quelques villages du PNR Loire-Anjou-Touraine, ou la périphérie du pays d'Othe. L'utilisation d'un *smartphone* connecté au réseau de manière appropriée est donc généralisée aujourd'hui, à de rares exceptions près. Le *smartphone* est donc aujourd'hui, comme terminal et comme point de connexion réseau, une interface vers presque toutes les dimensions du social aujourd'hui médiées par le numérique.



Carte 1 - Carte de couverture en téléphonie mobile 4G sur réseau Orange (simulée au 30/09/2021 à partir des données d'Orange; ARCEP 2022)

Cette carte est tirée du site de suivi https://monreseaumobile.arcep.fr/ de l'ARCEP. Orange a été choisi en tant qu'opérateur historique ayant repris les activités de France Télécom, et la norme de télécommunications 4G en tant que standard pour les terminaux début 2022. 99% de la population au moins est couverte pour les quatre opérateurs français. La couverture surfacique du territoire est de 92% pour Orange (Bouygues : 93%, Free : 90%, SFR : 94%).

II - SMARTPHONE ET VIE PRIVEE

Le *smartphone*, s'appuyant sur sa connectivité et ses capacités computationnelles de véritable ordinateur de poche, constitue aujourd'hui à travers son écran tactile la paroi d'une bulle qui nous rend virtuellement contigus dans l'écume à une très grande variété de personnes, de logiciels et d'espaces. Sa fiabilité technique est suffisante pour en faire même un *hub* logiciel et physique pour des dispositifs satellites relevant des *wearable technologies* ou *everywear*, à

savoir l'ensemble des dispositifs informatiques portables à la manière d'un vêtement (*wear*), comme les montres connectées. Le smartphone joue à l'échelle du corps et des prothèses annexes de type montre connectée le rôle de *hub* de l'enceinte connectée par rapport aux objets domotiques à l'échelle du logis. Il est, en outre, pleinement intégré dans les processus de commande de la domotique elle-même, qui s'appuie massivement sur des applications sur *smartphone* pour la configuration des différents objets connectés, quand bien même ils finiraient commandés préférentiellement à la voix à travers le hub domotique qu'est l'enceinte connectée.

C'est dans la partie de sa thèse consacrée au *smartphone* comme « miroir » de son utilisateur que Nova traite de la question du privé. Comme miroir, le téléphone individuel reflète les pratiques, les pensées, voire l'intimité physique des personnes. Pour autant, l'auteur nous fait part de son étonnement quant au fait que la question du *smartphone* comme potentiel « mouchard » soit à peine évoquée par ses enquêté (l'un d'entre eux employant tout de même le terme) : « La métaphore du « mouchard » fait partie de ces « descripteurs » minoritaires et mentionnés très rapidement par les usagers alors que c'est un thème que j'aurai a priori imaginé comme fondamental et présent comme un chapitre indépendant dans cette thèse. »[332] Il est à signaler que ce terme même n'est employé que quatre fois dans mon propre corpus, par deux enquêtés différents, et de manière spontanée – même si la thématique afférente est évidemment beaucoup plus développée par et avec mes enquêtés.

Nova esquisse dans la foulée une série d'hypothèses pour tenter d'expliquer cet état de fait : « Cependant, ce n'est pas le cas, la crainte de la surveillance étant présente dans les discours, mais en général évoquée rapidement, et surtout sans renvoyer à des pratiques spécifiques chez la grande majorité des enquêtés (installation de VPN, utilisation de logiciel de cryptage). Est-ce parce que les usagers se sentent démunis ? Est-ce parce que les conséquences dans les pays occidentaux ne sont pas assez visibles (malgré les révélations d'un Edward Snowden ou les affaires...) ? Est-ce que les moyens de se prémunir de cette surveillance nécessitent un apprentissage ? Ou est-ce qu'ils n'en ont pour le moment pas eu à subir les conséquences ? »

La principale porte vers et depuis les espaces réticulaires

Son importance majeure comme dispositif numérique est bien identifiée par les personnes interrogées dans le cadre de ce travail de recherche, malgré le fait qu'il ait été

[332] N. NOVA, *Figures mobiles: une anthropologie du smartphone*, s. d., p. 267

présenté comme traitant de la question de la vie privée, et relevant du numérique en général puis des enceintes connectées en particulier. Ainsi, le terme « téléphone » au singulier est évoqué 396 fois dans le corpus (dont 129 dans mes propos), et il est évoqué d'abord par les enquêtés dans 10 des 16 entretiens où il est évoqué. Surtout, il s'agit du deuxième terme significatif (113^{e} en général) évoqué par les seuls enquêtés après Google (396 occurrences, 89^{e} terme le plus évoqué en général). Pour « *smartphone* », le nombre d'occurrences est de 54, mais il est présent dans mes questions à 32 reprises, et plutôt à mon initiative (dans 6 des 11 entretiens où le terme est évoqué), ce qui permet de dire qu'il n'est pas le plus usité par mes enquêtés. Même dans le contexte d'une enquête portant plutôt sur les enceintes connectées et la domotique, l'importance première du téléphone/*smartphone* dans la vie des personnes interrogées est donc très nette. De fait, tous mes enquêtés, mêmes les plus critiques, sont équipés d'un *smartphone*. Seul E17 disposait d'un téléphone cellulaire basique dans les premiers temps de notre prise de contact, et même lui a fini par s'équiper d'un *smartphone* un an plus tard – quoiqu'il continue d'être opposée aux enceintes. Seul E5 a quant à lui pris des dispositions logicielles fortes et systématiques du type de celles évoquées par Nova (utilisation d'un VPN et du chiffrement) pour protéger sa vie privée dans l'utilisation de son *smartphone*

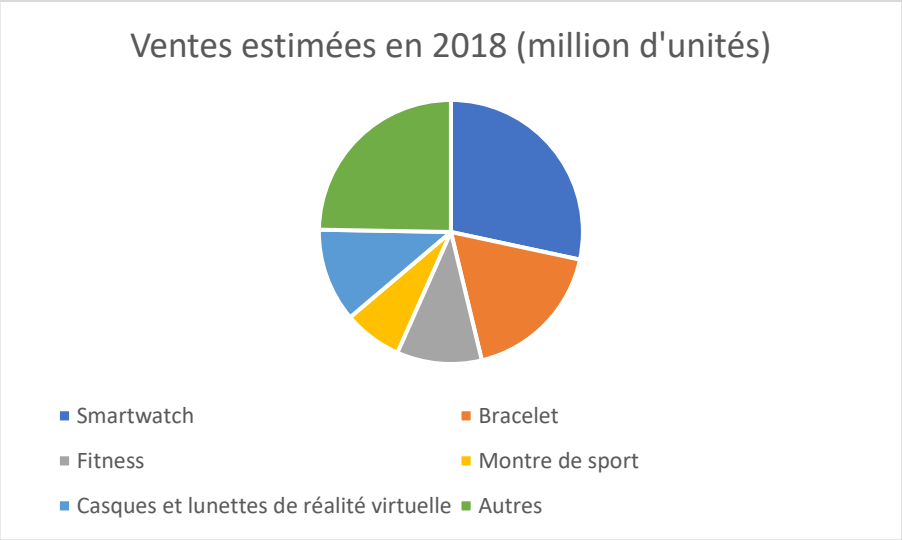
Le smartphone est un dispositif d'autant plus intéressant qu'il associe de plus en plus les deux sens de la notion d'habitèle, et qu'il condense les pratiques et les problématiques liées à la vie privée et à l'intimité. Pour reprendre les termes de Nova, il est à la fois « miroir » de nous-mêmes et « baguette magique » qui permet d'accéder à l'altérité sociale et spatiale. Il permet à la fois d'emmener et de connecter son intimité ou son identité numérique partout avec soi. Il n'est pas seulement un terminal avec lequel on interagit, mais aussi un moyen d'identification numérique de plus en plus utilisé, voire nécessaire. Le phénomène a été particulièrement mis en évidence lors de la pandémie de Covid-19, où le *smartphone* a servi pour beaucoup à produire leurs certificats de déplacement aux forces de police lors des épisodes de confinement, puis à justifier de leur statut sérologique ou vaccinal au moyen des différentes versions de l'application « anti-covid » en France et dans le monde[333]. Dès avant cela, il pouvait déjà être utilisé, quoique de manière moins répandue, pour faire office de carte de crédit (avec les systèmes *Pay* d'Apple ou de Google) ou encore de carte de transport en commun grâce à sa puce RFID. Depuis sa sortie en 2012, une application d'Apple, *Passbook*, renommée *Wallet* en

[333] Il faut néanmoins préciser que cet usage d'identification lors de la crise covid n'était pas, au moins en France, particulièrement liés aux espaces réticulaires, ces certificats étant disponibles localement sur l'appareil des personnes, ni plus ni moins que comme la version numérisée de passe ou de certificats pouvant être produits également sous forme papier. Les usages suivants, qui s'appuient sur la communication avec des bases de données distantes, passent cependant par le réseau Internet.

2015, permet d'ailleurs de concentrer un grand nombre de types de cartes d'identification, que ce soit pour les programmes de fidélité, les transports en commun ou le paiement afin de faire office, comme son nom l'indique, de portefeuille numérique.

S'il est donc une porte d'entrée de l'individu vers le vaste monde, le *smartphone* est aussi une porte d'entrée du vaste monde vers l'individu. Cette faculté à créer, dans tout le géoespace couvert par les cellules de téléphonie mobile, de la connexion bidirectionnelle, est à la fois ce qui constitue le principal intérêt et le principal défaut du téléphone mobile. Comme le *smartphone* est devenu l'objet-phare de notre habitèle, et qu'il nous accompagne partout dans nos vies quotidiennes, il confère à autrui un fort potentiel d'immixtion dans nos vies privées, nos intimités contemporaines. Cela est d'autant plus vrai en association avec la *wearable technology* (ou les objets plus communément appelés des *weareables*, que l'on peut donc *porter*), à savoir des habits ou des accessoires dotés de capteurs et de fonctions de télécommunication ; parmi lesquels les montres et bracelets connectés se taillent la part du lion (voir Figure 13). La traduction française habitronique, quoique peu reprise, est intéressante. Elle a été employée en 2015 lors de la conférence annuelle de l'institut informatique de la Haute École spécialisée de Suisse occidentale (HES-SO), Technoark[334] et dans un ouvrage[335], puis en 2019 dans deux autres publications scientifiques[336]. Malgré son insuccès, il reste intéressant de constater que c'est là encore la racine « habit », parente à habitèle et habitude, qui a été employée pour désigner l'augmentation numérique communicante d'objets et de vêtements portés à même le corps de l'utilisateur. Dans la vaste majorité des cas, ces objets *wearables* dépendent du *smartphone* qui fait office de modem et de routeur portable pour constituer comme une bulle de connectivité, une mini-cellule elle-même incorporée dans les méso-bulles que sont les cellules autour des antennes-relais connectant à leur tour les individus au réseau Internet, selon un principe

[334] G. BERRAUD, « Ces puces intelligentes qu'on porte sur nous », *Le Nouvelliste*, 31 janvier 2015, p. 4 (en ligne : https://www.theark.ch/media/document/0/conferencetechnoarkhabitronique_nf_31.01.2015.pdf)
[335] R. ACAS *et al.*, *Objets connectés : La nouvelle révolution numérique*, Saint-Herblain (France), ENI, 2015
[336] P. VELGHE, « «Lire la Chine». Internet des Objets, surveillance et gestion sociale en RPC. », *Perspectives chinoises*, vol. 2019, nº 2019-1, Centre d'Études Français sur la Chine contemporaine, 2019, p. 91-96 ; S. BENOUAKTA *et al.*, « Conception d'une antenne hélice pour fil textile RFID UHF extensible », dans *Actes JNM 2019*, Caen (France), 2019, p. 865-868



Source : Gartner (2017). https://fr-statista.com/statistiques/672203/marche-wearables-volume-estimation-monde/

Figure 13 - Volumes des ventes d'objets wearables en 2018

En cela, la rupture introduite par le *smartphone* dans les spatialités augmentées des individus est donc extrêmement forte puisqu'elle permet, dans une certaine mesure, de s'exonérer de la connectivité physique antérieure reposant sur des connexions filaires. Certains enquêtés pointent d'ailleurs très bien cette portabilité parfois envahissante de leur habitèle à travers le *smartphone*. Ainsi d'E5, qui perçoit bien du fait de sa trajectoire militante des risques à toujours être numériquement identifiable y compris dans l'espace public à cause de son *smartphone*. Dans un langage coloré, il explique ne pas toujours sortir de chez lui son téléphone en poche, qui sinon serait « toujours à moins de cinquante centimètres de [son] cul » (entretien 5, 1 h 32 min 40 s), et que « du coup pour moi c'est important de laisser des espaces où cette condition n'est pas vraie. » (entretien 5, 1 h 32 min 50 s). Et ce, alors qu'il dispose d'un Fairphone livré par défaut avec un système d'exploitation qui n'est pas lié aux serveurs de Google, et qu'il utilise majoritairement des applications orientées vers la protection de la vie privée. Fin connaisseur des réseaux internétiques, il s'agit ici pour lui de se préserver du traçage par son opérateur téléphonique à travers les connexions effectuées en permanence par les appareils cellulaires avec les antennes-relais environnantes. Si E5 est un cas-limite du fait de ses compétences techniques, qu'en est-il de la perception et des usages des autres enquêtés envers leur *smartphone* ?

Un danger très nettement perçu du smartphone pour la vie privée

La première des craintes explicitement exprimées par rapport à leur *smartphone* par beaucoup d'enquêtés est finalement des plus classiques, et concerne en fait sa fonction historique de simple téléphone mobile, permettant de recevoir des appels, mais aussi des SMS ou, plus récemment des notifications. Dans la série de questions du guide d'entretien où les enquêtés devaient estimer différents items sur une échelle allant du privé au public, celle concernant le numéro de téléphone a souvent provoqué une réaction de rejet concernant les sollicitations non désirées, si elle n'avait pas déjà été exprimée avant que cette question ne soit posée. La réaction d'E16 est représentative à cet égard :

> « E16: Non, généralement quand... ça me fait, toujours, j'ai toujours du mal, petite parenthèse, quand je fais une commande sur Internet ou quoi que ce soit, ils me demandent mon numéro de téléphone. Moi je veux pas. Je me dis qu'ils vont me foutre de la pub, je vais... C'est soi-disant pour le livreur, ahahah, tu me prends, en plus, pour une chèvre ! Non, j'ai du mal avec le numéro de téléphone. J'estime que c'est quelque chose de personnel, que je donne à qui j'ai envie. On me le demande pas de manière forcée. C'est très privé. Enfin, privé…» (entretien 10 ; 1 h 55 min)

Sa crainte en donnant son numéro de téléphone est donc de recevoir « de la pub », sous couvert de l'utilité de communiquer son numéro à un éventuel livreur lors d'une commande sur Internet. Pour E4 ou E19, la même crainte est exprimée par exemple lors des demandes de coordonnées à la création de cartes de fidélité dans les commerces. E16 insiste sur le caractère privé de l'information, avant de se raviser quelque peu (« Enfin, privé… »), ce qui illustre bien la dichotomie classique de l'ouverture ou de la fermeture appliquée aux communications : s'exposer est utile, et E16 veut pouvoir communiquer via son numéro de téléphone, mais c'est aussi un risque, dans la mesure où toutes les sollicitations ne seront pas désirées. Beaucoup d'autres enquêtés étaient dans le même cas, oscillant entre le caractère public et privé de l'information. Plus encore, la remarque d'E16 pointe implicitement qu'il n'a pas confiance dans les acteurs qui lui réclament son numéro, pas qu'il remet en cause l'utilité de communiquer son numéro à un éventuel livreur, ce qui serait légitime (« (…) tu me prends, en plus, pour une chèvre ! »). Rien d'étonnant à ce type de réactions chez beaucoup d'enquêtés : la défiance envers la publicité mobile est bien connue et mesurée. Dans un sondage OpinionWay en 2015, 48 % des sondés estimaient les notifications mobiles « envahissantes » ou « intrusive », alors même que le sondage proposait plus de possibilités de réponse au caractère nettement positif (« pratique », « intéressante », « pertinente », « agréable »), comme le montre la Figure 14.

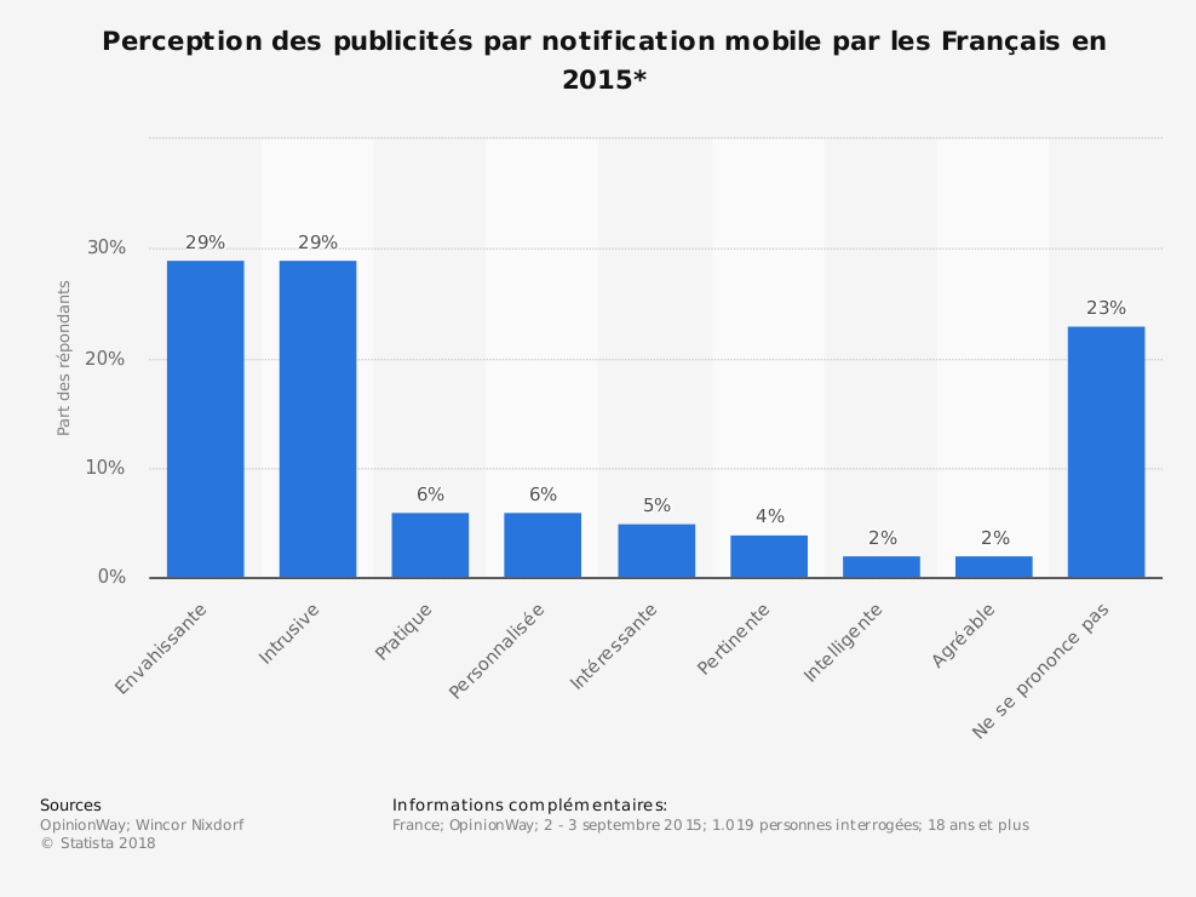


Figure 14 - Perception des publicités par notification mobile par les Français en 2015

Les propos d'E20 prolongent de façon éclairante ce premier constat simple. Elle explique que les publicités (qu'elle appelle « spam ») sur téléphone sont d'autant plus « super [intrusives] » que le téléphone est un « quand même un truc que j'ai sur moi » :

> « Parce que le téléphone c'est quand même un truc que j'ai sur moi. Là où les mails c'est moins intrusif, le téléphone c'est super intrusif. Et je ne supporte pas de recevoir... en fait j'ai un truc, j'ai un seul spam que je reçois c'est Pizza Hut, je n'arrive pas à le désactiver. Mais sinon je reçois très peu de spam sur mon téléphone. Même des appels ou ce genre de choses, j'en reçois très peu. Heureusement parce que je trouve ça très… Tu as toujours ton téléphone en permanence sur toi, enfin quand tu as un message tu as envie que ce soit le message d'un ami ou quelque chose. Un truc, un truc intéressant j'entends.
> JF: Un truc intime
> E20: Voilà, un truc perso. Déjà que j'ai des notifications inutiles. Voilà quand il y a quelque chose il faut vraiment que ce soit quelque chose qui est utile. C'est pour ça que pour moi le numéro c'est hyper…verrouillé. Par contre dans le cercle social, je lui donne beaucoup plus facile… Enfin c'est pas…
> JF: Oui, à une personne.
> E20: Même une personne que je connais très peu, si on doit se recontacter, ça ne

me dérange pas de lui donner mon téléphone.» (entretien 13 ; 2 h 17 min 40 s)

Dans son discours, il transparaît qu'elle ne conçoit pas qu'une publicité puisse être autre chose qu'une nuisance (« quand il y a quelque chose il faut vraiment que ce soit quelque chose qui est utile ») : là encore, l'utilité de communiquer son numéro n'est pas contestée, mais il ne doit être utilisé que dans le bon contexte. Elle insiste bien sur le fait qu'elle n'a rien contre recevoir un appel ou un message d'une personne même si elle la connaissait très peu, pour peu que ce message relève de son « cercle social », et pas d'une sollicitation commerciale. Le fait qu'elle répète deux fois en quelques phrases que le téléphone est quelque chose qu'on a « sur soi » en permanence n'est pas anodin, à plus forte raison dans le discours d'E20 qui fait état à plusieurs autres moments de son entretien de son besoin d'intimité, de sa pudeur, et d'une gestion fine de la manière dont elle expose des éléments de sa vie personnelle (au travail notamment). Sa réaction rend ici très lisible le lien quasi organique au téléphone mobile personnel, à la fois comme miroir et comme laisse, dans la terminologie de Nicolas Nova.

Plus spécifiquement au *smartphone* comme ordinateur mobile équipé d'une grande variété de capteurs et de capacités de connexion à divers réseaux, trois enquêtés permettent de cerner l'éventail des attitudes possibles. E1, E3 et E10 sont parmi les enquêtés les plus au fait des possibilités techniques de traçage offertes par leurs appareils. Leurs postures respectives par rapport à l'utilisation des services Google reflètent bien l'éventail des postures possibles quant à la surveillance via le *smartphone*. On l'a vu, chez le très militant E10, cela se traduit par une attitude active de défense contre la dissémination de ses données personnelles. E1 a une attitude intermédiaire : il a conscience des risques, et agit marginalement en conséquence. Il utilise par exemple le navigateur web Mozilla Firefox sur son ordinateur personnel, mais Google Chrome sur son *smartphone* Android, ce qu'il me déclare d'un air contrit. Lorsque je lui demande s'il sait que Mozilla Firefox existe aussi en version mobile, sa réponse est pragmatique : « Oui, je sais, mais il est moins bien » (entretien 01 ; 7 min 50 s). De même, sur la question du moteur de recherche, il utilise principalement Google, même s'il a déjà essayé Qwant : « Je sais, il faut utiliser Qwant, mais ça me fait chier » (entretien 01 ; 8 min 20 s). Quant à E3, il considère qu'il n'a rien à cacher, et utilise volontiers tous les services Google sans restriction. E14 et E15 présentent un profil comparable à celui d'E3 de ce point de vue. Ils se distinguent quelque peu en tant qu'utilisateurs quasi exclusifs de produits Apple, mais ils recourent à Google Maps pour la navigation.

Les craintes sont plus floues, sans être forcément moins présentes, au contraire, chez les autres enquêtés. Quand nous évoquons la question de Linky avec E16, celui-ci m'explique ne pas connaître du tout le dispositif, au-delà du nom de la marque. Après que je lui ai présenté les enjeux généraux identifiés dans les controverses autour de Linky, sur les plans de la santé et de la vie privée, et notamment le fait que Linky permette de savoir facilement quand un logement est occupé, E16 reprend immédiatement la balle au bond et fait spontanément le lien avec la géolocalisation du *smartphone* :

> « (…) Ca veut dire malgré tout qu'ils savent quand t'es chez toi, ils savent...
> E16: Pff, s'ils veulent vraiment savoir quand t'es chez toi, on a déjà un téléphone dans la poche, heu...
> JF: (acquiesce)
> E16: Quand tu vois le truc de Apple, où tu vois ta localisation, qu'il sait que là, c'est ta maison parce qu'il voit que tu y es de telle heure à telle heure, tu passes sur la route de tel endroit à tel endroit, donc il va garder l'info pour dire "attendez, peut-être mettre une pub à cet endroit"... Il y a déjà tellement d'infos qui peuvent à mon avis transiter comme ça pour induire... un biais de consommation ou quoi que ce soit.»
> (entretien 10 ; 39 min 10 s)

Il est assez fin connaisseur de son propre appareil pour savoir que sa géolocalisation est conservée de manière précise par son téléphone[337], et a visiblement déjà consulté ce menu. Il a également conscience des « biais de consommation » qui peuvent être provoqués par un opérateur de *marketing* au fait de ces informations. Son avis reste assez général, et il ne prétend pas savoir exactement quelles informations circulent au départ de son téléphone (« Il y a déjà tellement d'infos qui peuvent à mon avis transiter comme ça (…) »), quoiqu'il soit largement sensibilisé à la question. En tout état de cause, sa réaction reste intéressante en cela qu'il identifie bien le *smartphone* comme un risque supérieur pour la dissémination d'informations sur les personnes. Plus précisément, et malgré le fait que Linky fît encore l'objet d'une controverse publique au moment de la passation de l'entretien, E16 semble estimer que ce risque de dissémination par Linky est de toute façon forcément subsumé par celui crée par l'utilisation du *smartphone* ; ce dernier est vu par E16 comme un outil beaucoup plus puissant pour l'éventuelle surveillance de ses utilisateurs que tout autre dispositif, en l'espèce Linky.

[337] Précisons que, selon la génération de son iPhone et la manière dont il l'a configuré, il est tout à fait possible que ces données de géolocalisation ne soient pas utilisées à des fins publicitaires, du moins officiellement, voire qu'elles ne soient visibles que localement sur son téléphone.

Il est plus intéressant encore de voir comment certains enquêtés au bagage technique moindre réagissent lorsque je leur explique comment les mécanismes de traçage fonctionnent avec leur *smartphone*. Le cas d'E02 est ici intéressant. Elle exprime à plusieurs reprises une « gêne » assez floue à l'évocation de divers dispositifs, comme Linky ou les serrures connectées, même si elle minimise souvent la chose. Au moment de parler de ses échanges par messagerie (dans son cas, WhatsApp), elle est claire sur le fait que son carnet d'adresse ou le contenu de ses messages doivent rester privés, mais une explication du terme est, comme souvent, nécessaire au moment d'évoquer les métadonnées de ses échanges :

> « JF: C'est tout ça les métadonnées.
> E002: Mmhh... et donc la question c'est si ça me gêne ou pas ?
> JF: Ouais, et si c'est plus ou moins privé ou public ?
> E002: Ca j'aimerais que ça reste privé. Mais pas pour le truc en soi. Parce que j'ai rien spécialement à cacher ou quoi. Mais parce que, malgré toi, tu donnes des infos qui vont servir à... te catégoriser. » (entretien 2 ; 49 min 05 s)

De même, lorsque nous évoquons le fait que son carnet d'adresses ne reste pas seulement en local sur son téléphone, mais est transmis aux serveurs de WhatsApp, elle manifeste à nouveau sa gêne, à plus forte raison dans la mesure où elle a commencé par déclarer que ces informations étaient d'autant plus privées qu'elles étaient en fait les informations de ses contacts eux-mêmes (là où elle estime que son propre numéro de téléphone est plutôt public). Dans les deux cas, la gêne exprimée révèle bien, comme chez E16, une conscience floue de ce que les données produites ou captées via le *smartphone* font ou peuvent aisément faire l'objet d'au moins trois des familles de risques pointées dans la taxonomie de Solove – collecte, traitement, dissémination.

*

Si le *smartphone* est bien identifié comme un important vecteur de risques quant à leur vie privée par ses utilisateurs – voire le plus grand, il n'en est pas moins d'un usage généralisé. 100 % de l'échantillon de personnes interrogées est ainsi équipé, 95 % si l'on prend en compte le fait qu'un enquêté n'était pas encore doté d'un *smartphone* à notre première prise de contact. En France entière à la même époque, 75 % de la population de plus de 12 ans possédait un *smartphone* en 2018, 77 % en 2019[338]. Nous verrons dans la sous-partie « Le chantage du privacy paradox » (page 195) que cette disjonction entre discours et pratiques n'est

[338] *Baromètre du numérique 2021*, *op. cit.*, p. 29

qu’apparemment paradoxale, dans le cas du *smartphone* et plus largement avec les autres *wearables*. En tout état de cause, cette généralisation de l’usage du *smartphone,* qui subsume voire conditionne directement une grande partie des usages numériques contemporaines, questionne l’intérêt qu’a la limite du domicile : pourquoi s’intéresser à la *smart home* si le *smartphone* la transcende ? Quels usages et quelles perceptions spécifiques au logis augmenté prolongent les questionnements auxquels nous invitent déjà en grande partie le *smartphone* à l’ère numérique ?

Chapitre 3 - *SMART HOME* : L'AUGMENTATION DE L'ESPACE PRIVE PAR LA DOMOTIQUE

La question de l'augmentation de l'espace physique par des dispositifs numériques n'est pas neuve : des espaces publics très contrôlés par des moyens numériques existent déjà depuis la deuxième moitié du XXe siècle, dont on a vu qu'ils ont été le terrain d'investigation des *surveillance studies*, en particulier depuis les années 1980, avec la question de la vidéosurveillance particulièrement, mais aussi à travers l'intérêt pour des espaces comme les aéroports. Les individus sont aujourd'hui habitués à interagir avec des systèmes numériques, y compris pour des déplacements plus quotidiens avec les badges des abonnés pour les transports en commun, ou encore avec le paiement par carte bancaire, cas qui renvoient au premier sens de la notion d'habitèle. Mais là où cette mise en surveillance numérique de l'espace public semble avoir trouvé ses limites, soit qu'elle soit acceptée et stabilisée, soit qu'elle soit contestée comme dans le cas du quartier de Quayside à Toronto, celle de l'espace domestique est croissante. Elle émerge par ailleurs dans un contexte où le rapport au numérique et à la production et à la dissémination de données personnelles a été transformé par l'usage aujourd'hui majoritaire du *smartphone*, et qui nous a fait entrer dans le paradigme d'une utilisation ascendante, beaucoup plus personnelle et active des dispositifs numériques, là où l'augmentation numérique des espaces publics était plutôt descendante et imposée. Du point de vue académique, la question de la *smart home* émerge donc plutôt comme une sous-thématique de l'informatisation généralisée du monde.

Au-delà de sa seule dimension scientifique, le terme de *smart home* est également porté par des acteurs économiques majeurs, qui contribuent largement à sa définition à travers la manière dont ils considèrent le marché afférent. Du fait de leur besoin de créer un marché pour écouler leurs produits, ces acteurs accentuent davantage la segmentation thématique entre les différents systèmes pris dans l'IoT. Les industriels insistent davantage sur la nouveauté constituée par l'informatisation et la connexion du domicile, ainsi que sur les usages afférents : il s'agit de créer un sentiment de nouveauté (et de créer un besoin) chez le consommateur. Nous verrons notamment qu'ils tendent à identifier comme spécifiques les usages de l'IoT au domicile, ce qui se retrouve dans leur communication autour des produits domotiques très axée sur la notion de *home* / logis.

I - LA CONSTITUTION DU CHAMP SCIENTIFIQUE DE LA *SMART HOME*

Scientométrie du terme smart home

La notion de la *smart home* ou *smart house* est assez ancienne dans le champ de la recherche académique et spécialement en ingénierie. Les deux termes apparaissent notamment dans un certain nombre de publications des années 2000, première période d'intérêt pour la notion.

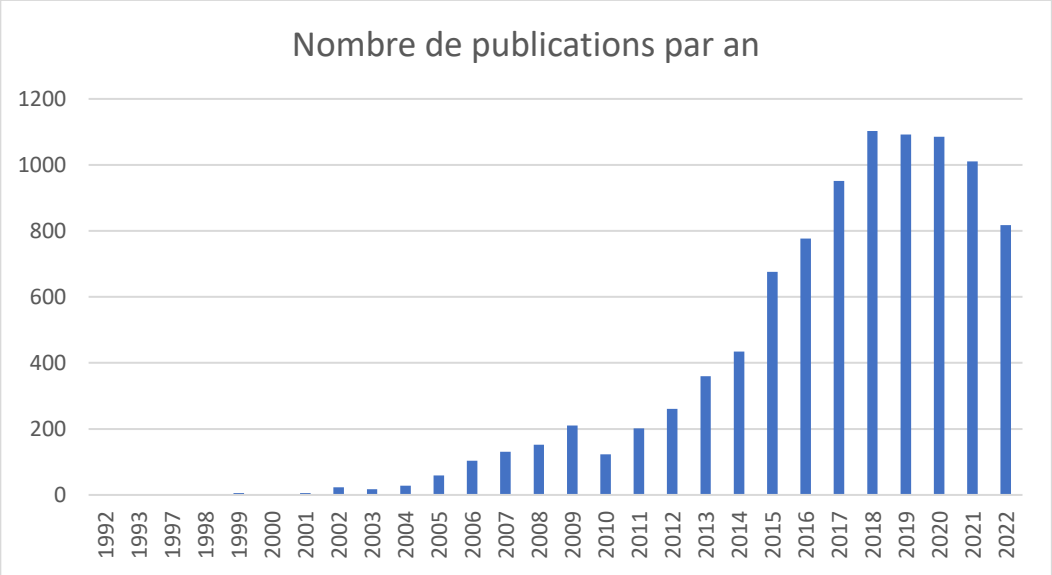


*Figure 15 - Nombre d'occurrences du terme « "*smart home" *» dans une requête portant sur l'ensemble des champs du Web of Science au 8 janvier 2023*

La requête sur le terme « *smart home* » dans le champ « *topic* » renvoie 9 657 pour une requête « *smart home* » sur tous les champs, corps de la publication compris. Pour les années 1992 à 2001, seules 20 publications contiennent « *smart home* » dans leur *topic* selon Web of Science. L'essentiel des publications sont d'ordre technique ou très prospectif, avec une focalisation sur la gestion de la température domestique notamment. Les rares textes plus axés vers les sciences sociales explorent la question du *care*, pour les personnes âgées notamment.

Les années 2002 à 2010 renvoient 847 publications, avec un premier pic de publications en 2009. Elles constituent une première vague d'intérêt académique et ingénieurial. L'écrasante majorité des publications relève toujours de l'informatique ou de l'électronique, mais 31 articles sont spécifiquement liés à la communication et sciences sociales, en plus d'une petite centaine d'articles sur le *care* et/ou les personnes âgées.

L’intérêt pour la thématique ne faiblit plus ensuite, et le nombre de publications augmente constamment à partir de 2011, avec une nette accélération entre 2014 et 2015 (de 434 à 676 publications) qui nous amène à la phase de plateau actuelle de 800 à 1 000 publications annuelles de 2017 jusqu’en 2022. Après un plateau entre 2018 et 2021, l’année 2022 semble marquer le début d’un recul de l’intérêt pour la question. Avec 7 513 publications depuis 2015, la thématique semble néanmoins avoir définitivement émergé.

Pourtant, et malgré quelques publications remarquables, les sciences sociales ne semblent pas avoir massivement participé à cet intérêt, à en croire la base de données de Web of Science. Sur cette dernière période, l’informatique, l’ingénierie et les télécommunications constituent toujours l’écrasante majorité des thématiques. La thématique santé se renforce (532 publications, incluant des doubles-comptes), dont 67 sur la seule gériatrie toujours. Les sciences sociales contribuent toujours à hauteur de quelques dizaines de publications, mais avec cette fois une diversification des domaines concernés, et notamment 16 mentions pour l’architecture, 18 pour les études urbaines et 10 pour la géographie, ce que l’on peut considérer comme un signal faible intéressant.

Un éditorial récent du numéro thématique de la revue scientifique *Communication & management*[339] intitulé « Une maison intelligente pour quoi faire ? Les enjeux des technologies de l'information et de la communication au service de l'habiter » résume adéquatement l’état de la question :

> *« La « maison intelligente » est un terme de plus en plus présent dans le discours social, à l’instar de termes associés comme domotique ou maison connectée. Elle a été présentée, rêvée et fantasmée dans des livres, des films et dans de nombreuses fictions. De ce fait même, elle nourrit des espoirs immenses et des craintes toutes aussi démesurées. Entre le fantasme d’objets qui réaliseraient les désirs des individus avant même qu’ils ne les aient formulés et son pendant pessimiste qui voit les objets prendre le*

[339] Dont on peut signaler que les éditeurs sont les premiers à relever qu’il pourrait sembler surprenant que leur revue consacre un numéro à cette thématique dans les pages liminaires du numéro : « De prime abord, nos lecteurs pourraient se demander quel est le rapport entre la thématique de la « maison intelligente » et la ligne éditoriale de la Revue COMMUNICATION & MANAGEMENT. L’intérêt porté à cette thématique réside à la fois dans la conception-modélisation des technologies de l’information et de la communication qui doivent être mobilisées pour être « au service de l’habiter » mais aussi à l’égard des multiples enjeux éthiques que soulèvent ces systèmes décisionnels et plus largement les démarches d’innovation. » *in* E. OIRY et L. VERLAET, « Éditorial - Une maison intelligente pour quoi faire ? Les enjeux des technologies de l’information et de la communication au service de l’habiter », *Communication & management*, vol. 17, nº 1, ESKA, 2020, § 2 (en ligne : https://www.cairn.info/revue-communication-et-management-2020-1-page-3.htm ; consulté le 18 avril 2022)

contrôle des individus et rendre leur vie privée visible à tous sans qu'ils puissent s'y opposer, la « maison intelligente » fait l'objet de débats passionnés. »

Cependant, l'expression *smart home* ne recouvre pas entièrement l'ensemble des pratiques que nous abordons dans cette thèse. Elle renvoie essentiellement aux augmentations du logis, alors même que de nombreux objets connectés présentés comme nomades, au premier rang desquels le *smartphone*, s'y inscrivent également. L'expression d'Internet of Things est en ce sens plus englobante.

L'Internet of Things appliqué au domicile

Dans les années 1990 encore, beaucoup de projections envisageaient la montée en puissance d'une informatique multimédia et interactive de plus en plus « ambiante » ou « pervasive », mais principalement à travers le mobilier urbain, les murs, ou des drones plus ou moins sophistiqués. C'était par exemple l'intuition de William J. Mitchell dans *City of Bits*. Pour l'architecte et urbaniste qu'était Mitchell, le bâti devait devenir une « interface avec le réseau : des quais de chargement pour les bits »[340]. Mitchell faisait l'hypothèse que l'imbrication réciproque des bâtiments, de l'informatique et de la robotique irait croissant, et même jusqu'à une certaine forme d'hybridation : « Claviers et souris vont cesser d'être les seules zones de collecte de bits, les capteurs seront partout. Écrans et effecteurs[341] se multiplieront. Au bout du compte, les bâtiments deviendront des interfaces informatiques, et les interfaces informatiques des bâtiments. »[342] Rappelons que la première édition de *City of Bits* date de 1996, c'est-à-dire onze ans avant la sortie du premier *smartphone* à succès, l'iPhone d'Apple. Cette hypothèse de Mitchell, si elle s'est matérialisée localement, ne s'est donc globalement pas vérifiée. Plutôt que d'augmenter directement l'espace, l'informatique s'est plutôt concentrée dans un dispositif, le *smartphone*, qui est aujourd'hui la principale interface informatique avec laquelle nous interagissons. La prémisse selon laquelle l'informatique serait de plus en plus présente dans nos spatialités s'est bel et bien vérifiée, mais selon des modalités que n'avaient pas anticipées Mitchell à une époque où la microinformatique et la

[340] « *Buildings and parts of buildings must now be related not only to their natural and urban contexts, but also to their cyberspace settings. Increasingly, they must function as* ***network interfaces – loading docks for bits****.* » W. J. MITCHELL, *City of bits*, *op. cit.*, p. 104

[341] Un effecteur, ou *effector* en anglais, désigne la partie d'un robot agissant sur son environnement pour effectuer une opération spécifique, comme une pince au bout d'un bras articulé qui peut saisir des objets. Le sens ne s'étend pas aux éléments robotiques d'usage général, comme des roues qui permettent au robot de se déplacer lui-même.

[342] « *Keyboards and mouse pads will cease to be the only bit-collection zones; sensors will be everywhere. Displays and effectors will multiply. In the end, buildings will become computer interfaces and computer interfaces will become buildings.* » W. J. MITCHELL, *City of bits*, *op. cit.*, p. 105

miniaturisation des batteries étaient encore limitées, et où les réseaux s'appuyaient sur une couche matérielle reposant surtout sur des câbles et presque pas sur les radiofréquences[343]. Ce, alors que les enjeux de connectivité et d'autonomie étaient et sont encore fondamentaux pour le développement de ces dispositifs portables[344]. Il faut également signaler que Mitchell avait malgré tout la bonne intuition d'anticiper que c'était bel et bien l'ordinateur, en l'occurrence miniaturisé et portable, qui serait l'outil déterminant de l'IoT – là où les réflexions initiales sur l'IoT accordaient sans doute une trop grande importance à la technologie RFID[345].

Plutôt que de partir conceptuellement d'un espace territorial auquel viendrait s'adjoindre des aménités numériques, le designer Adam Greenfield est plutôt parti des objets et dispositifs numériques et a interrogé leur déploiement toujours plus fin dans nos espaces quotidiens. Il évoque un certain nombre d'expressions existantes pour décrire la *numérisation* du monde : *ubiquitous computing*, informatique ambiante, informatique physique, médias tangibles… mais préfère les subsumer sous le terme « ubimédia »[346], proche de l'expression de « réseaux ubiquitaires » utilisée au Japon et en Corée[347]. Comme Mitchell, Greenfield entend ainsi décrire une informatique connectée hors des points d'accès à Internet habituels que sont l'ordinateur ou le téléphone. Le préfixe *ubi* renvoie à la notion d'ubiquité[348], et média emprunte

[343] Il faut en outre ajouter que Mitchell anticipait également une partielle « fin de l'espace » matériel au profit de la numérisation / dématérialisation d'espaces existants à travers ce qu'il appelait « *soft city* », et auquel il consacre un chapitre dédié à voir comment les vitrines des institutions deviennent leur page web plutôt que leurs sièges, que la connexion prendrait le pas sur la coprésence, que les « communautés » s'appuieraient désormais plutôt sur des espaces en ligne que sur le voisinage ou le quartier, qu'on recourrait à la télémédecine plutôt qu'à une visite à l'hôpital, etc.

[344] S. SENEVIRATNE *et al.*, « A Survey of Wearable Devices and Challenges », *IEEE Communications Surveys Tutorials*, vol. 19, nº 4, 2017, p. 2573-2620

[345] On peut en trouver un exemple chez B. BENHAMOU, « L'internet des objets », *op. cit.*. Il ne s'agit pas ici de minimiser l'importance de la RFID, évidemment très présente dans nos vies quotidiennes et même centrale dans la logistique contemporaine. Simplement, le caractère passif des puces RFID simples ne me semble plus justifier aujourd'hui de les tenir au même niveau que les véritables ordinateurs que constituent les objets connectés, à la fois capables de traitements de données et de pilotage d'actions : il y a entre ces deux versants historiques de la notion d'Internet des objets une différence de nature qui ne me semble plus pouvoir être subsumée sous le même terme. Stéphane Bortzmeyer signale d'ailleurs que la question d'inclure les puces RFID dans le champ de l'IoT a été contesté très tôt : « C'est le consortium privé Auto-Id qui a popularisé ce terme à la fin des années 1990, pour de simples raisons marketing. À l'époque, c'était limité à des étiquettes RFID n'ayant qu'une connexion très limitée, sans rapport avec l'Internet. Certains ont suggéré de réserver le terme d'« Internet des Objets » aux objets connectés en IP mais ces appels à la rigueur terminologique n'ont en général que peu d'impact. » S. BORTZMEYER, « RFC 8576: Internet of Things (IoT) Security: State of the Art and Challenges », sur *Blog de Stéphane Bortzmeyer*, avril 2019 (en ligne : https://www.bortzmeyer.org/8576.html ; consulté le 28 mars 2021)

[346] A. GREENFIELD, *Every[ware]: la révolution de l'ubimedia*, C. Fiévet (trad.), Limoges (France), FYP Éditions, 2007, p. 8

[347] B. BENHAMOU, « L'internet des objets », *op. cit.*, § 3

[348] En toute rigueur, *ubi* est en latin un simple adverbe de lieu, désignant la localisation. *Ubicumque* est l'adverbe signifiant « partout ». Par élision, *ubi* est souvent employé pour signifier « qui existe partout à la fois », comme dans le terme français « ubiquité ». On retrouve par exemple cette forme dans le nom de la société de logiciels Ubisoft. Voir F. GAFFIOT, « Ubi », dans *Dictionnaire latin français*, Paris (France), Hachette, 1934, p. 1620-1621 (en ligne : https://www.lexilogos.com/latin/gaffiot.php?q=ubique)

à la notion de multimédia, alors dominante, et qui renvoie à la pluralité des médias accessibles à travers une même interface informatique (l'ordinateur notamment). Greenfield insiste avant tout sur le caractère ubiquiste des technologies numériques à venir : « Avec l'ubimédia, les vêtements, les pièces de la maison et les rues deviennent des lieux de traitement et de médiation. Les objets domestiques, qu'il s'agisse d'une cabine de douche ou d'un pot de café, sont repensées comme autant d'endroits où l'on peut rassembler des informations, les prendre en compte ou interagir avec elles. Et tous les rites familiers de la vie quotidienne – notre manière de nous réveiller, de nous rendre au travail, de faire les courses – sont revus en une danse complexe mettant en jeu des informations sur nous-mêmes, l'état du monde extérieur et les options dont nous disposons à tout moment »[349]. Chez Greenfield, qui écrit une décennie après Mitchell, on trouve déjà beaucoup plus d'attentes reposant sur les objets plutôt que sur le bâti – ou sur le transfert pur et simple d'usages dans le « cyberespace ».

Dans un ouvrage de synthèse sur l'IoT en 2019, Jabraeil Jamali *et al.* présentent la notion de *smart home* comme un cas d'application du concept d'Internet des objets : ils en font même le premier cas étudié dans le chapitre qu'ils dédient aux usages de l'IoT. « Le terme "*smart home*" désigne le fait d'intégrer des automatismes dans une résidence privée, où des capteurs et mécanismes sont connectés à un système intelligent. Il s'agit de la base pour le contrôle automatisé et global du foyer. Un maximum de données doivent être collectées pour un fonctionnement optimal. »[350] Là où Greenfield parlait d'« *ubi*media », Jabraeil Jamali *et al*. utilisent plutôt l'adjectif déterminant anglais[351] « *any* » (voir leur schéma Figure 16), mettant ainsi en avant la pluralité virtuellement infinie des usages possibles de l'IoT plutôt que la dissémination de l'informatique (*ubi*). Cette logique de dissémination spatiale de l'informatique reste présente dans cette approche de l'IoT, puisque sont concernés à la fois *any device*, *any service* ou encore *any network*, et que la connectivité de l'IoT est supposée possible *anywhere*. Le fait que Jabraeil Jamali *et al*. insistent particulièrement sur la *smart home* parmi l'infinité des espaces potentiellement concernés et connectés dans l'IoT est donc d'autant plus révélateur de l'importance du logis augmenté au sein de l'IoT.

[349] A. GREENFIELD, *Every[ware]*, *op. cit.*, p. 8
[350] M. A. JABRAEIL JAMALI *et al.*, « Some Cases of Smart Use of the IoT », dans M. A. Jabraeil Jamali *et al.* (éd.), *Towards the Internet of Things: Architectures, Security, and Applications*, Cham, Springer International Publishing, 2019, p. 85
[351] La grammaire française n'emploie pas le terme d'adjectif déterminant, le terme rend ici le *determiner* anglais, qui peut renvoyer à un adjectif dans cette langue.

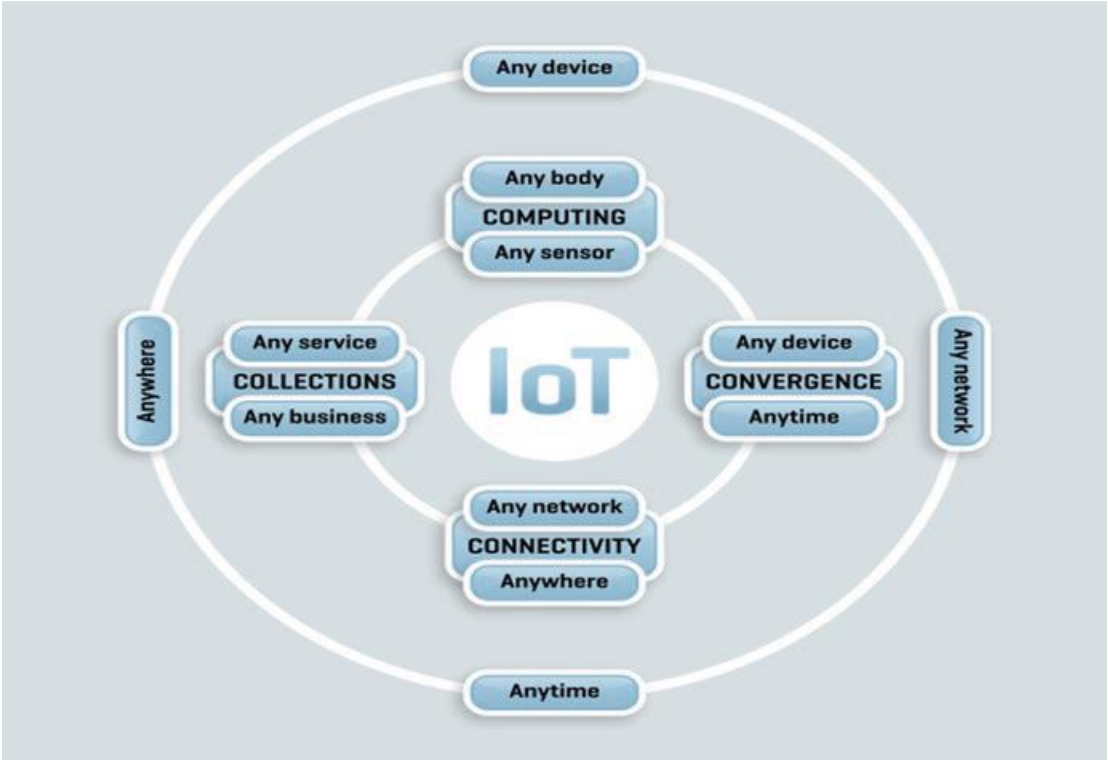


Figure 16 - "Les concepts en A et en C dans l'IoT" (Jabraeil Jamali et al., 2019)

En tout état de cause, et avant même le début des formalisations théoriques de la décennie 2010, des recherches appliquées avaient déjà été mises en œuvre en préfiguration de la notion de *smart home*. Dans le passage « *Requiem for a home* », de l'introduction de *The Age of surveillance Capitalism*, Zuboff décrit ainsi une expérience menée à Georgia Tech, la « *Aware home* », qui « malgré tout son appareillage numérique, devait être une incarnation moderne du « foyer » compris selon l'ancienne convention qui en fait le sanctuaire privé des personnes vivant entre ses murs » (trad. pers.)[352]. Il s'agit d'une maison-laboratoire de 468 m² bâtie sur trois niveaux, inaugurée en 1998, et dans laquelle la logique était d'introduire des capteurs, jusque dans les objets du quotidien, afin d'en monitorer l'usage. L'IoT en était alors à ses prémisses techniques, mais cette expérience portait déjà la *smart home* en germe. Ses concepteurs prônaient la capacitation et la maîtrise par les résidents de leur logis, en particulier leurs réseaux électrique et d'adduction d'eau, ou leurs appareil électroménagers. Plus particulièrement, et dans la ligne de la plupart des recherches initiales effectuées au début des années 2000, il s'agissait essentiellement d'accompagner par la technologie des personnes d'âge avancé à rester vivre à domicile (voir la sous-partie « Scientométrie du terme *smart*

[352] « *(…) for all its digital wizardry, the Aware Home would take its place as a modern incarnation of the ancient conventions that understand « home » as the private sanctuary of those how dwell within its walls* » S. ZUBOFF, *The Age of Surveillance Capitalism*, New York (États-Unis), PublicAffairs, 2019, p. 5

home », p. 157)[353]. Pour Zuboff, le projet a été mené à son terme industriel grand public par des sociétés comme Nest en termes de fonctions et d'usage. Il est d'ailleurs à signaler que la *Aware Home* est toujours en activité, et qu'elle est également utilisée par des industriels. Nest et Amazon sont notamment partie prenante de l'axe de recherche « *connected living infrastructure* », par exemple autour de la question de l'interopérabilité des objets connectés de différentes marques – l'application Wink App semble être un exemple de recherche appliquée important dans ce domaine pour *Aware Home*[354].

Pour autant, Zuboff insiste surtout sur le fait que les idéaux initiaux d'encapacitation des utilisateurs, notamment des moins autonomes physiquement, ont fini par être pris dans et même obérés par la logique du capitalisme de surveillance, au détriment de la maîtrise sur les données et leur exploitation. Ce dernier point est incontestable lorsque des dispositifs et services tiers impliquant des serveurs tiers de grandes entreprises comme Amazon sont utilisés, les données brutes n'étant plus disponibles pour l'utilisateur désormais dépendant du prestataire choisi. Je ne suis en revanche pas complètement Zuboff dans sa critique sur la moindre encapacitation des utilisateurs. Il faut ici distinguer la maîtrise sur la technologie et les usages qui en sont faits. Les utilisateurs n'ont en effet pas accès à l'ensemble de l'infrastructure technique et ne sont donc pas à même d'y faire preuve d'une totale « expertise »[355], et *ipso facto* découragés d'en développer une. Ils ne peuvent et doivent pas moins développer « aptitude, savoir-faire » voire « habileté »[356] dans l'utilisation des outils de la *smart home*. En outre, l'utilisation de ces outils augmente leur répertoire d'actions, ce qui est d'autant plus prégnant pour les personnes en situation de handicap. Quoiqu'elle soit limitée, il y a donc une véritable encapacitation des utilisateurs de ces technologies. En réalité, cette lecture critique que fait Zuboff de la *Aware Home* s'inscrit dans sa grille de lecture plus générale de l'informatisation du monde et du capitalisme de surveillance, bien résumée par Christophe Masutti : « (…) elle finit par constater que les promesses du techno-capitalisme qu'elle avait identifiées dans ses travaux précédents, viennent à se solder aujourd'hui par un envahissement oppressif de nos comportements, là où, au contraire, les technologies de l'information étaient censées nous

[353] « About the Aware Home Research Initiative - Georgia Institute of Technology », sur *Aware Home Research Initiative*, s. d. (en ligne : https://awarehome.gatech.edu/about-aware-home-research-initiative ; consulté le 24 avril 2022)
[354] B. D. JONES, « The Georgia Tech Aware Home - Supporting Research, Partnerships, Students, and Beyond », Atlanta (États-Unis), 28 mai 2019 (en ligne : https://awarehome.gatech.edu/sites/default/files/documents/AwareHome_slides.pdf ; consulté le 24 avril 2022)
[355] M. BUTLEN et J. DOLZ, « La logique des compétences : regards critiques », *Le francais aujourd'hui*, vol. 191, nº 4, Armand Colin, 23 décembre 2015, § 3 (en ligne : https://www.cairn.info/revue-le-francais-aujourd-hui-2015-4-page-3.htm)
[356] *Id.*

émanciper par effet d'amplification démocratique. »[357] Le discours de Zuboff doit donc être lu comme relevant d'un écart à un idéal déçu quant aux possibilités offertes par l'IoT appliqué au logis, sans aller jusqu'à être compris comme une totale incapacitation des acteurs enfermés dans un écosystème de logiciels et de dispositifs techniques sur lesquels ils n'auraient aucune prise.

La question de la maîtrise des données des *smart homes* par leurs habitants n'en soulève pas moins la question de la circulation des données produites par les dispositifs de l'IoT domestique, selon les modalités d'atteinte à la vie privée que nous avons plus largement identifiées. Du fait de leur circulation, il y a d'abord une dissémination en direction des différentes entreprises et services collectant les données afin, d'une part, d'offrir un service à leurs utilisateurs et, d'autre part, de générer un « surplus comportemental » dans la logique du capitalisme de surveillance. Là où nous avions avancé que cette approche était peu explicitement spatiale de prime abord (voir « Une approche peu explicitement spatiale de la circulation des données », p. 88), l'intérêt de la *smart home* est de montrer de façon très explicite en quoi il y a franchissement d'une frontière, celle du mur de la maison, là où la captation des pratiques strictement effectuées en ligne semblent sans doute moins évidemment attentatoires à la vie privée. Il s'agit d'ailleurs très probablement de la raison pour laquelle la *Aware Home* est le tout premier exemple que développe Zuboff dans son ouvrage : tout en n'étant pas le plus impressionnant en termes de conséquences pour les individus, il signale la mise-en-jeu même du logis en tant que type de lieu emblématique et absolu du privé (pour rappel, l'auteure parle de « sanctuaire », se plaçant ainsi dans le registre du sacré).

Plus classiquement, et prolongeant pour ainsi dire la pratique de dissémination des données, la question de la brèche (*breach*, chez Solove, voir Tableau 2, p. 63) est aussi beaucoup traitée dans la littérature sur l'IoT domestique. Pour Woodrow Hartzog, professeur de droit et d'informatique à l'université de Harvard, « L'Internet des objets fournit aux acteurs malintentionnés des voies nouvelles pour accéder à des informations sensibles et nous surveiller jusque dans nos maisons »[358]. Ce risque de piratage, s'il est inhérent à tout système informatique, est identifié comme étant plus grand encore pour l'IoT, et a même fait l'objet d'une RFC dédiée, la 8576, intitulée « *Internet of Things (IoT) Security: State of the Art and Challenges* »[359].

[357] C. MASUTTI, *Affaires privées: aux sources du capitalisme de surveillance*, Caen (France), C&F éditions, 2020, p. 390

[358] « *The Internet of Things gives malicious actors many new paths to accessing sensitive information and surveilling us in our homes.* » W. HARTZOG, *Privacy's Blueprint: The Battle to Control the Design of New Technologies*, Cambridge (États-Unis), Harvard University Press, 2018, p. 93

[359] O. GARCIA-MORCHON, S. KUMAR et M. SETHI, *Internet of Things (IoT) Security: State of the Art and Challenges*, Internet Engineering Task Force, 2019

Stéphane Bortzmeyer, dans un blog décrivant cette RFC, commence d'ailleurs par rapport qu'« Une blague très courante dit que, dans IoT (*Internet of Things*, l'Internet des Objets), le S veut dire sécurité… C'est peu dire que la sécurité de l'IoT est mauvaise. »[360] Ce risque tient notamment à la nature des données pouvant être compromises par des objets connectés, dont les capteurs peuvent par exemple donner accès visuellement ou phoniquement aux espaces privatifs[361]. Les auteurs de la RFC 8576 retiennent pour leur étude de cas de la sécurité dans l'IoT un système de gestion d'un bâtiment[362], ce qui va dans le sens que nous avons identifié d'un lien fort entre l'IoT et la gestion de l'espace domestique – quoique le cas concerne un bâtiment générique, qui pourrait aussi être par exemple un immeuble de bureaux. La RFC confirme nettement le propos d'Hartzog en identifiant onze types de menaces pesant sur l'IoT, dont neuf mettent en jeu la vie privée de leurs utilisateurs, six l'intégrité du réseau dans lequel les objets sont intégrés, et trois l'industriel ou le vendeur de l'objet, et trois l'utilisabilité de l'objet lui-même (voir Tableau 6).

[360] S. BORTZMEYER, « RFC 8576: Internet of Things (IoT) Security: State of the Art and Challenges », *op. cit.*

[361] Un exemple étonnant a par exemple été donnée par les journalistes du site web Reflets.info, qui ont informé les autorités ukrainiennes du fait que les caméras embarquées des voitures de police étaient facilement accessibles via Internet et pouvaient compromettre des informations tactiques et stratégiques importantes dans le cadre du conflit avec la Russie en 2022. Anon., « Reflets s'invite par hasard dans les voitures de police ukrainiennes », *Reflets.info - Journal d'investigation en ligne et d'information-hacking*, 2 mars 2022 (en ligne : https://reflets.info/articles/reflets-s-invite-par-hasard-dans-les-voitures-de-police-ukrainiennes ; consulté le 2 mars 2022)

[362] « *In this document, we consider a Building Automation and Control (BAC) system to illustrate the lifecycle and the meaning of these different phases. A BAC system consists of a network of interconnected nodes that performs various functions in the domains of Heating, Ventilating, and Air Conditioning (HVAC), lighting, safety, etc. The nodes vary in functionality, and a large majority of them represent resource-constrained devices such as sensors and luminaries.* » O. GARCIA-MORCHON, S. KUMAR et M. SETHI, *Internet of Things (IoT) Security*, *op. cit.*

Tableau 6 - Typologie synthétique des risques de l'Internet of Things d'après la RFC 8576

	Description rapide	Utilisabilité de l'objet	Risque pour l'industriel	Risque pour l'utilisateur	Risque pour le réseau
Logiciel vulnérable	Le logiciel de l'objet peut être mal pensé ou comporter des bugs			x	x
Risque pour la "privacy"	L'IoT permet d'inférer et disséminer des informations sur les individus			x	
Duplication des objets	Un objet peut être compromis dès sa production (ex: inclure une *backdoor*)		x	x	x
Substitution des objets	Un objet peut être interverti lors de son installation (ex: limiter les coûts avec un équivalent moins cher)		x		
Écoute clandestine	Les communications de l'objet avec d'autres objets ou un serveur sont interceptées			x	x
Attaque de l'homme-du-milieu	Un tiers peut se faire passer pour un intermédiaire légitime dans un échange sur un réseau		x	x	
Attaques contre le système d'exploitation	Compromission de l'objet pendant sa phase d'utilisation (ex: inférer la présence des personnes à leur domicile)	x		x	
Extraction d'informations privées	Accéder physiquement à un objet connecté pour le compromettre			x	x
Attaque du routage	Captation des paquets de données réseau en exploitant les propriétés de TCP/IP			x	x
Élévation de privilèges	Obtenir malicieusement des accès plus importants que prévu sur l'objet	x		x	
Attaque par déni de service	Saturer le réseau pour empêcher l'objet de communiquer normalement	x			x

En tout état de cause, cet intérêt académique singulier pour la *smart home* dans le champ de l'IoT me semble révéler une nouvelle facette d'une prise de conscience qui pouvait sembler achevée : non seulement Internet n'a pas entraîné de fin de l'espace pour les territoires urbains ou encore d'effacement des échelles intermédiaires entre l'individu et le Monde, mais il revivifie d'une certaine manière la prise en compte du logis comme type spatial et comme échelle. Il confirme également que le privé est très fortement mis en jeu par le déploiement de l'IoT, du fait de l'intrication croissante des objets connectés dans le quotidien et des risques spécifiques à ce type de systèmes informatiques communicants.

II - LE MARCHE DE LA *SMART HOME*

Cette évolution dans le champ académique est intéressante à deux égards : dans l'histoire technique et commerciale de l'informatisation, on peut la voir comme un prolongement attendu de la diffusion progressive et à une échelle de plus en plus fine de l'informatisation du monde. De ce point de vue, le processus est assez comparable à l'émergence et de à diffusion de l'ordinateur personnel (PC, *personal computer*) depuis les premiers ordinateurs commerciaux dits *mainframe*, à destination des entreprises et des administrations, comme l'UNIVAC de Remington Rand pesant 13 tonnes (1951)[363]. Du point de vue du discours sur l'espace, en revanche, cette évolution est plus étonnante. Nous sommes, pour ainsi dire, passés de l'échelle mondiale, qui est l'horizon spatial d'Internet, à l'échelle individuelle, avec l'émergence du *smartphone* et plus largement des *wearables*. On aurait pu penser que l'IoT n'aurait à son tour d'intérêt qu'à ces deux échelles[364] : utilisable *anytime, anywhere,* sur *any device* ou *any network,* plus indépendant du bâti que ne l'envisageait un penseur comme William Mitchell, pourquoi remettrait-il en avant des échelles intermédiaires et des espaces topographiques comme le logis ? Nous allons voir qu'une logique et des stratégies commerciales puissantes sont ici mises en œuvre que l'on avait pu déjà observer avec

[363] C. MASUTTI, *Affaires privées*, *op. cit.*, p. 48

[364] Pour Boris Beaude, si l'on excepte les tentatives d'États cherchant à instaurer des intranets nationaux et la logique d'hypercentralité des géants du numérique, Internet en général s'envisage d'abord plutôt à ces deux échelles : « (…) Internet rencontra le succès escompté et se diffusa dans le Monde entier, plus vite que ne le fit toute autre technologie de communication. L'adéquation entre le potentiel technique d'Internet et les attentes individuelles fut si puissante, que les usages se développèrent à un rythme inédit. Aussi, la croissance d'Internet fut si soudaine que son emprise sur le Monde contemporain s'est faite plus rapidement que notre capacité à en identifier l'influence sur nos pratiques. » B. BEAUDE, *Les fins d'Internet*, *op. cit.*, p. 12

la mise en produit de la ville comme *smart city*, dont la *smart home* procède à son tour comme mise en produit du logis.

Le ruissellement conceptuel de la smart city

Par rapport à la thématique de la *smart home*, celle de la *smart city* est intéressante en tant que préalable à la fois historique et scalaire. Historique, car le succès de la *smart city* précède celui de la *smart home* : l'émergence de la « ville intelligente » était déjà annoncée en 1992 à la fin de l'ouvrage *L'informatisation des villes* de Gabriel Dupuy[365], avant que la *smart city* ne soit activement promue dans les années 1990 et 2000 par des entreprises comme Cisco ou IBM, et que le terme finisse par s'imposer dans la littérature scientifique à partir de 2006[366]. Scalaire, car les technologies dites de *smart city* sont déployées à une échelle plus large, tout en entretenant une relation d'interspatialité avec celles de la *smart home*.

Comme la *smart home* à sa suite, la définition de la *smart city* présente l'intérêt d'être avant tout émique, et plus précisément à vocation commerciale. Selon Emmanuel Eveno dans un article de 2018 dans la revue *Quaderni*, « [elle] ne semblait rien devoir, jusqu'à il y a peu, aux mondes académiques tandis qu'[elle] était souvent perçu[e] comme ayant été imposé[e] par des acteurs économiques en quête de nouveaux marchés »[367]. Qu'on parle de *smart city* ou de « ville intelligente », Eveno n'en affirme pas moins que ce concept d'abord plutôt commercial reste assez signifiant, faute de mieux, pour être utilisé y compris par les chercheurs, et qu'aucune « autre expression, aussi synthétique et attractive, puisse aujourd'hui s'imposer »[368]. Il est en effet difficile de définir nettement ce qu'est une ville intelligente ou *smart*. Dans sa thèse sur la *Politique des données urbaines*, Antoine Courmont décrit ainsi « la ville intelligente [comme] une notion floue aux définitions multiples, selon que l'accent soit mis sur les technologies, les acteurs ou le gouvernement. On peut toutefois la définir de manière générique comme l'usage généralisé de données numériques pour rationaliser la planification et la gestion

[365] G. DUPUY, *L'informatisation des villes*, Paris (France), Presses universitaires de France, 1992 cité par S. BERNARDIN et G. JEANNOT, « La ville intelligente sans les villes ? », *Réseaux*, vol. 218, nº 6, La Découverte, 28 novembre 2019, § 1 (en ligne : https://www.cairn.info/revue-reseaux-2019-6-page-9.htm ; consulté le 3 mai 2022)
[366] M. DE JONG *et al.*, « Sustainable–smart–resilient–low carbon–eco–knowledge cities; making sense of a multitude of concepts promoting sustainable urbanization », *Journal of Cleaner Production*, vol. 109, 16 décembre 2015, p. 25-38 (en ligne : https://www.sciencedirect.com/science/article/pii/S0959652615001080 ; consulté le 3 mai 2022) cité par S. BERNARDIN et G. JEANNOT, « La ville intelligente sans les villes ? », *op. cit.*
[367] E. EVENO, « La Ville intelligente : objet au cœur de nombreuses controverses », *Quaderni. Communication, technologies, pouvoir*, nº 96, Les éditions de la Maison des sciences de l'Homme, 15 mai 2018, § 2 (en ligne : http://journals.openedition.org/quaderni/1174 ; consulté le 12 février 2021)
[368] E. EVENO, « La Ville intelligente », *op. cit.*

des villes »[369]. Cette production de données résulte de « la dissémination croissante des technologies de l'information et de la communication dans l'espace urbain » - l'auteur parle aussi d'informatique devenue « pervasive » dans « l'ère numérique »[370]. La grille de lecture que nous avons appliqué à la *smart home* comme déploiement de l'IoT dans le logis s'applique assez bien aussi à la *smart city* comme déploiement de l'IoT à l'échelle du quartier, de la ville, voire de la métropole. D'un point de vue technique, *smart city* et *smart home* ne diffèrent pas. Cette grille de lecture, si elle n'épuise pas tout le sens que peut embrasser la notion de *smart city*, n'en est pas moins un angle d'approche pertinent parmi les trois directions identifiées par Courmont.

Sur la base d'un travail de thèse consacré à la fabrique de la *smart city*, Ornella Zaza présente plus nettement encore cette dernière comme étant fondamentalement commerciale. D'après son enquête auprès de fonctionnaires de la ville de Paris et de techniciens de l'entreprise Cisco ainsi que de diverses *start-up* impliquées dans l'aménagement de la place de la Nation à Paris en 2015 sur la base d'outils tels que des caméras associées à des logiciels de reconnaissance d'images, des micros ou encore des capteurs de pollution, elle conclut que « L'espace public [est pour les acteurs de l'urbaménagement publics et privés] comme [un] marché à investir »[371]. La participation à la démonstration technologique de la place de la Nation avait, notamment pour les *start-up*s impliquées, pour principal intérêt de s'intégrer à un marché dominé jusque-là par les architectes, urbanistes et autres promoteurs immobiliers[372]. Jean-Marc Offner parle plus largement de ces acteurs comme de « nouveaux entrants » (sans doute faudrait-il désormais parler de « nouveaux entrés »), dans une approche moins strictement axée par la question de l'offre commerciale : en effet, au-delà de leur intégration au marché de la fabrique urbaine, ils « apporte[eraie]nt par ailleurs leurs capacités d'innovation dans un

[369] A. COURMONT, *Politiques des données urbaines : ce que l'open data fait au gouvernement urbain*, thèse de doctorat en science politique, Paris (France), Institut d'études politiques de Paris, 2016, p. 22
[370] *Ibid.*, p. 21
[371] O. ZAZA, « La mesure de l'humain », *Les Cahiers de la recherche architecturale urbaine et paysagère*, nº 3, Ministère de la culture, 26 décembre 2018, § 32 (DOI : 10.4000/craup.1153)
[372] « Le cas de cette startup était analogue à ceux d'autres startups et entreprises qui ont participé au démonstrateur place de la Nation : leur but était de tester des nouveaux produits, pour qu'ils soient ensuite vendables sur le marché. Si la numérisation de l'espace public devenait un secteur de marché, alors les startups et entreprises du numérique rentraient dans le jeu d'acteurs de l'aménagement urbain, qui auparavant était presque exclusivement composé d'architectes, urbanistes, paysagistes, agents publics, associations, promoteurs immobiliers, aménageurs, et, parfois, citadins. » *Ibid.*, § 37

champ technico-politique, l'urbanisme, marqué par un fort conservatisme des doctrines et des instruments »[373].

D'un point de vue technologique à présent, *smart city* et *smart home* relèvent en tout cas d'une même logique d'informatisation des espaces par le biais d'ordinateurs et de capteurs connectés entre eux, autrement dit du déploiement de l'IoT. La proximité sémantique des deux expressions est, en ce sens, parfaitement justifiée. Il y a en outre une relation pleinement interscalaire entre ces deux phénomènes, comme nous l'avons par exemple vu à travers l'utilisation des sonnettes connectées Doorbell de particuliers comme un véritable réseau de vidéosurveillance par les services de police de centaines de municipalités aux États-Unis (voir « L'espace sous surveillance: plus de refus possible ? », p. 78). En France, le cas des compteurs connectés Linky, qui font contribuer chaque foyer équipé à l'information du réseau de fourniture d'électricité (*smart grid*), en est également un bon exemple, quoique l'installation des compteurs Linky ne relève pas d'initiatives individuelles des usagers / consommateurs, et que les autorités municipales ne soient pas ici directement associées.

Ces exemples de relation interscalaire entre *smart city* et *smart home* ne doivent cependant pas être considérés comme une nouvelle norme : les deux échelles restent largement indépendantes, et Linky est d'ailleurs en France le seul exemple d'intégration à une échelle plus large de dispositifs domotiques connectés. S'appuyant sur l'exemple d'une grande métropole française, Jeannot et Maghin concluent ainsi que « l'intégration des données [des individus par l'échelon municipal] n'apparaît pas impossible, mais elle est bien difficile »[374]. Le fonctionnement très compartimenté des différents services municipaux et métropolitains explique selon eux largement cet état de fait, à rebours des promesses commerciales d'utiliser l'informatique pour intégrer l'ensemble des outils des administrations urbaines dans une même interface unique. Courmont met également en avant la complexité technique d'une « stratégie d'homogénéisation » au sein d'une même « plateforme » des données produites par différents services, sous différents formats et sous différentes licences, sans même parler d'intégrer des données produites hors du contrôle direct des agents municipaux[375]. Les difficultés dans la mise en œuvre de l'interopérabilité des données entre différents services semblent donc être le

[373] J.-M. OFFNER, « La smart city pour voir et concevoir autrement la ville contemporaine », *Quaderni. Communication, technologies, pouvoir*, nº 96, Les éditions de la Maison des sciences de l'Homme, 15 mai 2018, § 11 (en ligne : https://journals.openedition.org/quaderni/1172#tocto1n3 ; consulté le 14 février 2022)
[374] G. JEANNOT et V. MAGHIN, « La ville intelligente, de l'administration à la gouvernance », *Réseaux*, vol. 218, nº 6, La Découverte, 28 novembre 2019, § 98 (en ligne : https://www.cairn.info/revue-reseaux-2019-6-page-105.htm ; consulté le 7 octobre 2021)
[375] A. COURMONT, *Politiques des données urbaines*, *op. cit.*, p. 288

principal frein au développement d'une ville pleinement « intelligente » s'appuyant sur des remontées d'information par les résidents ou des objets connectés à l'échelle la plus fine.

Carte 2 - Le quartier de Quayside (Toronto) au redéveloppement convoité par Sidewalk Labs sur la mode de la smart city (source : Waterfront Toronto, 2022)

L'exemple le plus éclatant du lien possible entre *smart city* et *smart home* n'en reste pas moins le projet avorté de la filiale d'Alphabet, Sidewalk Labs, de connecter entièrement le quartier en rénovation urbaine de Quayside à Toronto (voir p. 85). Officialisé en octobre 2017, l'accord entre la ville et Sidewalk Labs portait sur l'une des plus grandes surfaces à redévelopper dans la partie centrale d'une métropole en Amérique du Nord[376], à savoir cinq hectares de quasi-friche portuaire au cœur de la zone du *waterfront* sur le lac Ontario (voir Carte 2). Le projet était d'autant plus ambitieux que, cette fois, une même entreprise, Alphabet, était en mesure d'intégrer dès le départ l'ensemble des dispositifs intelligents à toutes les échelles, y compris domestique, ainsi que les traitements logiciels afférents. Comme le rapportent Peel et Tretter, il s'agissait même là de réaliser pleinement l'ambition sous-jacente à la création de Sidewalk Labs selon les propos d'Eric Schmidt lui-même : « imaginez ce que vous pourriez

[376] K. PEEL et E. TRETTER, « Waterfront Toronto », *op. cit.*, p. 2

faire si quelqu'un voulait bien nous confier une ville »[377]. Au-delà même de la mise en place attendue de tout l'éventail de capteurs et de logiciels de modélisation possibles à l'échelle du quartier, il était prévu jusqu'à l'intégration des individus eux-mêmes via des portails numériques permettant, d'une certaine manière, une gestion de l'espace calquée sur des fonctionnements habituels sur un ordinateur. Par exemple, il était envisagé de connecter les accès résidentiels, jusqu'aux appartements individuels, et de les gérer sur le mode des droits d'accès sur un fichier : il aurait ainsi été possible d'accorder une autorisation temporaire d'entrer chez soi à un artisan lui aussi enregistré dans le système de Sidewalk Labs le temps de faire des travaux[378], ce qui aurait préfiguré une nouvelle étape possible dans l'histoire technique des dispositifs relevant de l'habitèle. Au bout du compte, c'est la question de la gouvernance et en particulier de la propriété et de la gestion des données des résidents au sein d'un « *data trust* » plus disputé que prévu qui aura eu raison du partenariat entre les autorités municipales et Sidewalk Labs[379]. La démission médiatisée d'Ann Cavoukian en octobre 2018, ancienne commissaire à la protection de la vie privée Ontario ayant rejoint Sidewalk Labs[380], et connue pour avoir proposé la notion de *privacy by design*[381], a été l'un des premiers signaux : elle expliqua son départ par une formule cinglante : « Je voulais que ce projet accouche d'une ville intelligente fondée sur le respect de la vie privée, pas sur la surveillance »[382]. En mai 2020, Sidewalk Labs a fini par abandonner officiellement la partie. En tout état de cause, et quoiqu'il n'ait pas été mené à son terme, le projet était sans doute le plus ambitieux du genre en termes d'intégration des « couches » (« *layers* ») matérielle et logicielle dans un lieu donné[383], dans une logique foncièrement multiscalaire allant de l'individu à son domicile et à tout un quartier.

Malgré l'échec de Sidewalk Labs à Toronto, on peut signaler que le projet d'associer finement les habitants et leurs pratiques avec un modèle numérique de leur logement, de leur bâtiment, voire de leur quartier, continue de susciter l'intérêt des professionnels du secteur du BTP comme de l'informatique. Anne Alombert et Émilien Cristia observent ainsi que les

[377] « Alphabet executive chairman Eric Schmidt said (…) the genesis of the thinking for Sidewalk Labs came from Google's founders getting excited thinking of "***all the things you could do if someone would just give us a city and put us in charge***," although he joked he knew there were good reasons that doesn't happen. » S. DINGMAN, « With Toronto, Alphabet looks to revolutionize city-building », *The Globe and Mail*, 17 octobre 2017 (en ligne : https://www.theglobeandmail.com/report-on-business/with-toronto-alphabet-looks-to-revolutionize-city-building/article36634779/ ; consulté le 3 mai 2022)
[378] K. PEEL et E. TRETTER, « Waterfront Toronto », *op. cit.*, p. 3
[379] L. AUSTIN et D. LIE, « Data Trusts and the Governance of Smart Environments », *op. cit.*
[380] S. O'SHEA, « Ann Cavoukian, former Ontario privacy commissioner, resigns from Sidewalk Labs », sur *Global News*, 21 octobre 2018 (en ligne : https://globalnews.ca/news/4579265/ann-cavoukian-resigns-sidewalk-labs/ ; consulté le 6 novembre 2018)
[381] R. CHATTELIER *et al.*, *La forme des choix*, Paris (France), CNIL, 2019, p. 10
[382] « *I wanted this to become a smart city of privacy – not a smart city of surveillance* ».
[383] K. PEEL et E. TRETTER, « Waterfront Toronto », *op. cit.*, p. 2

pratiques de *Building Information Modeling* (BIM) sont désormais courantes à l'échelle des bâtiments, pour leur construction et leur entretien[384]. En s'appuyant sur les « maquettes » numériques de plus en plus nombreuses issues des pratiques BIM, les industriels et *start-ups* du secteur envisagent une montée à l'échelle du quartier voire de la ville à travers le concept de *City Information Model-Modeling-Management* (CIM). La principale différence avec les projets de *smart cities* antérieurs est que l'ambition est moins de créer de toute pièce une ville *smart* ou encore d'augmenter l'urbain existant, mais plus simplement de capitaliser sur des pratiques professionnelles déjà usuelles pour construire moins une nouvelle infrastructure technique qu'une nouvelle échelle de gestion de l'existant. Quoique les auteurs pointent la dimension encore très « promotionnelle »[385] et prospective du CIM, cette approche plus pragmatique de l'augmentation numérique des espaces urbains pourrait finir par émerger à bas bruit plus vite que les projets de *smart cities* prométhéens dont Quayside Toronto a été la vitrine malheureuse.

L'espace domestique comme *spatial fix* : un immense marché émergent

Si le marché de la *smart* city semble aujourd'hui en berne avec 34 projets seulement initiés en 2020 contre plus de soixante par an entre 2015 et 2019[386], la donne n'est pas la même pour les objets connectés grand public et la *smart home* en particulier.

Le marché mondial des enceintes connectées seules était estimé à 17,04 milliards de dollars étatsuniens en 2019, et devrait atteindre près de 71 milliards de dollars en 2026 selon une étude de 360 Market Updates[387] (voir Figure 17). Si on prend en compte l'ensemble du marché de la « *smart home* », une étude de Reuters donne une estimation de 36 milliards en 2018, et une projection de 151 milliards dès 2023.

---

[384] A. ALOMBERT et É. CRISTIA, « L'espace urbain à l'épreuve de la révolution numérique : nouvelles technologies urbaines et intelligence collective », *ISTE Open Science*, vol. 6, nº 3, 7 mai 2021 (DOI : 10.21494/ISTE.OP.2021.0657 consulté le 15 mars 2023)

[385] « Même si le concept de « CIM » est aujourd'hui principalement utilisé à des fins promotionnelles à défaut de relever d'une réelle pratique, la modélisation numérique d'informations urbaines apparaît néanmoins comme une tendance pouvant raisonnablement s'imposer comme une activité liée à la fabrique et la gestion de la ville. » *in Ibid.*, p. 2

[386] S. MATHIS et A. KANIK, « Why you'll be hearing a lot less about 'smart cities' », *City Monitor*, 18 février 2021 (en ligne : https://citymonitor.ai/government/why-youll-be-hearing-a-lot-less-about-smart-cities ; consulté le 16 mars 2021)

[387] *Smart Home Market - Analysis by Size, Growth, Trend and Forecast to 2024*, Pune (Inde), Markets and Markets, 2019

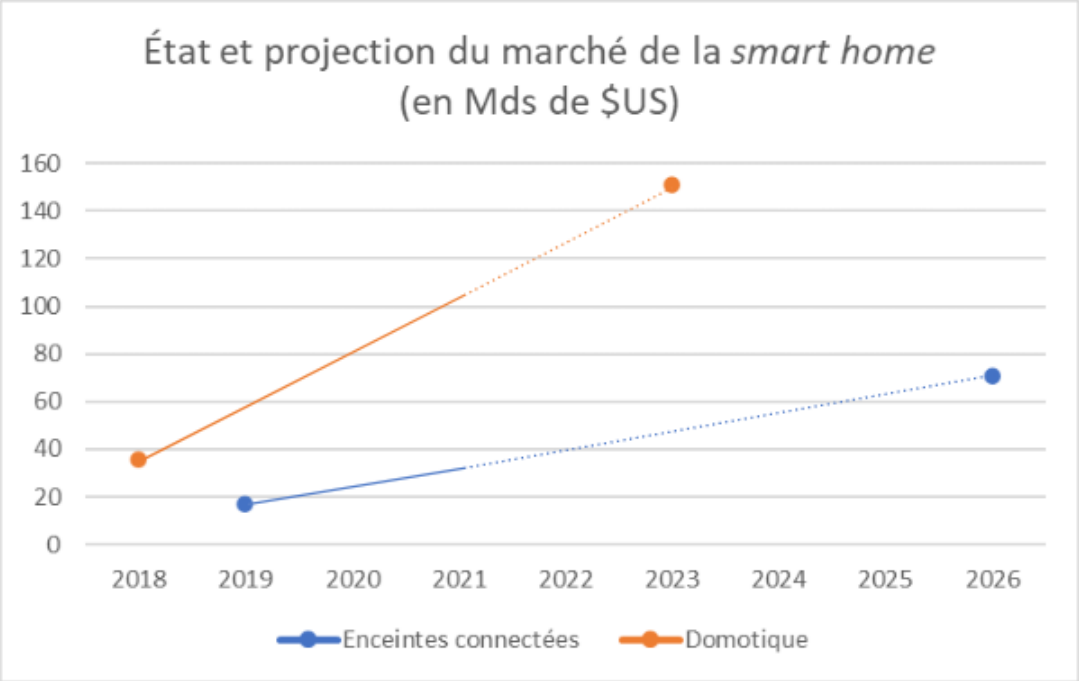


Figure 17 - Evolution du marché de la maison connectée. Réalisation JFP, 2021. Sources : Global Smart Voice Assistant Speaker Market, Pune (Inde), 360 Market Updates, 2020. Global Smart Home Market 2018 by Evolving Technology, Projections & Estimations, Business Competitors, Cost Structure, Key Companies and Forecast to 2023, Reuters, 2018.

Dans un rapport publié en mai 2019, la Hadopi et le CSA parlaient encore d'« un marché français récent et encore limité »[388] pour les seuls assistants vocaux. Il faut rappeler que les premières commercialisations officielles en langue française ont commencé en 2018 pour Amazon et Google. Pour autant, le marché de la *smart home* dominait déjà depuis 2015 en valeur parmi les objets connectés vendus dans le pays, devant même les *wearables* (voir Figure 18). Il faut cependant signaler que la catégorie *smart home* inclut ici l'équipement électroménager connecté. Cet électroménager peut relever de la dépense contrainte, si l'on considère par exemple que la gamme non-connectée d'appareils courants, comme les lave-linges, se réduit. Le volume de ventes en valeur peut aussi être gonflé du fait de prix dont l'ordre de grandeur est la centaine d'euros dans l'électroménager connecté, dans un marché porté par des appareils comme les robots-cuiseurs ou des aspirateurs-robots. En termes de pénétration du marché, il est donc probable que les *wearables* soient largement plus répandus – un bracelet connecté de sport, par exemple, ayant un prix dont l'ordre de grandeur est plutôt de la dizaine

[388] *Assistants vocaux et enceintes connectées: l'impact de la voix sur l'offre et les usages culturels et médias, op. cit.*, p. 6

d'euros. La part de marché de la *smart home* n'en reste pas moins révélatrice d'une tendance désormais bien installée et pérenne.

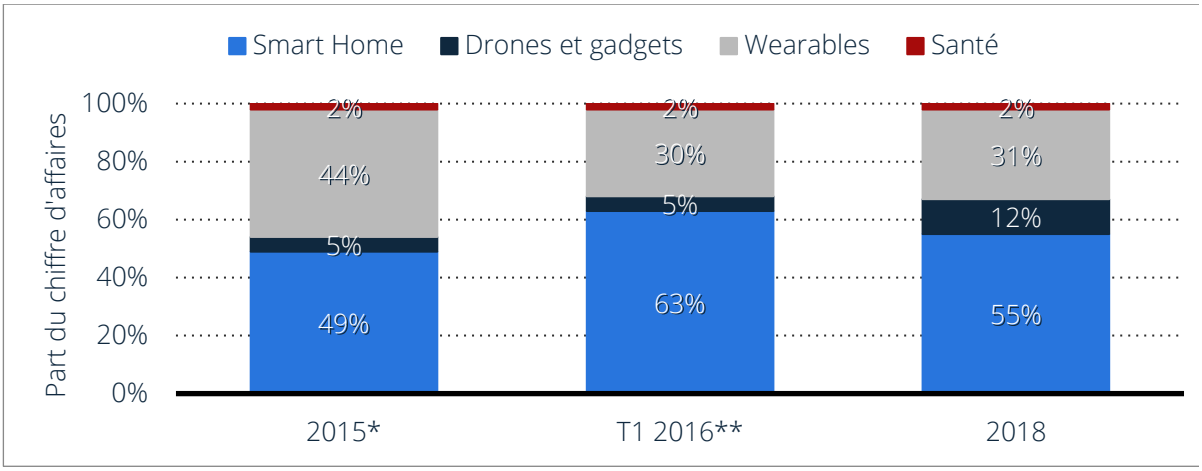


Figure 18 - Répartition du chiffre d'affaires du marché des objets connectés en France de 2015 à 2018, par segment (source : Gfk, 2019)

Si l'on se penche plus particulièrement sur les enceintes connectées en France, le taux de pénétration mesuré en février 2019 à 11 % reste effectivement faible, le plus bas des pays où les enceintes ont été d'abord disponibles (États-Unis, Royaume-Uni, Allemagne). Pour autant, les prévisions pour les années 2020 à 2025 anticipent un rattrapage assez rapide, avec plus d'un tiers (36 %) des ménages équipés d'ici le milieu de la décennie (voir Figure 19), soit peu ou prou le niveau déjà atteint aux États-Unis début 2020[389]. Cela, pour les seules enceintes connectées à proprement parler, et sans parler du fait que les assistants logiciels soient implémentés dans d'autres appareils que les seules enceintes de Google ou Amazon.

[389] B. KINSELLA, « Nearly 90 Million U.S. Adults Have Smart Speakers, Adoption Now Exceeds One-Third of Consumers », sur *Voicebot.ai*, 28 avril 2020 (en ligne : https://voicebot.ai/2020/04/28/nearly-90-million-u-s-adults-have-smart-speakers-adoption-now-exceeds-one-third-of-consumers/ ; consulté le 11 mai 2020)

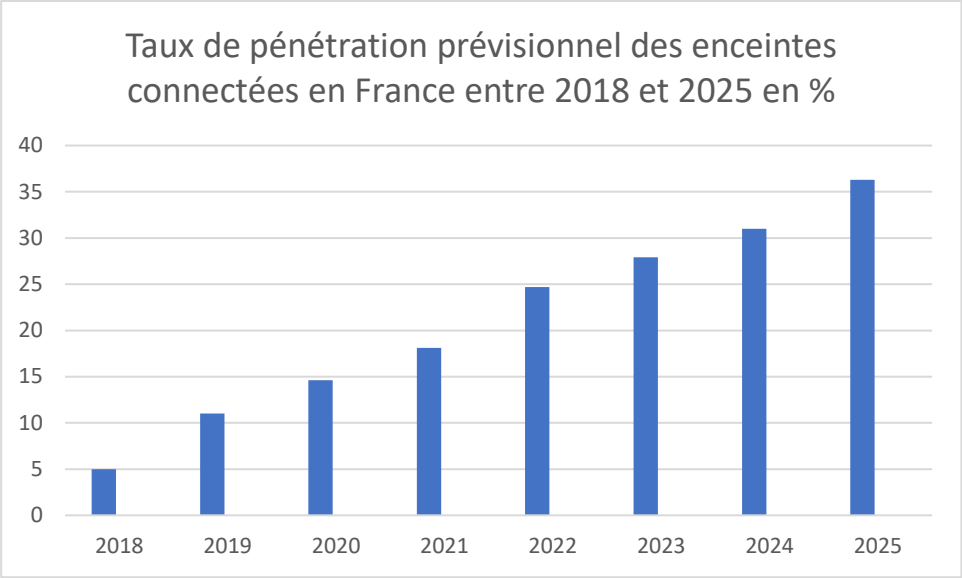


Figure 19 - Taux de pénétration prévisionnel des enceintes connectées en France entre 2018 et 2025 en % (source : Hadopi, CSA, 2019)

« [Étude] conduite par l'institut Harris Interactive du 7 au 18 février 2019, auprès d'un échantillon total de 2 605 individus : un échantillon principal de 2 505 individus, représentatif des internautes français de 15 ans et plus (selon la méthode des quotas, au regard de critères sociodémographiques : sexe, âge, catégorie socio - professionnelle, taille d'agglomération et région de résidence), complété par un sur-échantillon de 100 utilisateurs d'enceintes connectées au cours des 30 derniers jours et pour les marques les plus utilisées (Google Home, Amazon Echo et Apple HomePod), soit un total de 285 utilisateurs d'enceintes connectées au cours des 30 derniers jours. »[390]

En effet, une certaine diversification des acteurs et du marché est en cours : les smartphones et les enceintes connectées directement vendues par Google ou Amazon, et dans une moindre mesure par Apple, ne sont plus les seuls dispositifs d'accès aux assistants vocaux. Fin 2017 déjà, l'entreprise spécialisée dans le son Sonos était la première à intégrer les assistants d'Amazon et de Google dans son enceinte Sonos One[391]. Les assistants sont de plus en plus intégrés dans d'autres dispositifs que les enceintes des constructeurs, notamment les box Internet des FAI ou dans les téléviseurs dits intelligents. Du reste, l'enceinte connectée telle que nous la connaissons aujourd'hui, si elle reste sur une trajectoire commerciale ascendante, n'est probablement pas amenée à rester prédominante comme hub domotique, ni d'ailleurs comme objet-enceinte, comme nous en avons déjà fait l'hypothèse (voir « Un problème terminologique transitoire », p. 31).

[390] *Assistants vocaux et enceintes connectées: l'impact de la voix sur l'offre et les usages culturels et médias*, *op. cit.*, p. 80
[391] M. GEORGESCU DE HILLERIN et M. CIOLFI, « Sonos One, la première enceinte qui mixe Alexa et Google Assistant », *op. cit.*

Les enceintes connectées ne me semblent en fait même pas constituer un nouveau marché à proprement parler, ou pas durablement. Le prix modique auquel elles sont vendues, même en masse, couvre sans doute à peine les frais de fonctionnement des services logiciels distants desquels elles dépendent : une entrée d'argent pour le fabricant est faite à la vente, mais l'assistant vocal reste disponible sans véritable limite de durée. Seul Apple vendait ses HomePod nettement plus cher qu'Amazon ou Google, mais avec un discours commercial justement axé sur la qualité sonore de l'objet, plus que sur les services associés. L'absence d'abonnement laisse penser, que selon le modèle de la pseudo gratuité bien connue dans les services en ligne, le retour sur investissement du concepteur des logiciels associés aux enceintes se fait ailleurs.

Les enceintes connectées semblent plutôt être le point de départ de l'investissement de la domotique par le capitalisme de surveillance, en fournissant une nouvelle source de données et de canaux de diffusion pour les GAFAM, c'est-à-dire là où se fait réellement la création de valeur pour ces derniers. De ce point de vue, l'émergence de ces appareils peut être lue comme un *spatial fix*[392] du capitalisme de surveillance, qui cherche désormais à s'étendre au logis en en faisant une *smart home*. Si le domicile était déjà partiellement monitoré par ces entreprises, c'était surtout à travers des objets mobiles : ces objets se trouvaient être dans le domicile (ordinateurs, téléphone portable), mais la nouveauté est qu'il s'agit désormais d'équiper le domicile lui-même, ses installations fixes. Les fabricants jouent ici sur une tendance au « repli domestique » déjà identifiée par Kaufmann[393], dont Staszak complète l'analyse en arguant qu'il « affecte notre société occidentale (…) [en vue de] donner plus d'attention, de temps et surtout d'argent à l'aménagement de notre espace domestique »[394].

Cette évolution est parallèle à une autre évolution économique en cours, qui tend à faire du domicile des consommateurs une véritable plate-forme logistique individuelle. La livraison à domicile a en effet explosé, d'abord avec la vente par correspondance sur catalogue, puis plus encore avec Amazon ensuite, et aujourd'hui avec la multitude d'entreprises de livraison et leurs

[392] Pour reprendre une expression de David Harvey qui la définit ainsi : « Le *spatial fix* au problème de la suraccumulation implique la production de nouveaux espaces dans lesquels la production capitaliste peut continuer à croître (par des investissements d'infrastructure, par exemple), l'accroissement du commerce et des investissements directs, ainsi que l'exploration de nouvelles façons d'exploiter le travail » (trad. pers.). « *This 'spatial fix' (…) to the overaccumulation problem entails the production of new spaces within which capitalist production can proceed (through infrastructural investments, for example), the growth of trade and direct investments, and the exploration of new possibilities for the exploitation of labour power* » *in* D. HARVEY, *The Condition of Postmodernity - An Enquiry into the Origins of Cultural Changes*, Cambridge (États-Unis) et Oxford (Royaume-Uni), Blackwell, 1990, p. 183

[393] J.-C. KAUFMANN, *La chaleur du foyer. Analyse du repli domestique*, *op. cit.*

[394] J.-F. STASZAK, « L'espace domestique », *op. cit.*, p. 340

applications pour *smartphone* correspondantes. Ce marché déjà très riche continue de voir apparaître de nouveaux acteurs sur des secteurs de plus en plus précis et de plus en plus concurrentiels. À la livraison de toutes sortes de biens de consommation par Amazon ont succédé la livraison de courses à domicile par les enseignes de la grande distribution ainsi que la livraison de repas par Deliveroo, Uber Eats... 2022 voit émerger des acteurs internationaux sur le segment de la livraison rapide, de l'ordre de la demi-heure, de produits d'épicerie par l'espagnol Glovo, le turc Getir, l'allemand Gorillas…[395] Il s'agit là encore d'une forme de *spatial fix* : il n'y a plus à accueillir le client dans un lieu dédié à l'achat ou à la consommation sur place. On parle de *dark store*[396] ou de *dark kitchen* pour désigner ces nouveaux espaces qui se multiplient dans les centres-villes et ne sont fréquentés que par les manutentionnaires et les livreurs qui font le lien avec le consommateur final. Ces services permettent également de créer de nouvelles opportunités de vente, par exemple en livrant un repas pour lequel le consommateur n'aurait pas forcément consenti à se déplacer.

Pour Nicolas Nova, cet état de fait résulte en bonne partie de la facilité nouvelle avec laquelle les consommateurs et les livreurs peuvent opérer dans la *gig economy* grâce à leurs smartphones, qui font office de « baguettes magiques » grâce auxquels la livraison se fait avec une absolue « fluidité » et une grande rapidité, une fois la configuration initiale effectuée[397]. Le paradoxe est que le téléphone *mobile* sert ici à renforcer la présence dans le lieu d'ancrage par excellence qu'est le domicile : le smartphone ne sert pas ici à créer un « cocon » dans l'espace public, mais il est mis au service du logis comme cocon (voir « Le logis comme cocon », p. 111), vers lequel on fait se déplacer le monde plutôt que de se rendre soi-même dans le monde. Il s'agit d'éviter l'extérieur, et d'enrichir la vie domestique. La logique immunitaire joue ici à plein en revivifiant une limite entre l'extérieur et l'intérieur, entre le public et le privé. Il y a là comme un étonnant comblement de la distance métaphorique de la *home*, très convoquée dans les interfaces utilisateurs[398], qui mène le numérique à revenir du comparant au comparé par

[395] L. COROT, « Ces start-up qui lèvent des millions pour leur service de livraison de courses à domicile », *L'Usine Digitale*, 4 juin 2021 (en ligne : https://www.usine-digitale.fr/editorial/ces-start-up-qui-levent-des-millions-pour-leur-service-de-livraison-de-courses-a-domicile.N1100004 ; consulté le 18 juin 2021)
[396] *Id.*
[397] « S'il y a un changement pour les usagers, ce sont aussi les chauffeurs qui subissent les conséquences d'une telle évolution technique et de l'utilitarisme effréné inscrit dans ces apps. L'automatisation n'est jamais totale, et les conducteurs Uber ou les livreurs de nourriture (Deliveroo, UberEats) sont mis au pas par ces systèmes ; lesquels les enjoignent à une livraison rapide, prix à payer pour la fluidité magique perçue par les usagers » *in* N. NOVA, *Figures mobiles: une anthropologie du smartphone*, *op. cit.*, p. 178
[398] Dominique Boullier la signale lui-même dans son dernier texte sur l'habitèle : « à cette fluidité qui domine dans les termes, s'opposent dans le même univers numérique ceux « d'hébergement » (les serveurs qui hébergent) ou de « *home* », omniprésents sur tous les systèmes d'exploitation des portables ou dans les applications » *in* D. BOULLIER, « Rendre le numérique habitable : l'habitèle », *op. cit.*, p. 1

l'augmentation de l'espace domestique. Au-delà de sa dimension rhétorique, ce comblement résulte en fait d'une communication et d'une stratégie commerciale des plus explicites.

La mise en scène du foyer dans la communication des fabricants et vendeurs d'enceintes connectées

Le champ notionnel du foyer est convoqué depuis longtemps dans les interfaces, à l'instar du « bureau » très présent dans les systèmes d'exploitation des ordinateurs personnels. Mais il fonde aujourd'hui une large part, sinon la totalité, des stratégies commerciales d'entreprises majeures du numérique. L'exemple le plus marquant est sans doute l'entreprise Nest, rachetée par Alphabet pour aujourd'hui définir toute sa gamme d'objets liés à la *smart home*, présentée donc comme un « nid », et alors que leurs enceintes s'appelaient déjà Google *Home* avant ce rachat et le changement de nom de la société-mère de Google. Mais cette stratégie est aussi reprise par de plus petits acteurs, comme l'hébergeur de données individuelles Cozy, qui se veut le « domicile numérique » de ses utilisateurs[399], ou comme Purism, qui produit des ordinateurs et smartphones sécurisés qu'ils présentent comme un « *castle* » dans une reprise explicite de l'expression anglaise « *a man's home is his castle* »[400] (voir « *A man's home is his castle* : aspects juridiques », p. 106). La manière dont les enceintes connectées et les objets associés sont présentés en magasin en France et dans la communication des fabricants d'enceintes me semblent les meilleurs révélateurs de cette stratégie, dont j'identifie trois phases.

Dans un premier temps, la notion de foyer n'a pas été particulièrement convoquée dans la mise en rayon. Ces produits innovants et portés par des entreprises à l'image de marque très forte ont eu de manière assez classique l'honneur des têtes de gondole : il fallait mettre en avant ces produits à la fois très attendus, mais au fonctionnement encore méconnu, et au succès pas nécessairement assuré. L'exemple de la FNAC du centre commercial du CNIT, dans le quartier de la Défense à Nanterre le 21 février 2018, soit l'année de la commercialisation en France des premières enceintes connectées, est ici éclairant. S'il ne s'agit pas du plus grand magasin du groupe, il est l'un des plus importants du fait de la clientèle aisée, technophile et prescriptrice qui fréquente le premier quartier d'affaires du pays. Pour cette première année de commercialisation, c'est même tout le hall d'entrée qui était tapissé de produits Google (voir Photographie 2). Il est intéressant de constater que c'est pour le répéteur Wi-Fi de Google que

[399] Le service, français, est largement comparable à celui proposé par la Poste pour la conservation des documents administratifs, appelé Digiposte, et qui convoque pour sa part l'image du « coffre-fort numérique ».

[400] K. RANKIN, « Your Phone Is Your Castle », sur *Purism*, 11 septembre 2020 (en ligne : https://puri.sm/posts/your-phone-is-your-castle/ ; consulté le 15 octobre 2020) Il est à noter que l'image d'illustration en haut de la page est même littéralement celle d'un château, celui d'Arundel, dans le Sussex.

la « maison » est évoquée (« Le Wi-Fi sans interruption dans votre maison »), alors que les enceintes Google Home sont présentées comme fournissant un « Assistant (…) à votre service ».

Photographie 2 - Murs du hall d'entrée de la FNAC du CNIT (la Défense) le 21 février 2018 (auteur : JFP)

Par ailleurs, l'écran de télévision du hall, visible de l'extérieur, et monté sur une colonne centrale en travers du passage, c'est-à-dire le point de visibilité maximale du magasin, mettait autant en avant les enceintes Google Home que les répéteurs Wi-Fi de Google (voir Photographie 3).

Photographie 3 - Colonne centrale du hall de la FNAC du CNIT (la Défense) le 21 février 2018 (auteur : JFP)

Cette scénographie commerciale initiale était donc très frontale, peu explicite, et plutôt dévolue à accompagner et à créer un engouement des clients pour une gamme de produits nouvelle. Ces produits Google étaient également présents en bonne place à l'intérieur du magasin, mais sans mise en scène spécifique, à proximité des linéaires dédiés aux smartphones. Un homme et une femme, visiblement en couple, et âgés d'une soixantaine d'années, y interrogeaient le vendeur sur les finalités de la Google Home. Une question de la femme est révélatrice de la nouveauté que constituaient alors ces objets, puisqu'elle lui a demandé « si ça peut s'utiliser hors de la maison ». La réponse du vendeur a d'abord été « Non, c'est d'ailleurs pour ça que ça s'appelle Google Home », avant qu'il ne développe plus techniquement sur le fait que ces appareils devaient être branchés sur le secteur et connectés en Wi-Fi. Par ailleurs, et sans exagérer sur la représentativité du discours de ce vendeur en particulier, qui a en outre fini par les diriger vers un collègue « qui est un spécialiste », il a moins insisté sur les fonctions domotiques (n'évoquant que la possibilité de piloter la télé) que sur les capacités conversationnelles de l'Assistant de Google : « derrière il y a en fait toute une intelligence artificielle », à qui poser des questions du type « comment on dit bonjour en chinois ? », et qui permettrait à terme « un tas de choses » comme de commander un taxi ou une pizza, ce qui se faisait déjà aux États-Unis. Cette mise en rayon peu spécifique se retrouvait également dans le magasin Darty du centre commercial des Quatre Temps, de l'autre côté de la dalle de la Défense :

« • Passage au Darty des 4 temps, stimulé par le passage à la FNAC.

◦ Google Home y est bien sûr présent aussi (l'enseigne l'offrait à partir de 300 € d'achats, pendant les fêtes), mais beaucoup moins mis en valeur.

◦ Il a quand même son panneau indicateur dans l'allée centrale et une petite tête de gondole rayon enceintes. Il est même possible d'en manipuler un, qui sort son message pré-enregistré (cf. vidéo). »

Extrait de carnet de terrain du 21 février 2018

Plus tard dans l'année, en juillet, je faisais encore le même constat dans un autre magasin Darty dans le XVIIe arrondissement de Paris, quoique le lien avec la domotique y ait été fait un peu plus nettement :

« Je suis allé voir comment étaient vendues les enceintes connectées au Darty de la porte de Saint-Ouen. C'est très décevant : juste un stand minimaliste pour Google Home. Je n'ai pas vu de personnes ayant l'air intéressées. Sans doute beaucoup moins intéressant que Chatelet, la Défense ou d'autres du même acabit. Les télévisions de présentation passaient des publicités pour Google Home et une boîte de domotique connectée aux assistants personnels (Sowee je crois?) »

Extrait de carnet de terrain du 5 juillet 2018

L'expérience s'est confirmée, cette fois dans une FNAC lyonnaise, au centre commercial de la Part-Dieu :

« les enceintes connectées ne sont pas du tout mises en valeur. Elles ont leur petit rayon habituel, à côté des autres enceintes, mais sans être spécialement valorisées. Les personnes que j'ai observées dans le rayon se concentraient plutôt sur les enceintes Bluetooth, aucun vendeur ne semblait disposé à faire de la réclame. »

Extrait de carnet de terrain du 12 juillet 2018

Et elle s'est répétée, cette fois dans un magasin généraliste Auchan, de nouveau aux Quatre Temps, le 3 novembre 2018. Là encore, malgré tout, l'association en rayon des enceintes avec d'autres produits axés sur la domotique (caméras de vidéosurveillance de marque Qilive, disque-dur externe My Cloud Home de marque Western Digital) commençait à être plus explicite (voir Photographie 4).

« Je passais juste acheter mon carnet, mais j'ai aussi trouvé des GH au rayon électronique. Absolument pas mis en valeur, dans une vitrine fermée sans cérémonie ni exemplaire de test. En revanche, présentées avec des caméras de surveillance et d'un serveur domestique, cf. photo »

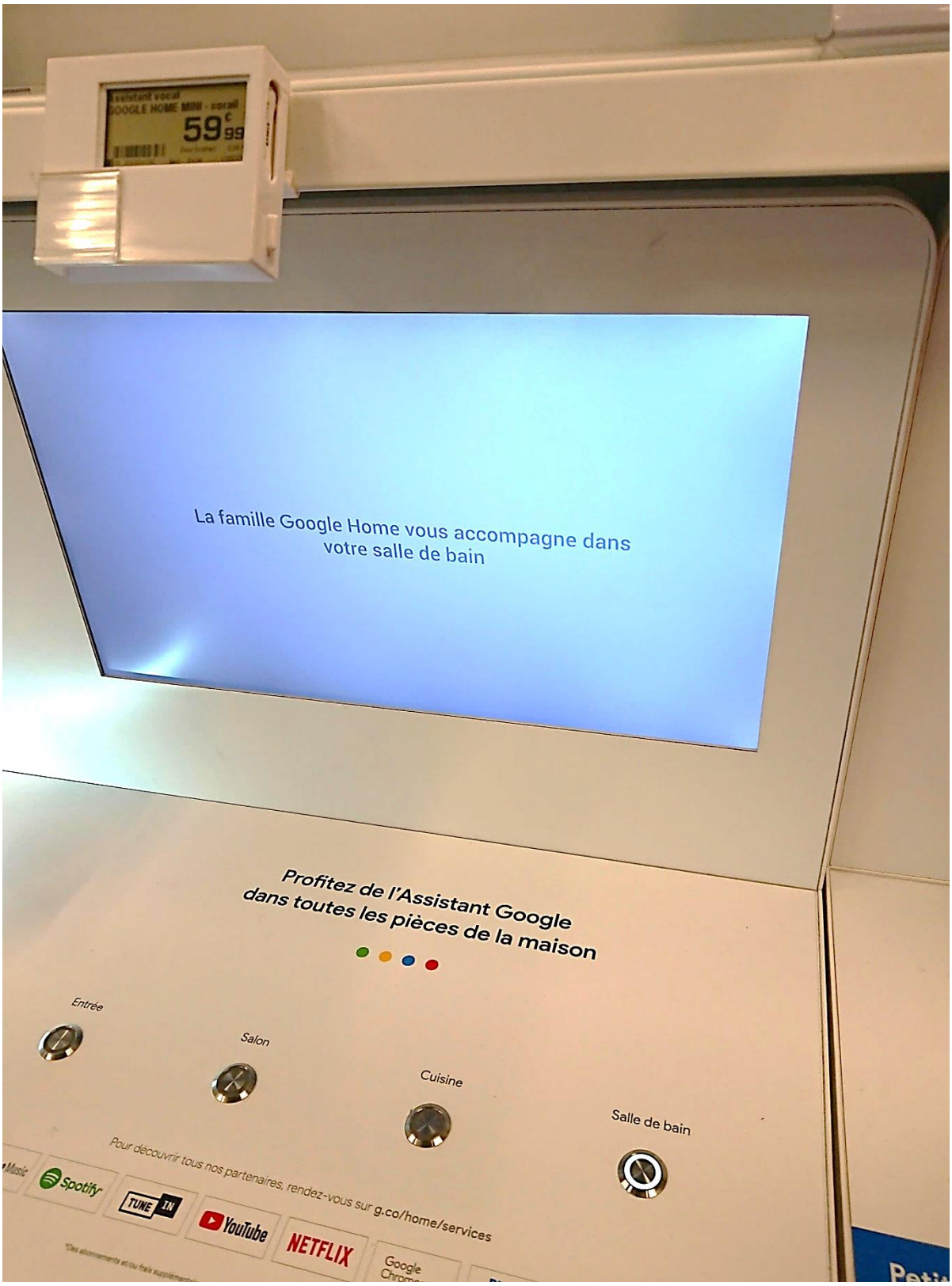
Extrait de carnet de terrain du 3 novembre 2018

Photographie 4 - Mise en rayon d'enceintes connectée dans un magasin Auchan (auteur : JFP, 2018)

Dans un deuxième temps, la mise en scène des enceintes s'est considérablement précisée, particulièrement pour les enceintes de Google, et plutôt dans les magasins spécialisés. La mise en scène du foyer a été particulièrement explicite à travers une mise en rayon dans des sortes de maisonnettes en bois, dont la forme évoque celle d'un toit, et dont la matière évoque une certaine chaleur associable au foyer (voir Photographie 5) – ce choix n'est pas anodin, il aurait été possible d'insister, par exemple, sur le registre de l'efficacité informatique ou de la modernité en recourant à des matières plus métalliques. Cette forme de mise en rayon apparue en 2018 se retrouvait systématiquement dans les FNAC et les Darty des régions parisiennes et lyonnaise dans la période.

Photographie 5 - La mise en scène des produits Google Home à la FNAC du Forum des Halles à Paris le 19 décembre 2018 (auteur : JFP)

Au-delà de la forme du toit évoquant la silhouette d'une maison, et identifiable d'assez loin, la mise en rayon est aussi passée par une spécialisation par pièce des produits proposés en association avec les enceintes connectées de Google. Cela passait par les choix d'assortiment de produits en rayons, une lampe connectée à intensité lumineuse variable étant plutôt proposée pour la chambre que la salle d'eau. En outre, certains magasins étaient dotés de tablettes tactiles ou encore d'un écran associé à une petite console munie de boutons, permettant de lancer une animation en musique accompagnée d'une voix off décrivant des mises en situation d'objets connectés associés à une Google Home selon les pièces de la maison (voir Photographie 6), et parfois une enceinte Google Home préconfigurée permettant de se rendre compte de sa sonorité (Photographie 7).

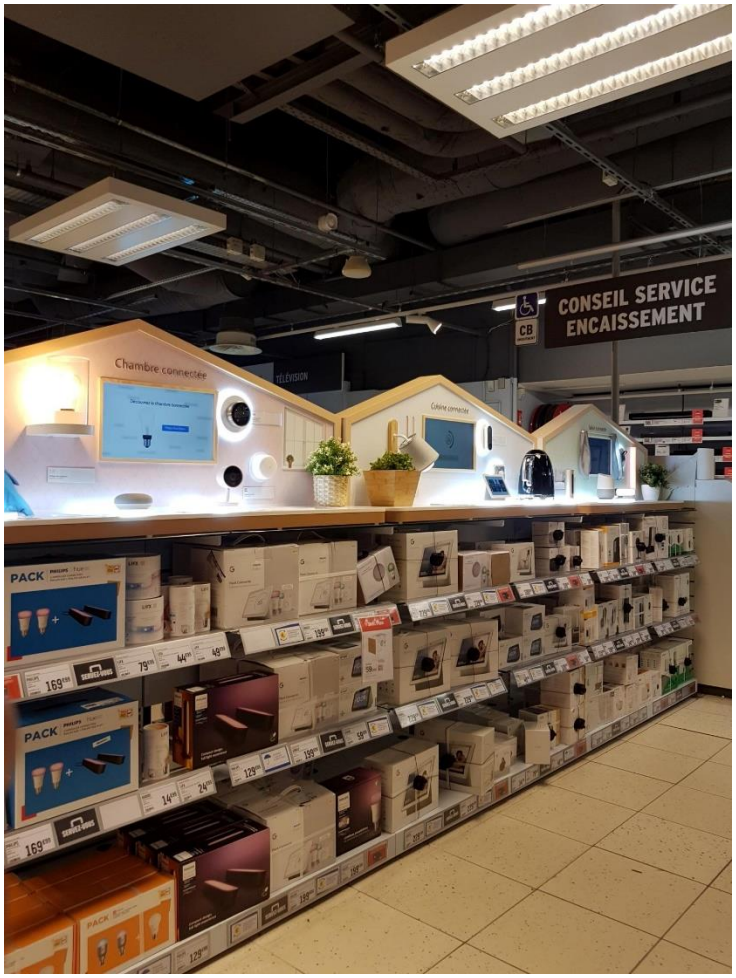


Photographie 6 – Détail d'une console de présentation de Google Home selon les pièces de la maison au Boulanger Rosa Park à Paris le 19 décembre 2018 (auteur : JFP)

Photographie 7 - Une console de présentation activant une enceinte Google Home selon les pièces de la maison au Darty de Cergy le 18 décembre 2018 (auteur : JFP)

Cette logique de séparation par pièce de la maison, cette fois jusque dans la mise en scène du linéaire, a été poussée au maximum en 2019. La présentation sous une forme de toit en bois était alors reprise pour chaque pièce de la maison, en indiquant désormais, de gauche à droite, « chambre connectée », « cuisine connectée » et « salon connecté », ici dans une FNAC lyonnaise (voir Photographie 8). Le soin accordé à cette mise en rayon semble confirmer à la fois le succès commercial escompté un an plus tôt, et la confiance du distributeur dans cette gamme (ici, autour de Google Home). Chaque « pièce » est scénarisée autour d'une petite vidéo de présentation synchronisée avec le rayonnage en magasin : l'enceinte connectée « répond » aux ordres de la vidéo, certains objets associés s'activent, comme les ampoules connectées, ou

sont, au minimum, progressivement mis en valeur par le jeu d'allumage et d'extinction de petits spots lumineux intégrés au mobilier du rayonnage.



Photographie 8 - Une mise en rayon par pièce "connectée" de la maison autour de Google Home à la FNAC de Lyon Part-Dieu le 19 décembre 2019 (auteur : JFP)

Avec l'arrivée des enceintes connectées intégrant un écran et une caméra, comme la Nest Hub Max, les vidéos promotionnelles sont parfois déportées vers des modèles de présentation (voir Photographie 9). La première vidéo sur ce modèle est intéressante en cela qu'elle est censée montrer quelles sont les fonctions de base d'un tel appareil pour le chaland. Or, elle commence à l'extérieur de la maison, dans la rue, d'où le personnage Nico reçoit une notification de mouvement chez lui et reçoit les images prises par l'enceinte sur son smartphone : il s'agit en fait de son chien qui a activé le détecteur de mouvement. Une fois rentré, une interaction vocale est mise en scène. Les phrases du type « je suis rentré » (dans la vidéo) ou encore « bonne nuit », derrière leur apparence anodine ou simplement conviviale (son Nest Hub lui répond d'ailleurs sur un ton enjoué « Bienvenue à la maison ! »), servent généralement à désactiver certaines fonctions ou à en activer d'autres selon les routines

configurées, ce qui reste implicite dans la vidéo. Ici, il s'agit de désactiver le détecteur de mouvements, et peut-être de lancer le chauffage. De fait, la vidéo continue en énumérant les fonctions qu'elle peut déclencher, comme « allume[r] la lumière, régle[r] le thermostat », le tout, « automatiquement », et avec comme texte incrusté « contrôle de la maison connectée ». Elle se termine sur cette même expression de « maison connectée », dont elle permet de renforcer le « confort », le « contrôle » et la « sécurité », ce qui pourrait aussi bien être le triptyque de ce qu'on peut attendre de tout logis. La « maison connectée » est avant tout une maison, et les objets connectés sont présentés comme s'y intégrant naturellement pour en augmenter les qualités.

a. « Contrôlez ce qui se passe chez vous grâce à la Nest Cam intégrée. »

b. « Regardez le flux en direct, ou recevez-une alerte en cas de mouvement. »

c. « « Okay Google, je suis rentré ! ». « Bonjour Nico, bienvenue à la maison ! » Avec l'assistant Google, vous pouvez contrôler plus d'un millier d'appareils connectés compatibles. »

d. « Allumez la lumière, réglez le thermostat, et effectuez bien d'autres tâches automatiquement. Google Nest Hub Max : plus de confort, de contrôle et de sécurité dans votre maison connectée. »

Photographie 9 - Mosaïque de captures d'écran d'une vidéo promotionnelle Nest Hub Max présentée à la FNAC Lyon Part-Dieu le 21 septembre 2021

Dans le cas d'Amazon, l'idée a parfois été d'insister sur le fait qu'une enceinte connectée faisait un excellent présent pour Noël, par exemple en décorant le rayon d'un ruban

évoquant l'emballage d'un papier-cadeau (Photographie 10). On notera tout de même l'expression imprimée « Maison connectée » et l'association explicite avec d'autres produits qui mettent aussi en avant l'idée de *smart home*. On retrouve par exemple un thermostat connecté Netatmo (en haut à droite), une ampoule connectée Philips Hue (en bas à droite), une sonnette connectée Ring (deuxième en partant du bas à droite), une prise connectée Amazon Plug (en haut à gauche) ou encore une caméra de surveillance (en bas à gauche). Tous ces produits sont activables (comme l'ampoule) ou susceptibles d'une description vidéo en pressant le bouton associé.

Photographie 10 - Tête de gondole pour les enceintes Amazon Alexa et des produits associés dans le Boulanger Rosa Parks à Paris le 18 décembre 2018 (auteur : JFP)

Dans les Apple Store proposant des HomePods, la logique d'épure habituelle à la présentation des produits dans ces magasins l'emporte sur toute mise en scène particulière à la *smart home* : les enceintes connectées de présentation sont simplement alignées à bonne distance les unes des autres sur une vaste paillasse en bois, à l'instar des smartphones et des ordinateurs de la marque (voir Photographie 11). L'idée est de ne pas surcharger l'espace de présentation du magasin avec des murs d'emballages en carton en libre-service, et d'inviter plutôt à la manipulation des appareils qui sont laissés à la disposition des visiteurs – supervisés malgré tout par un nombre important de vendeurs. Avec l'arrêt de la production des HomePods

au profit des seuls HomePods Mini, leur part s'est encore réduite dans le linéaire. Quant aux objets connectés compatibles, certes de marques partenaires et non Apple, ils sont relégués dans un rayonnage beaucoup plus classique au fond du magasin. Il est par ailleurs à signaler que, tant que les produits Apple étaient encore présentés dans d'autres magasins type FNAC, Darty ou Boulanger, leur mise en rayon n'avait rien de particulier : ils étaient présentés comme des produits parmi d'autres, signe sans doute du faible intérêt porté par Apple à cette catégorie d'objets – ses smartphones ou ses ordinateurs, qui sont ses produits-phares, ont généralement une mise en scène soignée qui tranche avec les mises en rayon plus habituelle, se rapprochant de la présentation en Apple Store même hors les murs de la marque.

Photographie 11 - Les enceintes Apple sont présentées à la manière des autres produits de la marque, ici à l'arrière-plan, dans l'Apple Store de Lyon Part-Dieu le 23 décembre 2018 (auteur : JFP)

Google et, dans une moindre mesure, Amazon, sont donc les deux marques qui ont le plus travaillé la présentation de leurs produits en magasin. Le lien avec la maison connectée, plutôt absent au début, a été fait de manière progressive et jusqu'à un certain niveau de raffinement, pièce par pièce, par Google. La volonté d'associer en un même rayon les enceintes à des objets connectés compatibles, sans doute poussée également par les distributeurs, contribue à l'idée qu'émerge une gamme de produits cohérente, autour de la « maison connectée ». Ces produits ne se voient pas encore dédier d'ailes complètes des magasins

spécialisés, comme les téléviseurs, les téléphones, la Hi-Fi, les lave-linge (pour les Darty et les Boulanger) ou les livres (pour les FNAC), mais le soin accordé aux rayons qui leur sont dédiés est révélateur. D'une part, on n'attend plus du client qu'il aille chercher son enceinte connectée dans l'aile son, sa webcam de surveillance dans l'aile image, ou sa prise connectée au rayon câbles et quincaillerie. D'autre part, et c'est une nouveauté, ces produits très différents sont rassemblés autour d'une thématique spatiale transversale, la « maison connectée », et plus selon une typologie technique. Jusqu'ici, tout au plus pouvait-on parfois trouver un rayon pour les objets « d'extérieur ». Il est impossible d'affirmer que cette tendance soit pérenne, mais cette évolution constitue à tout le moins un signal faible intéressant, et surtout révélateur de la stratégie commerciale des fabricants et des distributeurs d'objets domotiques connectés.

CONCLUSION PARTIELLE

Après avoir largement battu en brèche les pesanteurs de l'espace matériel topographique dans l'activité de transmission de l'information, on pourrait trouver étonnant que le numérique réinvestisse aujourd'hui puissamment un type d'espace et un imaginaire, le logis, la maison, la *home*, qui sont synonymes de l'ancrage et de la territorialité les plus forts pour l'individu contemporain. N'y a-t-il pas un paradoxe à *brancher* aujourd'hui des enceintes connectées dans les habitats d'où nous avons évacué les téléphones fixes au profit de *smartphones* disposant, d'un point de vue technique, de fonctionnalités égales, et le plus souvent supérieures, à ces mêmes enceintes ? S'arrêter à cette question serait ne pas voir que réinvestir aujourd'hui le domicile, y compris dans sa fixité, dans sa pesanteur spatiale, ne signifie absolument pas le retour à une situation *ex ante*. La maison connectée est certes toujours une maison, mais une maison largement augmentée, et donc transformée. Comme le smartphone a pu être un instrument de repli, un « cocon », malgré sa capacité inouïe à la connexion (littéralement) tous azimuts et sa batterie nous libérant des attaches filaires, la *smart home* est une *home* sans forcément rester le donjon de la vie privée dont les murs bien concrets étaient la condition et le symbole quasi sacré d'une rupture entre le vaste monde et nos mondes individuels ou familiaux.

Reconnaître cet état de fait, ce n'est cependant pas renoncer à toute forme de privacité au nom d'un dogme tout aussi abusif de la connexion à outrance. On doit pouvoir choisir d'ouvrir une brèche dans cette muraille en y perçant une fenêtre, et sans forcément l'abattre tout entière.

Partie 3 - LA VIE PRIVEE : PARADOXES D'UN COMPROMIS QUOTIDIEN

L'augmentation numérique des espaces publics s'étend de plus en plus aux espaces privés, que leurs habitants équipent désormais des nouveaux dispositifs sédentaires de l'IoT. Le *smartphone* avait déjà initié cette tendance comme appareil portable personnel doté d'importantes capacités de connexion, de captation et de computation, utilisé autant au logis que dans l'espace public. Dans le même temps, la vie privée continue d'être présentée comme une valeur importante et à protéger des immixtions extérieures par des internautes globalement conscients des risques liés à l'informatique ambiante. De nombreux observateurs voient là une contradiction fondamentale dans laquelle il serait possible de déterminer quel intérêt des utilisateurs prime en rendant compte de leurs pratiques effectives plutôt que de leurs discours. Mis dans une situation de choix non idéale, l'utilisateur arbitre entre ses différents intérêts, et accepte certains compromis qui permettent d'établir l'ordre de ses priorités réelles. Dans le contexte qui nous occupe, si la vie privée est une valeur apparemment si importante et que la logique immunitaire est fondamentale dans nos être-au-monde, pourquoi tant d'individus acceptent de « renoncer » à leur vie privée et à livrer tant d'informations personnelles aux entreprises du numérique, GAFAM en tête ? N'y aurait-il pas ici un *privacy paradox*, un paradoxe de la vie privée ? Contre cette grille de lecture qui tend à présenter les utilisateurs des TIC comme fondamentalement inconséquents avec leur vie privée, je proposerai plutôt de lire cet état de fait comme le résultat d'un chantage continuel qui leur est fait (chapitre 1).

Ce chantage s'appuie notamment sur la disproportion scalaire entre les acteurs économiques collectifs et les utilisateurs individuels, dans un contexte où la numérisation du monde force ces derniers à des compromissions plutôt qu'à de simples compromis. Pour autant, la vie privée comme processus immunitaire ne se déploie pas uniquement à son échelle la plus élémentaire, l'individu, elle écume aussi à l'échelle collective des groupes civiques : le consommateur particulier est aussi un citoyen dont les intérêts sont portés par des institutions publiques ou des associations (chapitre 2). Nous verrons d'abord que la loi et la régulation sont

déterminantes, *a fortiori* avec l'entrée en vigueur du règlement général pour la protection des données (RGPD) dans l'Union européenne en 2016. L'augmentation numérique en cours de l'espace domestique en tant qu'espace emblématique du privé permet d'observer comment la thématique de la vie privée est prise en compte aujourd'hui par ces acteurs. Il s'agit d'un moment de mise à l'épreuve du privé, où émergent de nouvelles tensions et de nouveaux contextes, pour reprendre les cadres notionnels de Rey et Nissenbaum (voir « La vie privée en situation », p. 58). Nous verrons que les entreprises peuvent être intéressées à la défense de la vie privée, en contradiction apparente avec leurs intérêts économiques. Je présenterai à cette fin les résultats, certes mitigés, d'une recherche-action menée en 2018.

Nous verrons enfin qu'une solution technique prenant en compte la dimension spatiale de la circulation des données existe à travers le traitement local des captats et requêtes par les assistants connectés (chapitre 3). Le traitement local des données peut apparaître comme une manière de redonner de la consistance aux murs du logis au niveau logiciel, dans une forme de retour au paradigme topographique classique du domicile. Appliqué à des technologies numériques qui en rendaient les limites poreuses, ce principe concilierait l'émergence des nouvelles pratiques de l'IoT domestique avec des « normes » sociales (au sens de Nissenbaum) déjà bien établies. Il s'agirait en somme de transposer au logiciel les formes historiques de l'immunité domestique. Ce qui pourrait apparaître comme une martingale appuyée sur les principes de la *privacy-enhancing technology* se heurte néanmoins à des difficultés de faisabilité et d'adoption par les utilisateurs eux-mêmes.

Chapitre 1 - LE CHANTAGE DU PRIVACY PARADOX

I - CECI N'EST PAS UN PARADOXE

La première réflexion sur la notion de *privacy paradox* a été faite en 2001 par Barry Brown[401], du département de recherche de l'industriel Hewlett-Packard à Bristol[402]. Brown n'était pas initialement focalisé sur la notion de vie privée, mais sur « l'expérience » en ligne des utilisateurs (« *Studying the Internet Experience* ») en fonction de l'ergonomie générale des sites web, et pour le commerce et les communautés sociales en particulier. C'est surtout en ce qui concerne le commerce en ligne que des réserves ont été émises par les enquêtés de Brown en termes de vie privée.

Le premier risque perçu par eux était d'abord la possibilité d'une utilisation frauduleuse de leurs données, bancaires notamment. En ce début des années 2000, la pratique du commerce en ligne restait assez nouvelle, et la confiance dans le paiement en ligne restait à construire contre un « discours médiatique »[401] plutôt anxiogène. La construction de cette confiance passe selon Brown par des expériences positives rapportées par des pairs et, plus fortement encore, par des expériences personnelles positives qui rendent le processus habituel. Cette crainte ne semble plus aujourd'hui fondamentale dans la détermination des conduites des internautes, bien que le risque soit toujours identifié comme un risque. Dans une enquête commanditée par la société d'informatique Unisys en 2015, « une part importante des répondants s'attendent également à des violations de leurs données personnelles dans les secteurs de la banque et de la finance (50%), du commerce de détail (44%), des services publics (43%) et au niveau des administrations publiques (41%). »[403] Il n'est cependant pas fait de distinction de degré entre

[401] B. BROWN, *Studying the internet experience*, Bristol (Royaume-Uni), HP Laboratories, 2001, p. 16. Traduction personnelle.

[402] Cette antériorité est notamment identifiée par Spyros Kokolakis dans son article de revue de littérature sur la notion. Voir S. KOKOLAKIS, « Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon », *Computers & Security*, vol. 64, 1er janvier 2017, p. 123 (en ligne : https://www.sciencedirect.com/science/article/pii/S0167404815001017)

[403] Le sondage semble avoir été fait auprès d'un millier de personnes en France, sans beaucoup plus de précisions : « L'enquête Unisys Security Insights est un sondage mondial fournissant des informations détaillées sur les attitudes des consommateurs concernant une variété de problématiques de sécurité. L'enquête a été réalisée entre avril et mai 2015 par Lieberman Research Group en Amérique Latine, en Europe en Malaisie et aux États-Unis, et au moyen de sondages en Australie et en Nouvelle-Zélande. Les réponses proviennent de 11 000 personnes dans 12 pays : l'Australie, le Brésil, la Colombie, la France, l'Allemagne, la Malaisie, le Mexique, les Pays-Bas, la Nouvelle-Zélande, l'Espagne, le Royaume-Uni et les États-Unis. » Voir « Une enquête d'Unisys révèle qu'une écrasante majorité de Français sont préoccupés par la collecte et l'utilisation de leurs données personnelles via Internet », sur *Unisys*, 20 juillet 2015 (en ligne : https://www.unisys.com/fr/news-release/fr-unisys-security-insights/ ; consulté le 27 septembre 2019)

les risques encourus : il est finalement assez courant que des bases de données incluant des informations à caractère personnel soient piratées, mais assez rares que les données bancaires des clients soient compromises par ce biais. Et comme Brown le disait déjà en 2001, les banques couvraient financièrement leurs clients contre ces fraudes[404]. Du reste, l'utilisation frauduleuse par des tiers de données bancaires relève moins d'un problème de vie privée que du vol pur et simple. Dans la taxonomie de Solove, l'utilisation frauduleuse de données bancaires peut être considérée du point de vue de l'acteur traitant de ces données bancaires, ou de celui du voleur. Dans le premier cas, cette pratique relève de la catégorie « traitement de l'information » et en particulier de l'« *insecurity* » en ce qui concerne l'acteur traitant des données[405], mais le voleur n'est pas en soi impliqué dans un problème de vie privée s'il ne traite pas lui-même la donnée à la base, il est comme hors-cadre. Un tel vol relèverait également de la catégorie « dissémination de l'information » et de la pratique d'« appropriation » en cela que l'identité du « sujet des données » (numéro de carte de crédit d'une personne et son code associé) est utilisée « pour servir les buts et intérêts d'un autre »[406], sous la forme d'un vol d'argent. Dans ma propre enquête, cette inquiétude est mesurée par les questions « Avez-vous déjà renoncé à un achat parce que vous n'aviez pas suffisamment confiance au moment du paiement ? » et « Avez-vous déjà souscrit à un service de sécurisation de paiement en ligne, par exemple avec un procédé qui évite de communiquer votre numéro de carte habituelle ? », tirées du questionnaire du Crédoc pour son rapport annuel *Baromètre du numérique*. Cette inquiétude n'est plus majeure pour mes enquêtés, ni, quoique dans une moindre mesure, pour l'ensemble des Français[407].

Mais le principal intérêt de l'article de Brown est dans sa formalisation de ce qu'il présente dans cet article comme un paradoxe :

> *« Bien que les individus tendent à décrire une peur générale envers « Big Brother » ou contre les atteintes à leur vie privée, ils n'en sont pas moins tout à fait disposés à donner des informations détaillées à propos d'eux, pourvu qu'ils y trouvent quelque bénéfice. On le voit à leur utilisation de cartes de fidélité tous les participants, à une exception, possèdent une carte*

[404] B. BROWN, *Studying the internet experience*, *op. cit.*, p. 17
[405] « L'insécurité implique un manque de soin apporté à la protection des informations stockées contre les fuites et les accès non autorisés », trad. pers. de « *Insecurity involves carelessness in protecting stored information from leaks and improper access* » D. J. SOLOVE, *Understanding privacy*, *op. cit.*, p. 104
[406] « *Appropriation involves the use of the data subject's identity to serve another's aims and interests*. », trad. pers., *in Ibid.*, p. 105
[407] *Baromètre du numérique 2021*, *op. cit.*

de fidélité d'une sorte ou d'une autre, et qu'ils utilisent pour des achats dans les magasins conventionnels. Même celles et ceux qui s'étaient plaints au nom de leur vie privée auparavant semblaient satisfaits que leur consommation soit suivie au moyen de cartes de fidélité. »[408]

Cette première formalisation du *privacy paradox* est certes faite à partir de l'exemple des cartes de fidélité utilisées dans les magasins physiques, mais s'appliquent également aux pratiques en ligne qui sont le thème plus général de l'article de Brown. Il poursuit à la page suivante en parlant de « ce qui se présente peut-être comme une sorte de paradoxe » dans lequel des personnes se disant attachées à leur vie privée sont prêtes à la sacrifier pour « un tout petit gain »[409], formulations à la tournure implicitement critique. L'auteur esquisse trois solutions à ce paradoxe. D'abord, citant Isaacs et Tang à propos de la captation vidéo[410], il pointe qu'on peut désirer conserver le contrôle sur son image ou ses données, quand bien même pour décider de les partager *in fine*. Il évoque ensuite la possibilité que certaines informations soient jugées triviales, en l'espèce l'historique des achats faits en association avec une carte de fidélité, et que les discours sur la vie privée tenus par ses enquêtés puissent porter sur d'autres informations ou types d'information plus sensibles.

Mais l'hypothèse sur laquelle Brown insiste le plus est que les internautes pourraient en fait penser qu'ils « doivent » (« *should* », dans l'article original) mettre en avant leur intérêt pour la défense de leur vie privée avant tout « pour apparaître comme des individus raisonnables »[411]. Pour Brown, il y a moins paradoxe qu'insincérité des utilisateurs dans le fait qu'ils accordent une grande importance à leur vie privée, insincérité que Brown prétend mesurer empiriquement en voyant pour quel maigre prix les utilisateurs sont prêts à renoncer à des informations personnelles. L'auteur fait même le parallèle avec la théorie du vote caché dans

---

[408] « *Indeed, while individuals would describe a general fear of "big brother", or having their privacy infringed, they were still perfectly willing to give their personal details out so long as there was some advantage to this. This can be seen in the participants' use of loyalty cards – all of the participants except one had some sort of loyalty card that they used when making purchases in conventional stores. Even those who had previously complained about their privacy appeared happy to have their shopping tracked with a loyalty card.* », trad. pers. *in* B. BROWN, *Studying the internet experience*, *op. cit.*, p. 17

[409] « ***This perhaps presents something of a paradox****, in that while our participants seemed to be willing to volunteer general worries about privacy, in turn* ***they were also willing to lose that privacy for very little gain.*** », trad. pers. *in Ibid.*, p. 18

[410] E. ISAACS et J. TANG, « Studying video-based collaboration in context: from small workgroups to large organisations », dans K. Finn, A. Sellen et S. Willbur, *Video Mediated Communication*, Mahwah (Etats-Unis), Lawrence Erlbaum Associates, 1997

[411] Trad. pers. i*n* B. BROWN, *Studying the internet experience*, *op. cit.*, p. 18

l'étude des résultats électoraux, qui correspond à l'hypothèse selon laquelle des électeurs pourraient mentir sur leur intention de vote en public ou à un institut de sondage avant de révéler leur vraie nature dans le secret de l'isoloir – le cas a typiquement été envisagé pour le vote d'extrême-droite, qui peut être difficile à assumer en public.

Brown est en revanche beaucoup plus direct sur le contexte et même sur l'agenda dans lequel il se place pour développer cette idée : « Les résultats qu'une étude comme la nôtre met au jour sont des résultats qui doivent servir au design. Dans le cas présent, les résultats discutés ici ont été produits pour explorer les opportunités offertes par les nouvelles technologies d'Internet. Nous mettons ici l'emphase sur ce que l'on peut apprendre des expériences-utilisateurs et sur la manière dont nous devons designer les technologies pour accompagner ces activités »[412]. En tant que chercheur en R&D dans la section « *Publishing Systems and Solutions* » aux Hewlett Packard Laboratories de Bristol depuis 1995, on peut faire l'hypothèse que Brown n'a jamais tant cherché à accompagner la réflexion sur la protection de la vie privée des internautes, mais bel et bien à justifier le fait qu'il ne s'agissait pas d'une orientation stratégiquement intéressante pour son employeur. Même si son concept a connu un certain succès dans la littérature scientifique[413], il s'agit en fait essentiellement d'un réquisitoire contre une préoccupation présentée comme une baudruche.

En somme, la prémisse même du papier de Brown (il faut avant tout développer de nouveaux usages) ne pouvait que mener au *privacy paradox*, puisqu'il s'agissait avant tout de justifier la mise en œuvre de nouveaux usages commercialement exploitables par Hewlett Packard, idéalement sans friction éthique ou réglementaire. Brown ne prend pas au sérieux l'ambivalence sous-entendue dans le terme de paradoxe, et l'argument de la vie privée avancé par les personnes qu'il interroge ne lui semble pas même vraiment relever de la dissonance cognitive, comme cela sera davantage le cas chez d'autres auteurs reprenant le terme par la suite. Selon Brown, il s'agit au mieux d'un écran de fumée, d'un vœu pieux, et au pire d'une complète hypocrisie plus ou moins inconsciente de la part des utilisateurs. Il ne manque pas de sel que le premier article à évoquer le *privacy paradox* ne le traite pas lui-même comme un paradoxe, employant le terme de manière trompeuse en postulant plutôt une hypocrisie fondamentale des utilisateurs de services numériques.

---

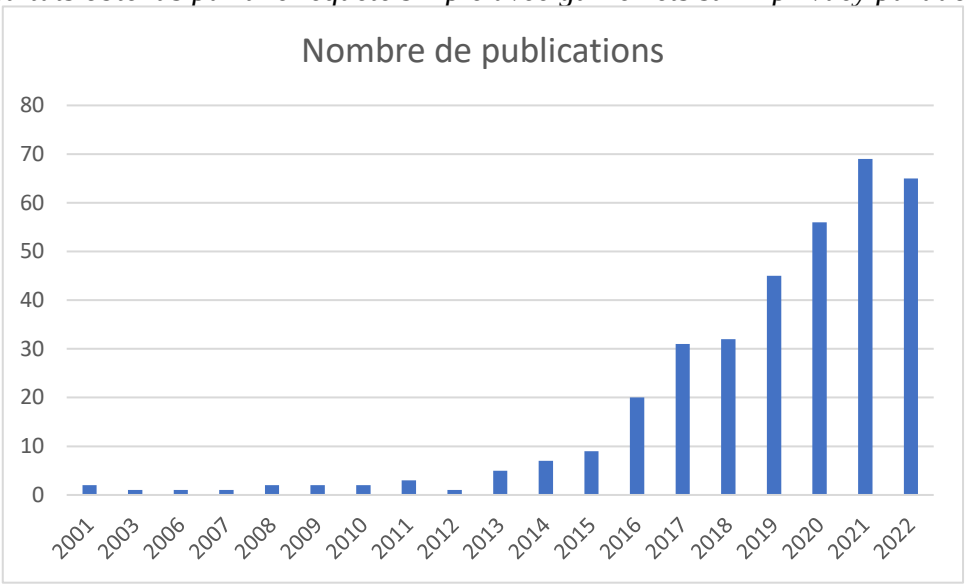
[412] « *The results that a study such as this one uncovers are therefore results for design. In this case, the results discussed here have been produced so as to explore the opportunities for new internet technologies. The emphasis here is on what we can learn about users experiences and how we might design technologies to support these activities.* », trad. pers. *in Ibid.*, p. 4

[413] S. KOKOLAKIS, « Privacy attitudes and privacy behaviour », *op. cit.*

Il n'en reste pas moins que la thématique a concerné 354 publications recensées par *Web of Science* entre 2001 et 2022, surtout dans le domaine de l'informatique (137 publications), suivi immédiatement par le marketing (89) et la communication (58). À partir de 2013, cette tendance est nettement croissante, avec un maximum de 69 publications en 2021 (voir Figure 20). La question reste importante en 2022 à 65 occurrences, avec néanmoins une légère baisse par rapport à 2021.

Figure 20 - Nombre de publications sur le privacy paradox par année dans Web of Science au 9 janvier 2023

Résultats obtenus par une requête simple avec guillemets sur « privacy paradox »



II - TENSIONS DU PRIVE ET DISSONANCE COGNITIVE

Le discours qui affirme qu'il y aurait un « paradoxe », une hypocrisie des utilisateurs quant à l'utilisation de leurs données personnelles et à l'importance qu'ils accordent à leur vie privée sert d'abord les intérêts économiques des entreprises qui trouvent un intérêt à exploiter ces données. Le premier article qui a formulé ce paradoxe ne visait donc pas véritablement à l'intellection de ce paradoxe. L'expression n'a-t-elle pour autant aucun sens ?

Quoique la genèse du concept me semble en invalider largement la portée heuristique, certains auteurs ont cherché à quantifier très pragmatiquement la valeur financière accordée par les individus à leur vie privée. Un résultat de cette approche économiste du *privacy paradox* qui a connu un certain succès médiatique au-delà du champ de la recherche est celui de Carrascal *et al.* (2013), qui ont évalué à 7 € la valeur effective de leur historique de navigation et à 25 € pour leurs données d'état-civil auprès de 168 internautes espagnols dont l'activité en ligne a été monitorée durant quelques semaines au moyen d'un plug-in installé dans leur navigateur web, selon le principe de l'enchère inversée[414]. La conclusion qui en a été tirée est que les internautes donnent à ces données la valeur d'un sandwich Big Mac de la chaîne de restauration rapide Mc Donald's, comme l'indique le titre de l'article présentant ces résultats. Cette conclusion a été assez largement reprise dans la sphère médiatique, comme dans un éditorial de Jean-François Codère, journaliste de *La Presse*, cette fois-ci pour évoquer le prix (un Big Mac) pour lequel les gens seraient prêts à céder un échantillon de leur ADN[415]. Il ne s'agit pas ici de nier cette réalité : il y a bien souvent une disjonction entre le discours et les actes individuels quant à la défense de la vie privée. Plus exactement, et pour reprendre Calvin Gotlieb dans un texte encore antérieur à l'article de Brown : « la plupart des personnes, quand d'autres intérêts sont en jeu, n'accordent pas suffisamment d'importance à la vie privée pour lui donner une valeur »[416]. Il ne s'agit donc pas de dire que les gens mentent quand ils disent accorder de l'importance à leur vie privée, mais que cet enjeu leur semblera généralement trop vague lorsqu'il est mis en concurrence avec d'autres intérêts plus immédiats, comme une rémunération financière ou en nature. C'est d'ailleurs ce que confirme E11, une des enquêtées à la fois les plus fatalistes vis-à-vis de la vie privée, et des plus enclines à profiter des services numériques commerciaux qui exploitent des données personnelles :

> « Ce que je veux dire, c'est que, comment... justement, je pense que les gens sont peut-être moins inquiets quand ça répond vraiment à une demande.
> JF: (acquiesce)
> E11: Le côté suspicieux il arrive vite quand on... il va s'essouffler quand, en fait, on y trouve notre compte.

---

[414] J. P. CARRASCAL *et al.*, « Your browsing behavior for a Big Mac : economics of personal information online », dans *Proceedings of the 22nd international conference on World Wide Web*, New York (ÉUA), Association for Computing Machinery, 2013, p. 189-200 (en ligne : https://doi.org/10.1145/2488388.2488406 ; consulté le 2 juin 2022)

[415] J.-F. CODERE, « Don d'ADN pour un burger », *La Presse*, 26 avril 2014 (en ligne : https://plus.lapresse.ca/screens/4c47-b330-5357ba5b-b386-2311ac1c6068|6HlR00chIHX~.html ; consulté le 2 juin 2022)

[416] « most people, when other interests are at stake, do not care enough about privacy to value it. » trad. pers. *in* C. C. GOTLIEB, « Privacy: A Concept Whose Time Has Come And Gone », dans D. Lyon et E. Zuriek (éd.), *Computers, Surveillance, and Privacy*, s. l., 1996 cité par D. J. SOLOVE, *Understanding privacy*, *op. cit.*

JF: Ouais.
[690,9] E11: Si par exemple on y trouve pas son compte on pourrait faire "ahhh", là, avoir un peu des doutes, enfin je sais pas, vous voyez ce que je veux dire ?» (entretien 7, 10 min)

Dans son cas, « y trouver son compte » ne renvoie pas forcément à un gain financier, et elle développe assez longuement sur les découvertes intéressantes qu'elle a pu faire, par exemple sur Spotify en ce qui concerne la musique, grâce aux recommandations algorithmiques de cette plateforme de *streaming**.

Pour autant, ce pseudo paradoxe me semble trouver rapidement ses limites.

D'abord, il n'est pas si universel que l'avance Brown, et sa généralisation est contestable y compris dans les termes d'un échange contre des avantages plus aisément mesurables. Il est d'ailleurs amusant que deux de mes propres enquêtés se soient inscrits en faux contre le *privacy paradox* dans la situation même que décrit Brown dans son article :

« E18: Je sais pas, on a acheté un truc un peu cher, ça valait le coup de prendre une carte de fidélité, donc on se dirige vers le...
E19: Ah oui ! C'était au Printemps, ça y est, je vois ce que tu veux dire.
E18: On prend mon nom, prénom, mon adresse, tout ça, téléphone, c'est obligatoire, et après elle m'a demandé ma tranche de revenus. Et E19 a répondu...
E19: Oui, c'était moi ! J'ai dit "et puis quoi encore ?". Mon groupe sanguin, la date de ma dernière vaccination antitétanique ?
JF: (rire)
E19: Enfin...
E18: Et du coup, on n'a pas pris la carte.
E19: (continuant) Le niveau de ma glycémie ?
[7241,5] E18: Je leur avais donné mon téléphone, mais déjà c'était...
E19: Déjà... moi je réagis assez mal (je pouffe) quand j'ai ce genre de demandes.
E18: Et après, moi, quand elle a demandé le salaire...
E19: Bah, "allez vous faire voir". C'est bon, on va payer 10 % de plus. » (entretien 12, 2 h 0 min)

Dans cet échange qui concernait littéralement le cas paroxystique décrit par Brown, à savoir le recours à une carte de fidélité permettant au vendeur de mieux tracer les achats de ces clients en l'échange d'un rabais sur leur achat (ici onéreux), les enquêtés E18 et E19 ont fini par refuser la carte et le rabais précisément parce qu'ils estimaient que trop d'informations leur étaient demandées. Ils n'étaient pas même contre le principe général de la carte, puisque E18 indique même avec un peu de honte qu'il avait déjà donné son numéro de téléphone, en plus d'informations d'état-civil. Mais au moment de communiquer en plus leur tranche de revenus, ils ont renoncé à la carte de fidélité. Il leur est difficile de dire si c'est la nature de cette

information ou l'accumulation de questions qui a précipité ce choix – du reste, on peut signaler qu'ils m'ont donné cette information sans difficulté en fin d'entretien. E19 conclue néanmoins sans détour « C'est bon, on va payer 10 % de plus. » Un autre enquêté, E5, qui est le plus au fait des pratiques de surveillance dont il peut faire l'objet, évite même d'utiliser sa carte bancaire : il s'agit ici moins de renoncer à un gain financier direct qu'à une modalité de paiement généralement pratique et rapide. Lorsque nous nous sommes retrouvés devant chez lui avant son entretien, il m'a indiqué avoir une course à faire au magasin du coin de la rue, et j'ai pu constater qu'il réglait en liquide. Après que je lui ai demandé si cette démarche avait un sens particulier, il m'a confirmé qu'il s'agissait pour lui de limiter l'exposition de ses habitudes d'achat, et que le paiement en espèces était la seule façon de régler anonymement. Tout aussi anecdotiques que les cas cités par Brown, ces exemples illustrent néanmoins qu'il n'est pas forcément évident que personne ne refuse le traçage ou la collecte de données, y compris lorsque ces données sont vénielles ou que cela leur offrirait un gain immédiat de quelques dizaines d'euros, ou de quelques secondes en caisse.

L'approche par les tensions ainsi que par l'intégrité contextuelle défendue par Bénédicte Rey ou Helen Nissenbaum est en fait beaucoup plus féconde et subsume celle du *privacy paradox*. Ainsi, E18 et E19 ont accepté de me communiquer une information, le niveau de leurs revenus, dans le cadre d'un entretien scientifique dont ils comprenaient la démarche et dont ils savaient qu'il ne donnerait pas lieu à une circulation préjudiciable de cette information, *a fortiori* car elle serait anonymée. Et ce, alors qu'ils ne retirent aucun bénéfice direct de cet entretien. Ils ont cependant refusé de la donner à l'employé d'un magasin Printemps car leur modèle de menace est surtout lié au *spam*, et que cette information leur semblait plus sensible dans ce contexte particulier. Même s'il n'est pas exclu qu'ils aient pu communiquer cette information à une entreprise commerciale pour un gain potentiel encore plus important, cette situation particulière est donc bien mieux décrite dans le cadre de l'intégrité contextuelle que par le *privacy paradox*. En outre, l'intégrité contextuelle permet de prendre également en compte la conscience plus ou moins grande qu'ont les utilisateurs quant à l'utilisation qui sera faite de leurs données : si E18 et E19 ne sont pas dupes et ont été d'autant plus rétifs à céder une information qu'ils jugeaient importante, bien des enquêtés ou des utilisateurs ne sont pas forcément conscients de ce qui peut être et de ce qui sera fait de leurs données – il n'est pas dit que leur consentement soit vraiment informé dans ce que le *privacy paradox* présente comme une simple transaction. Nous verrons plus longuement dans la sous-partie suivante qu'ils sont

même bien souvent induits en erreur dans ce domaine (voir « Tromper l'utilisateur aujourd'hui », p. 207).

En somme, du point de vue individuel, le *privacy paradox* pêche au minimum par excès de pragmatisme en ramenant tout au bénéfice direct voire au prix pour lequel des utilisateurs seraient prêts à céder des données personnelles. Les utilisateurs, comme la plupart des acteurs sociaux, sont effectivement pragmatiques, mais moins dans le sens où ils chercheraient à maximiser leur profit en toute chose qu'au sens où leurs actions suivent une rationalité qui leur est propre à partir des informations dont ils disposent. Ainsi, ce pragmatisme n'empêche pas de *valoriser* aussi certaines valeurs et d'agir en fonction d'elles. Cette approche pragmatique est bien identifiée par Kim Bartel Sheehan dans son article de 2011, *Toward a Typology of Internet Users and Online Privacy Concerns*[417]. Si les utilisateurs de services numériques ou numérisés sont prêts à céder certaines informations, c'est au fond comme n'importe quel individu voulant participer au « monde de la consommation », que ce soit en ligne ou hors ligne[418]. Sheehan ajoute que la perception de ce qui est privé est « hautement contextuelle » et variable selon les individus[419]. Sur cette base, Sheehan s'appuie sur un rapport d'Alan Westin pour la Federal Trade Commission des États-Unis publié en 1996, qui distinguait trois profils de personnes dans leur rapport à la vie privée en ligne. Les « fondamentalistes » ne sont prêts à aucun compromis ou presque, et très sourcilleux sur la manière dont leurs données sont collectées et utilisées. Les « non-concernés » se moquent de l'utilisation de leurs données, et adoptent peu ou prou l'attitude consistant à affirmer qu'ils n'ont « rien à cacher », selon une expression fréquemment utilisée – et déconstruite[420]. Le troisième profil regroupe le plus grand nombre de personne, les « pragmatiques » : il s'agit des personnes qui, sans se moquer de la manière dont leurs données seront collectées et utilisées, n'en utilisent pas moins des services numériques jugés utiles en arbitrant ces décisions au cas par cas. Sheehan se fonde sur une enquête par questionnaires pour tester l'hypothèse de chiffrage de Westin (voir Tableau 7). Fait intéressant, et congruent avec des études du même type faites avant la diffusion des TIC, les pragmatiques sont en fait largement les plus nombreux : c'est cette catégorie d'individus qui peut être le plus sujette à

[417] K. B. SHEEHAN, « Toward a Typology of Internet Users and Online Privacy Concerns », *op. cit.*
[418] « *many individuals realize that they have to give up some privacy to participate in the consumer world* » *in Ibid.*, p. 21
[419] « *It is also important to recognize that all individuals do not perceive privacy similarly, because privacy is highly contextual* » *in Id.* Il développe à la page suivante : « *The contextual nature of privacy is evident since concepts of privacy can change according to environmental and personal factors, so that individuals' desire for privacy is innately dynamic. Individuals are continually engaging in an adjustment process in which desires for privacy are weighed against desires for disclosure and personal communication with others* »
[420] D. J. SOLOVE, *« I've Got Nothing to Hide » and Other Misunderstandings of Privacy*, *op. cit.*

une forme de *privacy paradox*. Tantôt accepteront-ils des pratiques attentatoires à leur vie privée si le gain estimé est suffisant ou le risque perçu peu élevé, tantôt les refuseront-il si ces conditions ne sont pas réunies. Par définition, les deux autres groupes sont peu ou pas concernés : les fondamentalistes devraient refuser tout traçage quoiqu'il arrive, et les non-concernés l'accepter dans tous les cas s'ils y trouvent le moindre intérêt. Dans les faits, bien entendu, ces catégories ne sont pas si caricaturalement hermétiques, comme nous le verrons par exemple dans les rapports différenciés à la collecte audio ou vidéo parmi les enquêtés de la présente thèse, y compris chez des utilisateurs plutôt catégorisables comme non-concernés (voir « L'image considérée comme plus critique que le son », p. 281).

Tableau 7 - Répartition des profils d'individus selon leur rapport à la protection de leur vie privée en ligne d'après Westin (1996) et Sheehan (2006)[421]

Privacy concern: Typology comparison

Group	Westin	This study
Fundamentalists	25%	3%
Pragmatists	50%	81%
Unconcerned	25%	16%

Note. Chi squared = 24.035, $p < .0001$.

Enquête envoyée par courriel à 3724 choisis au hasard dans quinze pays, et à laquelle 889 ont entièrement répondu.

En tout état de cause, cette typologie introduit déjà plus de nuance dans l'appréhension des attitudes vis-à-vis de la vie privée que ne le fait le *privacy paradox*. Là où les tenants du *privacy paradox* traitent au fond tous les individus comme des non-concernés qui s'ignorent ou qui se cachent, le type de personnes le plus représenté est en fait celui des pragmatiques. Ni tout à fait fondamentalistes, ni tout à fait non-concernés, ils sont, ne serait-ce que par leur nombre, le groupe-clé dans la réflexion autour de la vie privée (voir « Présentation des enquêtés principaux », p. 431).

Un dernier élément à prendre en compte est que le *privacy paradox* aborde le problème de la vie privée sous un angle strictement individuel. Brown se demande ce que fait tout individu

[421] K. B. SHEEHAN, « Toward a Typology of Internet Users and Online Privacy Concerns », *op. cit.*, p. 27

isolé quand on lui propose d'échanger des informations personnelles contre un gain financier, et il en conclue que tous les individus agissent selon la même rationalité, à savoir contre leurs discours et intentions affichées. Ce faisant, il se focalise sur le rapport d'échange vie privée / service entre chaque individu et l'entreprise avec laquelle il *négocie* cet échange, sur le compromis qui est mesuré sous la forme d'un prix financier. Cette approche est biaisée à deux titres. D'abord, elle méconnaît la dissymétrie entre ces deux types d'acteurs : l'individu n'a que très rarement connaissance des enjeux de l'échange (que sera-t-il fait des données collectées pour établir sa carte de fidélité ?), et pas de réel pouvoir de négociation (l'offre est simplement à prendre ou à laisser). Un bon indicateur de cette dissymétrie entre ces deux types d'acteurs est le fait que les documents légaux relatifs à la vie privée des services numériques sont impossibles à lire en entier. Déjà en 2008, Aleecia MacDonald et Lorrie Faith Crannor estimaient entre 181 et 304 heures le temps de lecture de ces documents par an pour un Étatsunien moyen[422]. S'il est normal que ces conditions d'utilisation, rédigées par des juristes devant tenir compte d'un cadre légal plus ou moins contraignant dans le cas de l'utilisation de données personnelles, soient peu faciles à lire, le résultat n'en est pas moins que les utilisateurs ne peuvent matériellement pas lire ces documents, et finissent par ne plus vraiment s'en soucier. Dans une expérience conduite auprès de 543 participants croyant tester un nouveau réseau social fictif, Jonathan A. Obar et Anne Oeldorf-Hirsch ont ainsi mesuré que la plupart des utilisateurs acceptaient la politique de confidentialité sans la lire. Ceux qui la consultaient y consacraient en moyenne 73 secondes, pour un temps de lecture complet estimé à une trentaine de minutes. Au bout du compte, 97 % des utilisateurs acceptaient ces conditions, alors même qu'elles incluaient des clauses abusives, comme la communication des données collectées à leur employeur et à une agence de renseignement des États-Unis, voire franchement humoristiques, comme le fait que l'accès au service était conditionné au don d'un nouveau-né à l'entreprise[423].

Mais surtout, il s'agit de considérer des individus disparates face à des pratiques qui touchent en réalité des collectifs (groupes affinitaires, utilisateurs d'un service, citoyens d'une nation…) précisément pour atomiser les effets perçus de ces pratiques et les légitimer malgré

[422] A. M. MCDONALD et L. F. CRANOR, « The Cost of Reading Privacy Policies », *I/S : A Journal of Law and Policy for the Information Society*, vol. 4, nº 3, 2008, p. 563 (en ligne : https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf?sequence=1&isAllowed=y)

[423] J. A. OBAR et A. OELDORF-HIRSCH, « The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services », *Information, Communication & Society*, vol. 23, nº 1, Routledge, 2 janvier 2020, p. 128-147 (en ligne : https://doi.org/10.1080/1369118X.2018.1486870 ; consulté le 9 juin 2022)

leurs effets éminemment collectifs et politiques. Si les enjeux restent faibles quand on ne considère que la question de la souscription à une carte de fidélité dans un magasin physique, le problème n'est plus du tout le même quand on généralise cette approche du *privacy paradox* à toutes les situations comparables dans une ère numérique où la collecte d'informations personnelles se fait dans la quasi-totalité des espaces et à partir d'un nombre considérable (et croissant) de sources de données. Dans ce contexte, présenter la collecte d'informations personnelles devenue systématique comme une simple transaction occasionnelle de gré à gré ne sert qu'à en déguiser la dimension systématique et collective.

S'il est tentant de réduire au seul intérêt individuel la préservation d'informations qui sont, après tout, personnelles, la vie privée n'en est pas moins aussi un enjeu largement collectif. Ainsi, d'après Solove, « la valeur de la vie privée doit être déterminée sur la base de son importance pour la société, et pas uniquement en termes de droits individuels »[424] : ces deux facettes de la question sont même aussi importantes l'une que l'autre.

*

Au bout du compte, parler de *privacy paradox* aujourd'hui encore semble être de moins en moins pertinent, alors même que le terme est de plus en plus discuté dans la littérature scientifique. Au-delà du fait que la notion a été proposée par un auteur n'y croyant pas vraiment lui-même, sa valeur heuristique est quasi nulle. Elle vise avant tout à saper les bases de toute revendication quant à la vie privée au nom d'une approche prétendument pragmatique consistant à mettre en lumière l'absence d'un alignement parfait entre valeurs affichées et pratiques effectives des individus, alors que la base d'une approche réellement pragmatique des faits sociaux consiste justement à explorer de telles contradictions apparentes, qui sont bien plus souvent la norme que l'exception. Attendre des individus que leurs valeurs et leurs pratiques soient constamment alignées, c'est méconnaître cette évidence sociologique que la majorité de la population ne fait pas que ce qu'elle veut, mais qu'elle fait avec ce qu'elle a.

Plus encore, nous allons voir que le *privacy paradox* pris au premier degré résulte moins d'une hypocrisie généralisée des individus que d'une stratégie industrielle et commerciale des entreprises dont le modèle d'affaire repose sur l'exploitation des données personnelles, avant de voir comment une vraie prise en compte des enjeux de vie privée peut passer à travers des choix de design non-trompeur, et par la régulation.

[424] « *the value of privacy must be determined on the basis of its importance to society, not in terms of individual rights* » trad. pers. *in* D. J. SOLOVE, *Understanding privacy*, *op. cit.*, p. 10

III - TROMPER L'UTILISATEUR AUJOURD'HUI

La logique de discours derrière l'emploi de l'expression *privacy paradox* consiste à pointer l'inconsistance des revendications en matière de vie privée, qui seraient contredites par les pratiques individuelles qui n'en tiendraient pas vraiment compte. On a vu que la prémisse implicite d'une telle approche est la symétrie entre les individus et les entités à qui ils confient ou non des informations les concernant, entreprises au premier chef. Or, les individus n'ont qu'une très faible marge de manœuvre dans cette apparente négociation (bien souvent, accepter ou refuser les conditions fixées par l'entreprise), et ce simulacre de négociation lui-même n'a en fait presque jamais lieu comme dans l'exemple canonique de la souscription à un programme de fidélité, choisi par Brown en 2001.

Un indice que la captation et la circulation de données personnelles à partir de l'utilisation de services numériques ne relève pas d'un échange réellement sincère et informé est que les individus ne croient eux-mêmes pas toujours aux réglages de confidentialité de leurs services en ligne. Par exemple, alors même que je venais simplement de lui poser la question du choix qu'il ferait entre devoir communiquer son historique de navigation ou sa géolocalisation à un tiers fictif, E16 met spontanément en doute le fait qu'un réglage de navigation privée puisse être efficace :

> « E16: Si je devais choisir, clairement la géolocalisation. Garder mon historique privé, et vraiment privé, quoi, mais est-ce que l'historique est vraiment privé ? (petit rire) Bon, là on dépasse mais...» (entretien 10; 1 h 50 min 10 s)

Il développe ensuite plutôt sur la question de l'intérêt ou non de connaître la géolocalisation d'une personne, mais cette remarque est révélatrice d'une défiance. Sans que l'on puisse dire avec certitude ce à quoi pense E16 en demandant si cet historique est vraiment privé, par exemple s'il s'agit de savoir si l'on parle de son historique de navigation stocké localement sur son terminal ou s'il inclut également les diverses mesures de traçage par cookie ou directement en ligne, par son FAI ou des acteurs comme Facebook par exemple, qui peut suivre qui a visité les pages incluant des fonctionnalités de partage (« *like* », postage sur le profil…), le résultat est finalement le même : une forme de défiance généralisée contre l'idée que sa navigation en ligne puisse être véritablement privée, quelle que soit le moyen de la monitorer. Cette méfiance est également présente chez E20, qui ne croit même pas aux pages disant explicitement qu'elles ne traceront pas les données de leurs visiteurs :

> « Après donc ça c'est le premier problème, après histoire que Netflix garde mes données c'est dingue mais ça me choque même plus. C'est vrai quoi on sait tellement que toutes les entreprises stockent nos données, maintenant quand on va sur internet, maintenant il y a la bannière des cookies donc on sait qu'ils gardent tout enfin... que quelque part c'est de moins en moins choquant et c'est même triste de dire ça mais ...
> JF: Typiquement sur cette bannière de cookies est ce que tu vas aller sur les paramètres ?
> E20: Alors maintenant je mets toujours non, mais je crois que ça marche pas (elle rit)
> JF: Alors oui c'est compliqué mais
> E20: Bas il y a certains sites ou tu peux mettre 'non' donc moi je mets 'non' et tout disparait, je me souviens plus ce que ça fait enfin voilà. Non je ne vais pas paramétrer chaque fois. »
> (entretien 13 ; 43 min 10 s)

Elle s'efforce de « [mettre] toujours non » quand une bannière lui demande si elle accepte le dépôt de cookies sur son terminal, ce qui constitue un effort non-négligeable, et même alors qu'elle n'a pas confiance dans le fait que ce paramétrage ait une quelconque efficacité. Elle n'a du reste pas complètement tort : en 2019, la journaliste Elsa Trujillo rapporte qu'une plainte a été déposée auprès de la CNIL par le Centre européen pour la défense des droits numériques, connu sous le nom de NOYB (None Of Your Business), pour dénoncer plusieurs sites comme Allociné, CDiscount ou *Vanity Fair* qui ne tenaient pas compte du refus de leurs visiteurs et les traçaient quelle que soit leur réponse sur la bannière dédiée[425]. E20 parle même un peu plus loin d'un « ras-le-bol » quant à toutes les actions à faire pour s'assurer que ses pratiques en ligne se fassent dans le respect de sa volonté et de ses intérêts. Elle a le sentiment de devoir lutter contre les intérêts antagonistes de beaucoup de services qu'elle utilise, ce qui passe parfois par le renoncement à lire un site qu'elle consulte, typiquement pour une information derrière un *paywall* (une bannière invitant le lecteur à payer pour accéder au site) dont elle sait qu'elle pourra la trouver ailleurs, et parfois par un renoncement à ses principes, en acceptant par exemple l'enregistrement de cookies de traçage plutôt que de chercher à les paramétrer dans une interface volontairement peu ergonomique. On sent dans son propos un balancement entre la volonté de mettre en œuvre ses principes et une lassitude qui se traduit par un rapport pragmatique à ces dispositifs : « E20 (…) Après je suis pas très consistante et je le fais pas tout

[425] E. TRUJILLO, « Sur ces sites français, refuser les cookies ne suffit pas à ne plus être tracé », *BFM TV*, 10 décembre 2019 (en ligne : https://www.bfmtv.com/tech/vie-numerique/sur-ces-sites-francais-refuser-les-cookies-ne-suffit-pas-a-ne-plus-etre-trace_AN-201912100036.html ; consulté le 14 juin 2022)

le temps et c'est pas un soucis permanent et je pense à autre chose dans la vie, donc voilà ». (entretien 13, 44 min 50 s).

Au-delà de la question technique spécifique de ces exemples consistant à se demander si et comment l'historique de navigation est exploité, on peut replacer cette question dans le contexte plus large qui est celui de la *trace* numérique et de son exploitation. Évoquant la question des traces numériques en géographie dans un article éponyme, Mericksay *et al.* présentent « (…) la notion de trace et sa déclinaison géonumérique (…) selon quatre grandes perspectives permettant sa caractérisation

- flux / marque ;
- volontaire / involontaire ;
- implicitement géolocalisée / explicitement géolocalisée ;
- individuelle / agrégée »[426]

Si la trace est à la base un concept plutôt utilisé par les géographes dans un contexte territorial (les auteurs évoquent par exemple la trace de pas), son champ d'application s'est considérablement élargi avec l'émergence des technologies numériques. On peut désormais la définir « comme des données personnelles, descriptives de l'activité ou de l'identité d'un individu », « activité » qui ne se borne donc plus à l'espace territorial, et qui peut également renvoyer à la dimension idéelle de l'« identité »[427]. Dans ce contexte, il est particulièrement intéressant que la trace se caractérise, entre autres, selon l'opposition entre la trace volontaire (quand l'individu cherche à laisser sa marque) et involontaire (quand la traduction de l'activité de l'individu sous forme d'une trace se fait à son insu). Des quatre couples de caractéristiques d'une trace proposés par les auteurs, celui qui oppose volontaire et involontaire est probablement celui qui est le plus remarquablement déséquilibré aujourd'hui dans la production de traces numériques. Si l'on excepte des approches comme celle du *quantified self*, qui consiste à cumuler diverses mesures sur soi-même, comme avec les bracelets de suivi de l'activité de la marque sportive Strava évoquée par les auteurs au début de leur article, l'essentiel des traces collectées en ligne à propos des individus se fait aujourd'hui à leur insu ou, du moins, pas à leur initiative. Même dans ce dernier cas, l'exemple des bracelets Strava montre bien comment des

[426] B. MERICSKAY, M. NOUCHER et S. ROCHE, « Usages des traces numériques en géographie : potentiels heuristiques et enjeux de recherche », *L'Information géographique*, vol. 82, n° 2, 9 juillet 2018, p. 39-61 (en ligne : http://www.cairn.info/revue-l-information-geographique-2018-2-page-39.htm ; consulté le 5 octobre 2018)
[427] *Ibid.*, p. 42

traces volontairement produites par les individus peuvent être ré-utilisées par des tiers à l'encontre de leurs intérêts – en l'espèce, en permettant de suivre l'activité et les cheminements dans diverses bases étatsuniennes secrètes à partir des profils publics de personnes identifiées comme des militaires.

Malgré un cadre réglementaire de plus en plus contraignant dans le domaine de la protection des données personnelles (voir « De la loi informatique et libertés au RGPD », p. 223), la production, la collecte et le traitement de traces numériques est devenu si essentiel aux entreprises contemporaines s'inscrivant dans le capitalisme de surveillance que le design même des interfaces de paramétrage des services en ligne et des objets connectés en est considérablement affecté. Le terme de *dark pattern* a été formé par le designer Harry Brignull au début des années 2010 pour décrire les pratiques de design trompeuses visant à inciter les utilisateurs à faire des choix de paramétrage spécifiques, voire contraires à leurs attentes, en les guidant au moyen d'une interface prévue à cet effet. Brignull décrit par exemple le cas de l'interface du système d'exploitation des iPhones de l'époque, iOS 6, dans lequel les utilisateurs étaient induits à accepter le traçage de leurs activités sur leur s*martphone* à des fins publicitaires. La technique consistait ici à jouer sur une double négation : plutôt que de proposer une option positive et explicite de type « Suivi publicitaire » à activer ou à désactiver, selon les canons habituels du design utilisateur, il était proposé aux utilisateurs d'activer ou de désactiver une option « Limiter le traçage publicitaire » (« *Limit ad-tracking* ») : ainsi, les utilisateurs n'étaient pas incités à activer ou à désactiver le traçage publicitaire, sur le mode de l'interrupteur, mais à activer ou non la « limitation » du traçage publicitaire[428]. Pour Brignull, un *dark pattern* se définit ainsi :

> *« Un* dark pattern *est une interface-utilisateur soigneusement conçue pour piéger l'utilisateur de sorte à lui faire faire des choses qu'il n'aurait pas forcément faites, comme acheter une assurance en même temps qu'un objet, ou s'engager pour un paiement récurrent. Habituellement, on pense à un mauvais design comme le résultat d'une insuffisance ou d'une paresse de son créateur – mais sans mauvaise intention. Les* dark patterns*, quant à eux, ne résultent pas d'une erreur. Ils sont précisément recherchés sur la base*

[428] H. BRIGNULL, « Dark Patterns: inside the interfaces designed to trick you », *The Verge*, 29 août 2013 (en ligne : https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you ; consulté le 7 juin 2022)

d'une connaissance solide de la psychologie humaine, et n'ont pas l'intérêt de l'utilisateur pour finalité »[429]

L'intérêt de cette définition est d'affirmer que ce choix de design est volontaire, et malintentionné, ce qui est signifié par l'emploi du terme *dark* que l'on retrouve dans d'autres expressions dépréciatives telle que *dark web* par exemple[430]. En outre, elle constitue un argument puissant contre le *privacy paradox* en cela qu'elle met bien en évidence que les utilisateurs sont souvent moins négligents quant à la protection de leur vie privée que plus ou moins fortement incités à l'être. Si l'on reprend la typologie de Sheehan, les *dark patterns* sont conçus pour faire apparaître les pragmatiques comme des non-concernés, et les seules personnes qui feront l'effort de comprendre ces designs pour tenter de faire respecter leurs choix seront renvoyés, à juste titres, au nombre des fondamentalistes. Le danger du *privacy paradox* réside dans l'invisibilisation des pragmatiques, qui seraient à n'en pas douter beaucoup plus nombreux à assumer la même position que les fondamentalistes si ce choix ne leur était pas rendu si coûteux qu'ils en sont conduits à assumer celle des non-concernés.

Alessandro Acquisti et Jens Grossklags identifient cinq facteurs expliquant d'où provient cette distorsion entre les choix effectifs et les valeurs affichées des utilisateurs :

- « une information limitée, en particulier quant aux bénéfices et aux coûts », qui concerne les informations fournies par le prestataire de service,
- « une rationalité limitée » qui rend difficile l'évaluation de ces bénéfices et ces coûts par l'utilisateur lui-même,
- « les distorsions psychologiques », comme l'excès ou le manque de confiance en soi de l'utilisateur, sa propension à être influencé, d'éventuels comportements addictifs, etc.,
- « l'idéologie et les attitudes personnelles », notamment pour les personnes qui estiment que les garanties quant à leur vie privée ne doivent pas avoir de coût, mais plutôt être rendues obligatoires par l'État,

[429] « *A dark pattern is a user interface carefully crafted to trick users into doing things they might not otherwise do, such as buying insurance with their purchase or signing up for recurring bills. Normally when you think of "bad design," you think of the creator as being sloppy or lazy — but without ill intent. Dark patterns, on the other hand, are not mistakes. They're carefully crafted with a solid understanding of human psychology, and they do not have the user's interests in mind.* », trad. pers. *in Id.*

[430] J.-F. PERRAT, « Un "deep/dark web" ? Les métaphores de la profondeur et de l'ombre sur le réseau Tor », *op. cit.*

- « le comportement quant au marché », dans lequel il y aurait effectivement une valorisation supérieure du coût financier évité par rapport au coût symbolique des données personnelles[431].

L'information et la rationalité limitées et les distorsions psychologiques nourrissent plus particulièrement la défiance envers les prestataires quant à la gestion des données de leurs utilisateurs, parfois désignée par le terme de *techlash*.

La notion de *techlash*, qui désigne une méfiance grandissante des consommateurs à l'endroit des entreprises du domaine technologique, semble être un symptôme de la manière dont le *privacy paradox*, même pris au premier degré, pourrait être en train de se résoudre. Rana Foroohar en donne une définition pour la section « *Year in a Word* » fin 2018 dans le *Financial Times* :

> *« L'animosité générale croissante contre les grandes plateformes technologiques de la Silicon Valley et leurs équivalents chinois. »*[432]

Ce mot-valise formé sur *tech* (élision de *technology*) et *backlash* (retour de bâton) aurait été proposé par le journaliste Adrian Wooldridge en 2013[433] avant d'être de plus en plus repris dans la presse d'opinion jusqu'à sa consécration par le *Financial Times*. Il a également été un des finalistes du *Oxford Dictionary* là encore comme mot de l'année[434]. Il est aussi identifié dans certains travaux scientifiques ou dans la littérature grise, par exemple par Sanjay Nair à partir des résultats du Edelman Trust Barometer[435], et quoique *Web of Science* ne recense encore que quatorze occurrences du terme au 9 janvier 2023 (voir Figure 21).

[431] Trad. pers. *in* A. ACQUISTI et J. GROSSKLAGS, « Privacy attitudes and privacy behavior - Losses, Gains, and Hyperbolic Discounting », dans J. Camp et R. Lewis, *The Economics of Information Security*, Alphen aan den Rijn (Pays-Bas), Kluwer Academic, 2004

[432] « *The growing public animosity towards large Silicon Valley platform technology companies and their Chinese equivalents*. », trad. pers. *in* R. FOROOHAR, « Year in a Word: Techlash », *Financial Times*, 16 décembre 2018 (en ligne : https://www.ft.com/content/76578fba-fca1-11e8-ac00-57a2a826423e ; consulté le 15 juin 2022)

[433] A. WOOLDRIDGE, « The coming tech-lash », *The Economist*, 18 novembre 2013 (en ligne : https://www.economist.com/news/2013/11/18/the-coming-tech-lash ; consulté le 16 juin 2022)

[434] *Word of the Year 2018 - Shortlist*, Londres (Royaume-Uni), Oxford Languages, 2018

[435] S. NAIR, « Trust in Tech Is Wavering and Companies Must Act », sur *Edelman*, 8 avril 2019 (en ligne : https://www.edelman.com/research/2019-trust-tech-wavering-companies-must-act ; consulté le 23 mars 2022)

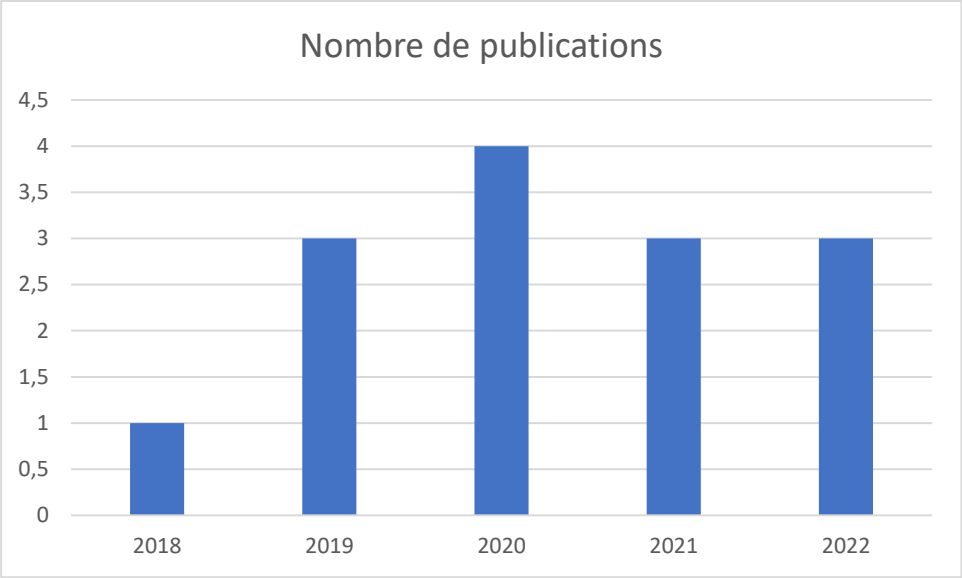


Figure 21 - Nombre de publications comportant le terme "techlash" sur Web of Science au 09/I/2023

En effet, si au premier degré le *privacy paradox* pointe l'écart entre les pratiques effectives et un sentiment général quant à la protection de la vie privée, pour laisser entendre qu'elle n'est pas une valeur aussi fondamentale que ce que prétendent les individus, le fait que ces mêmes individus en viennent aujourd'hui à se méfier de la technologie en général peut être vu comme la confirmation que le *privacy paradox* est à la fois bien compris et subi. Si sa première occurrence sous la plume de Wooldridge insistait davantage sur la problématique sociale de l'émergence d'un groupe de dirigeants d'entreprises richissimes de la Silicon Valley dans le contexte du mouvement *Occupy Wall Street*, le terme englobe aujourd'hui les réticences contre les produits et services logiciels créés par ces entreprises. Quoique Nair rapporte que le baromètre Edelman est encore globalement très favorable au secteur technologique (comparativement à l'indice de confiance envers les médias, par exemple), il rapporte néanmoins une part croissante de la catégorie « confiance faible » (« *weak trust* ») dans les pays développés, avec 61 % de réponses favorables dans la catégorie « les entreprises technologiques ont un trop grand pouvoir sur la diffusion de l'information », et 39 % de réponses favorables seulement dans la catégorie « les entreprises technologiques font passer les intérêts et le bien-être de leurs utilisateurs avant leurs profits »[436]. Cette défiance qui n'est encore probablement qu'un signal faible dans cette enquête par sondage est en tous les cas nettement représentée

[436] *Id.*

dans mon propre échantillon, y compris parmi certains utilisateurs que l'on peut considérer comme non-concernés.

Dans une longue tirade, E20 exemplifie de manière assez complète et articulée comment le *techlash* peut s'intégrer dans la réflexion des individus. Quoiqu'ingénieure et très au fait de la dimension technique comme des opportunités offertes par le numérique, elle reste assez méfiante quant à la sincérité et aux modèles commerciaux des entreprises. Son cas est donc d'autant plus intéressant qu'il n'y a chez elle aucune forme d'aversion de principe à la technologie en elle-même :

> « E20: alors, ça me gênerait moins. Dans le sens où je n'ai pas peur que quelqu'un vienne chez moi et pirate mes données. Ce n'est pas cette peur là que j'ai. Donc ça reste effectivement moins problématique. Là où ça ne fonctionnerait pas, c'est qu'en fait je n'ai pas confiance en l'acteur. C'est-à-dire que même s'il me dit que c'est en local, (elle hésite) si toi tu me dis que c'est en local, je vais te faire confiance. Si un acteur essaye de me vendre un produit en me disant « mais vous inquiétez pas c'est en local, on récupère rien » je ne leur fais pas confiance. Parce que je ne suis pas capable de juger et du coup, je ne saurais pas s'ils ont raison ou s'ils sont en train de m'arnaquer tu vois. (moyenne pause) Le problème ça va être...on en revient à la pub Apple. Le problème c'est que voilà : entre ce qui est annoncé, ce qui est vrai derrière, heu... Si je n'ai pas un acteur de confiance qui m'aide à mettre la barre. Et m'aide à me dire oui ou non. Par défaut, vu le climat actuel et vu ce qu'on sait actuellement, je serais sur de la non-confiance. Et pour remettre le curseur sur la confiance il va falloir... du concret ou pas d'ailleurs. Mais une information, autre que la boîte commerciale.»
> (entretien 13, 1 h 32 min 40 s)

Le point sur lequel elle insiste le plus est qu'elle n'a aucune confiance dans les informations fournies par « la boîte commerciale ». Il ne s'agit pas ici d'une défiance envers le commerce en général, mais bien du contexte logiciel où il est difficile de savoir ce qui est fait des données qui la concernent – quoiqu'elle ne le précise pas aussi frontalement, elle n'a sans doute pas de problème de confiance en ce qui concerne les produits numériques matériels : elle pourrait par exemple toujours vérifier elle-même que tel disque-dur dispose bien de l'espace de stockage annoncé sur son visuel commercial, on serait alors dans le registre de ce qu'elle appelle le « concret ». Le deuxième point intéressant est qu'elle place cette défiance dans un contexte temporel qu'elle présente comme particulier : « Par défaut, vu le climat actuel et vu ce qu'on sait actuellement, je serais sur de la non-confiance ». Dans la suite de l'échange, elle évoque notamment le cas d'Edward Snowden. Il faut rappeler par ailleurs que j'ai rencontré E20 dans un atelier de vulgarisation au logiciel libre et à la protection de la vie privée : elle est donc

largement sensibilisée à la question, et déjà dans une démarche active de prise de contrôle sur la collecte et la dissémination de ses traces numériques. En cela, elle valide donc l'idée que le *techlash* s'inscrirait dans un temps récent, peu ou prou depuis 2018, année durant laquelle un certain nombre de scandales autour des GAFAM ont justifié la reconnaissance médiatique du terme. Par ailleurs, elle rebondit ici sur l'exemple de la dernière publicité d'Apple à date, évoquée quelques minutes plus tôt, et qui s'inscrit dans la ligne *marketing* de l'entreprise consistant à se présenter comme un champion de la vie privée : on notera qu'elle n'accorde donc guère de confiance à cette ligne de conduite affichée.

IV - LES DIFFERENCES PERÇUES ENTRE LES DIFFERENTS ACTEURS PUBLICS ET PRIVES DE LA COLLECTE DE DONNEES

La notion de *techlash* s'applique aux grandes entreprises du numérique, GAFAM et BATX en particulier. Le secteur public n'est cependant pas épargné par une forme de défiance du public dans son utilisation des outils de surveillance électronique et numérique, qui précède même largement le *techlash* dans le temps (voir « Une demande sociale ancienne autour de la vie privée », p. 47). De fait, selon Jacob R. Appelbaum, « Les deux principaux adversaires en matière de surveillance sont les acteurs d'État et les entreprises, bien qu'il n'y ait parfois pas de différence significative entre eux »[437]. Ces défiances n'en prennent pas moins des formes différenciées, en particulier dans mon échantillon, là où la littérature scientifique anglophone semble moins nuancée.

La différence entre la surveillance numérique par des entreprises commerciales et par les acteurs publics semble de plus en plus ténue à David Lyon également : « (…) l'Internet est devenu un espace de surveillance qui abolit les distinctions entre le *monitoring* et les activités de traçage des agences de renseignement, de la police, des services *marketing* et publicitaires d'un côté, et les initiatives de surveillance de la vie quotidienne de l'autre. Les pratiques des agences de renseignement, de la police, des services *marketing* et publicitaires sont difficiles à

[437] « ***The two most prevalent surveillance adversaries are state [Gre14b] and corporate [Zub19, Int21a, Int21b] actors, though in some situations there is no meaningful distinction between these.*** *Fusion Centers [Wik21i] for example, are an American domestic intelligence apparatus that aggregates data provided by government agencies, corporations, and private persons, resulting at times in Americans being persecuted for engaging in constitutionally protected activities. Surveillance data of all kinds collected from other terrains [Goo21, War15b] readily merges into the Internet's IP traffic flows. This collection is not merely through passive observation of our communications, but also through active interaction and exploitation, along with analysis of behavioral data, other systems data, and data at rest.* », trad. pers., *in* J. R. APPELBAUM, *Communication in a world of pervasive surveillance: Sources and methods: Counter-strategies against pervasive surveillance architecture*, thèse de doctorat en mathématiques et informatique, Eindhoven (Pays-Bas), Technische Universiteit Eindhoven, 2022, p. 3

distinguer les unes des autres pour diverses raisons, dont les impératifs de secret commercial ou sécuritaire »[438]. De fait, la différence formelle entre ces différents types de surveillance est de moins en moins grande, tant du point de vue des techniques utilisées (captation audio et vidéo, traçage de l'activité en ligne, *machine learning*, profilage des individus…) que des sources de données. Les réseaux sociaux, par exemple, sont aujourd'hui utilisés par les services fiscaux français pour traquer les différences entre les trains de vie effectifs et déclarés d'éventuels fraudeurs. En ce qui concerne les enceintes connectées, elles ont été mobilisées à plusieurs reprises aux États-Unis déjà dans le cadre d'investigations criminelles. Au premier semestre 2022 aux États-Unis, un grand mouvement d'inquiétude publique quant à la possibilité d'avorter a également vu le jour autour de l'utilisation possible et avérée des données personnelles produites par des services commerciaux pour repérer et parfois retrouver physiquement les femmes susceptibles de se rendre dans un service médical pratiquant l'IVG, dans un contexte de remise en cause et de criminalisation de l'avortement[439]. En France, l'association de défenses des libertés civiles numériques la Quadrature du Net a développé à partir de mars 2018 un angle d'action autour de la « Technopolice » qui vise avant tout les pouvoirs publics, à savoir l'ensemble des moyens par lesquels « la Smart City révèle son vrai visage : celui d'une mise sous surveillance totale de l'espace urbain à des fins policières »[440], autrement dit les pratiques de surveillance médiées par le numérique et en direction des habitants dans l'espace public urbain. Pour autant, et malgré cette convergence générale entre les divers acteurs mobilisés du point de vue des moyens, ils semblent être aujourd'hui encore distingués du point de vue des finalités de cette surveillance.

---

[438] « (…) *the internet has become a surveillant space that also smudges the distinctions between monitoring and tracking activities of security agencies, police and corporate marketers and advertisers on the one hand, and the surveillance initiatives of everyday life, on the other. What security agencies, police and corporate marketers do is hard to discern, for a number of reasons, including agency and commercial secrecy* » *in* D. LYON, « Surveillance capitalism, surveillance culture and data politics », *op. cit.*, p. 65

[439] « Même si la pratique n'est pas encore généralisée, il existe déjà des cas, dans le système judiciaire américain, où des femmes ont été condamnées pour des avortements illégaux à cause de leurs activités en ligne : recherches sur Google, emails, discussions via des applications de messagerie, publications sur des réseaux sociaux, etc. Et au début du mois, Vice révélait qu'au moins un data broker (une société qui collecte et agrège des informations d'internautes via de nombreuses sources, afin de revendre ensuite des profils détaillés à des annonceurs et des entreprises) vendait des données de géolocalisation liées à des cliniques proposant des avortements. Permettant ensuite à d'autres entités de cibler ces personnes avec des publicités personnalisées, des contenus de désinformation, etc. » *in* L. RONFAUT, « L'avortement est un enjeu de cybersécurité », *Numerama*, 15 mai 2022 (en ligne : https://www.numerama.com/politique/960951-lavortement-est-un-enjeu-de-cybersecurite.html ; consulté le 16 juin 2022)

[440] LA QUADRATURE DU NET, « Manifeste », sur *Technopolice*, s. d. (en ligne : https://technopolice.fr/presentation/ ; consulté le 20 juin 2022). Ce manifeste a également été signé par quelques dizaines d'associations françaises dont notamment la Ligue des Droits de l'Homme et Attac, ains que par l'équivalent hollandais de LQDN, *Bits of Freedom*.

En ce qui concerne les grandes entreprises du numérique, la défiance est presque générale dans mon échantillon. Seuls deux enquêtés n'ont aucun problème avec le traçage de leurs activités en ligne, mobilisant l'argument selon lequel ils n'auraient rien à cacher. Pour les autres, même parmi les plus technophiles et non-concernés par les questions de vie privée, il y a au minimum une défiance contre le ciblage publicitaire. Pour les plus militants, toute forme de traçage est logiquement problématique, et ils s'en accommodent avec un certain fatalisme, au mieux, quand ils n'essaient pas activement de s'y soustraire pour l'un d'entre eux.

En revanche, et contrairement à ce qu'avance David Lyon, tous font assez bien la distinction entre surveillance publique et privée. E5 par exemple distingue captation vidéo individuelle au moyen d'un smartphone et captation vidéo publique ou parapublique installée dans l'espace. C'est la différence entre la circulation des données qui semble faire la différence : les données captées par un individu seront peut-être enregistrées sur un serveur de sauvegarde, au plus, mais les données collectées par la vidéosurveillance sont beaucoup plus susceptibles d'être ré-utilisées et, aujourd'hui, traitées par des logiciels de reconnaissance faciale qui garderont trace du passage de tel individu dans tel espace vidéosurveillé. De fait, à ma question sur le statut de la captation vidéo par une enceinte connectée dotée d'une webcam activée en permanence chez un particulier, il identifie cette situation comme un cas-limite entre les deux pôles constitués par la captation vidéo strictement individuelle et la vidéosurveillance à proprement parler. Au-delà de ce qui est fait concrètement des captats vidéo, et qui justifierait une différence de nature entre ces pratiques, « sur le fond » (voir ci-dessous), E5 évoque aussi plus prosaïquement la question de la différence d'habituation entre la vidéosurveillance dans l'espace public urbain et les nouveaux capteurs domestiques à moitié privés qui se généralisent aujourd'hui dans la domotique connectée à Internet :

> « La différence elle ne peut être que... comme ils sont intégrés dans le mobilier urbain, soit dissimulés à l'intérieur des panneaux, soit tellement présents que tu ne peux pas les voir... À un moment tu finis par être moins sensible parce que leur présence t'est soustraite. Tu ne peux pas l'apercevoir.
> JF: (acquiesce)
> E5: Mais l'enjeu est le même. De fond. » (entretien 3 ; 21 min 10 s)

L'habitude joue ici un grand rôle, puisque s'il reconnaît lui-même s'être presque habitué, malgré qu'il en ait, à la vidéosurveillance classique. Il est cependant à relever que, à d'autres moments de l'entretien, il redevient beaucoup plus véhément contre les nouvelles pratiques de vidéosurveillance plus ciblées, fondées sur la reconnaissance faciale ou associées au *tracking*

publicitaire. D'abord, parce qu'elles sont plus intrusives bien sûr, mais aussi parce qu'elles peuvent encore être combattues, et enfin parce qu'il n'a pas eu le temps de s'assagir à leur propos. Cette habituation à la vidéosurveillance se retrouve également dans le discours d'E20 :

> (…) Après dans un lieu public oui bah, quand il y a une caméra... après, je ne trouve pas ça non plus hyper agréable qu'il y ait une caméra, je ne crois pas ici qu'il y ait une caméra. ? (Elle cherche la caméra du regard) Si, il y a une caméra en haut.
> [501,6] [>JF?]: J'ai pas vérifié mais... (en parlant de la caméra) (…) Même dans un lieu public c'est gênant mais il y a un côté moins gênant ?
> [>E20]: Déjà maintenant on s'y est habitués, d'un côté, parce que même dans la rue, il y a quand même pas mal de caméras. Il y a un côté, enfin, un côté rassurant, alors les caméras dans la rue, il y a un côté un peu rassurant aussi ou je me dis le jour où il y a un souci enfin... c'est bête, mais quand je retire de l'argent je me dis c'est assez rassurant qu'il y ait une caméra. Bon, même si le jour où il y a un souci (inaudible, petit rire) mais voilà on se dit que... s'il y a un problème on peut retrouver les gens.
> (entretien 13, 8 min 20 s)

Elle aussi est ambivalente à ce propos, puisqu'elle trouve les caméras un peu « gênant[es] », mais elle estime que nous nous y sommes collectivement « habitués » et n'y fait plus très attention pour sa part. En outre, elle distingue clairement les espaces dans lesquels une telle surveillance est légitime : ce n'est que parce que la vidéosurveillance s'exerce dans un espace public (ou d'accès public, comme le guichet d'une banque) qu'elle l'accepte, là où elle exprimait quelques minutes avant l'extrait sa réticence envers la présence d'enceintes connectées tous micros ouverts dans les espaces privés qu'elle fréquente (et en particulier chez une amie proche à qui elle a fait déplacer sa Google Home dans la pièce voisine lors d'une visite). Enfin, elle signale bien qu'elle accepte d'autant mieux la vidéosurveillance que cette pratique lui semble d'un intérêt du point de vue de la sécurité ou des enquêtes policières – elle évoque notamment le cas alors tout récent de l'attentat à la bombe du 27 mai 2019 rue Victor Hugo à Lyon, dont l'auteur a été suivi sur plusieurs kilomètres par le réseau de vidéosurveillance de la ville.

De fait, la question de l'intérêt collectif de pratiques de traçage ou de surveillance au détriment de la protection de leur vie privée individuelle ne choque presque aucun enquêté de l'échantillon. Outre la question classique de la vidéosurveillance, E7 évoque par exemple l'optimisation des réseaux publics. Pourtant très méfiante vis-à-vis de la technologie et n'aimant pas être tracée en général, elle est beaucoup plus accommodante quand ce traçage est effectué de manière agrégée, d'une part, et pour optimiser un service public, comme elle l'explique à propos des transports en commun :

« E7: Parce que forcément, ils regardent bien tes données. Enfin, pas les tiennes, mais ils regardent bien le global pour savoir à quelle heure les gens rentrent, pour adapter les transports, des trucs, bon. Du coup c'est pour ça, d'un côté je me dis "oh, c'est énervant, mais en même temps ça fait partie du jeu, quoi". (pause) Je suis un peu partagée ! (rire plus franc)
E6: Moi le Navigo ça me gêne pas du tout. Pour le coup, non.
JF: (acquiesce)
E7: Sauf si tu étais un individu recherché ! (ton un peu dramatique) » (entretien 3, 36 min 19 s)

Bien qu'ils résident à Lyon, ce couple d'enquêtés évoquent le passe Navigo, à savoir le passe des transports en commun parisiens. Pour eux, les libertés individuelles en matière de protection de la vie privée n'ont rien d'absolu. Le fait que leurs données personnelles soient agrégées ou anonymées leur semble une condition nécessaire mais suffisante pour qu'elles puissent être utilisées par des acteurs rendant un service d'intérêt général. E6 évoque à nouveau le cas plus tard dans l'entretien, réaffirmant que l'anonymisation (il parle de caractère « impersonnel ») est nécessaire « E6 : Ouais. Après, encore une fois, c'est si c'est impersonnel. » (entretien 3, 2 h 1 min 45 s). En somme, il n'a rien contre le fait que son trajet quotidien pour se rendre sur son lieu d'études soit enregistré à condition qu'il soit anonymé.

Il est à noter que le fait de « ne pas être recherché » est spontanément évoqué par E7, comme E20 évoquait spontanément le terroriste de la rue Victor Hugo, ou E4 ceux du Bataclan (dans l'entretien 1). De manière générale dans l'échantillon, la distinction est nettement faite entre l'individu recherché et coupable, et l'individu sans histoire pris dans la masse des habitants de l'espace urbain. Les enquêtés acceptent bien, voire réclament, qu'il soit possible de retrouver le premier, à condition que la masse des suivants ne soient, après collecte et traitement de leurs données identifiantes initiales, envisagés précisément que comme une masse. En somme, et comme c'est d'ailleurs l'esprit des lois de protection de la vie privée depuis Informatique et Libertés et encore aujourd'hui avec la transposition du RGPD en France, la question de la finalité du traitement des données semble essentielle aux enquêtés. Les finalités d'intérêt général étant bien comprises et la plupart des enquêtés ayant une confiance élevée dans les institutions, il est finalement logique qu'ils soient nombreux à bien accepter les pratiques de traçage par les acteurs publics et parapublics, telles que les sociétés de transport en commun. E7 résume sa pensée dans une formule amusante et révélatrice vis-à-vis des institutions publiques comparativement au secteur privé :

« E7: (…) J'ai pas totalement confiance, mais je sais pas, c'est peut-être un truc un peu chauvin, c'est mon État (je ris) alors que Google c'est pas mon État, je sais pas

(sur un ton assez enjoué) »
(entretien 3, 1h 36 min 50 s)

Le cas de Linky, le compteur électrique connecté promu par ERDF au nom des possibilités nouvelles de pilotage du réseau électrique – et des économies afférentes qui seraient rendues possibles – est aussi intéressant : tous les enquêtés reconnaissent son utilité, malgré les réserves relayées médiatiquement en matière de vie privée ou même de santé du fait de l'émission d'ondes électromagnétiques lors des échanges entre le terminal et le réseau par courant porteur en ligne (CPL). Il est à noter que cette dernière réserve était inconnue des enquêtés à qui j'en ai fait part, à l'exception d'E16 qui ne s'en inquiète pas pour autant.

En somme, le *techlash* s'applique bien essentiellement aux GAFAM et entreprises du numérique qui, si elles fournissent à la rigueur des services gratuits à titre individuel aux enquêtés, sont plutôt perçues comme menaçantes ou prédatrices quant à leurs données personnelles. On peut d'ailleurs relever que ces réticences peuvent concerner des services dont on pourrait tout à fait les considérer comme d'utilité publique, et que leurs utilisateurs encensent. Un cas assez souvent évoqué par les enquêtés est celui de Google Maps, qui est directement évoqué 19 fois dans le corpus, dont 8 par moi. Il est spontanément évoqué par les enquêtés dans 5 entretiens sur les 7 dans lesquels le service est abordé. Il s'agit de l'un des services-phares de Google depuis plus de dix ans, et encore aujourd'hui du service *geoweb* grand public le plus utilisé au monde[441].

Seul E5 reste opposé à toute forme de surveillance collective, même publique, et y compris pour des raisons sécuritaires : il semble avoir fait sien les discours plus élaborés de militants et de chercheurs comme Appelbaum ou Lyon, et surtout d'Edward Snowden pour lequel il confesse une grande admiration.

« Oui ! Je crois que les deux côtés, il y a deux côtés de la surveillance : le commercial et le côté étatique.
JF: (acquiesce)
E5: ...qui sont liés de manière incestueuse, qui se nourrissent mutuellement. Donc, heu... Ce qui entre dans le canal de renseignement me semble une menace aux libertés, aux formes de gouvernement que nous avons construit au cours des siècles. Et ceux qui rentrent par la case du côté commercial, heu...
[2077,2] JF: Quand tu dis le renseignement, tu parles de mettre une *backdoor*, un

[441] « D'un simple point de vue technique, il est difficile d'ignorer les outils plébiscités par le public pour produire et visualiser ses données personnelles et dont la fluidité d'affichage, permise par des capacités de serveur énormes, est parfois meilleure que les solutions des professionnels. Les fonds de Google Maps ont aussi tendance à acquérir le statut de référentiel de localisation, malgré leur manque de précision parfois. » *in* T. JOLIVEAU, « Le géoweb, un nouveau défi pour les bases de données géographiques », *op. cit.*, § 17

truc direct ?
E5: Alors, c'est pas comment ça, c'est: quel est le but ? Donc, oui, que ce soit... Quelque chose fait par la NSA me semble une menace aux libertés ET ça alimente ces liens incestueux entre appareil militaire, paramilitaire et appareils commerciaux, capitalistes. Le complexe militaro-industriel. Ce qui rentre du côté publicitaire, commercial, finit par nourrir le premier. Parce que ce sont des silos de données, des océans de données qui sont ensuite pris par le... accaparés par les puissances analytiques de sécurité.
JF: (acquiesce)
E5: Donc il y a... Même si les canaux, les points d'entrée sont différents, je suis convaincu qu'il y a une porosité énorme (il insiste sur énorme) entre ces... océans de données qu'on collecte différemment. Même si on pouvait laisser l'enceinte Amazon... je me pose la question, et non. Je me pose même pas la question, pour moi c'est clair qu'il faut considérer que ça ça finit par rentrer dans les mains d'une force militaire avec des... ses objectifs propres. Donc ça finit par être une menace aux libertés via le... le coté des industries et des entreprises de la surveillance. » (entretien 2, 33 min 33 s)

On voit bien dans cet extrait long que sa pensée sur la question est très articulée, et très critique. Il évoque une relation « [incestueuse] » entre secteurs public et privée, pour appuyer sur le côté contre-nature de la « porosité » entre ces types de collecte de données. Snowden avait lui-même particulièrement tenu à mettre en lumière ces relations, et une bonne partie du choc provoqué par ses révélations tenait précisément au fait que les citoyens du monde se sont aperçus que leurs activités les plus vénielles médiées par des services non-étatiques finissaient par être analysées (certes le plus souvent de manière superficielle) par des agences de renseignement aux moyens techniques très considérables. À ma question sur les *backdoors*, à savoir une pratique de renseignement finalement très classique et descendante consistant à intégrer des mouchards pour ainsi dire officiels dans un code-tiers, E5 répond clairement qu'il ne s'agit pour lui-même pas de cela : c'est bien l'ensemble des jeux de données (« des silos de données, des océans de données ») produits dans des conditions normales d'utilisation des services qui sont mobilisées par les services de renseignement comme la NSA. Sur le point précis qui nous intéresse, les captats audio collectés par les enceintes connectées ne lui semblent pas devoir faire exception. Dernier point intéressant : E5 précise que le « moyen » l'intéresse moins que le « but ». Que les données des entreprises commerciales soient récupérées *via* une *backdoor* logicielle ou par une forme de *backdoor* légale n'est pas pertinent. Il pointe avant tout du doigt le fait que la logique de surveillance soit désormais généralisée, et qu'elle révèle « une menace aux libertés, aux formes de gouvernement que nous avons construit au cours des siècles ». Quoiqu'il soit très au fait des modalités techniques de la collecte et du traitement des données

personnelles issus de services commerciaux par les acteurs d'État (il évoque notamment les pratiques de l'entreprise Palantir à la suite de l'extrait), c'est avant tout une préoccupation plus générale quant aux libertés civiles et à la démocratie qui motive son inquiétude. À l'instar de Lyon, d'Appelbaum [442] ou de Snowden, c'est probablement aussi son tropisme vers les phénomènes observés aux États-Unis qui renforce cette méfiance envers la collusion entre les secteurs public et privé. Il ne s'agit pas de croire naïvement que l'État français serait moins prompt à la surveillance de masse, mais il est indéniable que les capacités techniques des États-Unis sont largement supérieures, d'échelle mondiale[442], et surtout mieux documentées. On peut faire l'hypothèse que c'est l'une des raisons pour lesquels les enquêtés de mon échantillon français conservent encore une certaine confiance envers les pouvoirs publics de leur pays.

*

Un pan non-négligeable de la pensée sur les données personnelles fait peser sur l'utilisateur final le renoncement à sa vie privée, qu'il monnaierait ou échangerait volontiers contre des services pour un prix modique. Nous avons vu que la réalité est beaucoup plus nuancée, ne serait-ce qu'en cela que les utilisateurs ont conscience de cet état de fait. Cette posture ambiguë relève bien davantage d'une forme de pragmatisme dans l'utilisation de services numériques toujours plus incontournables, et d'une forme de défaitisme quant à la possibilité de protéger sa vie privée en ligne du fait la dissymétrie des forces entre utilisateurs et fournisseurs de services, ces derniers recourant parfois même d'ailleurs à des pratiques déloyales voire manipulatoires afin de mieux profiler leurs utilisateurs. Pour autant, nous allons voir désormais que la puissance publique et les acteurs collectifs de la société civile ne sont pas dépourvus ni inactifs face à ces pratiques.

[442] Qui revendique cette focalisation sur les États-Unis : « *The perspective in this thesis is necessarily dominated by the United States of America, whose activities impact nearly every person on planet Earth. The focus on America is deeply political: it is the moral duty of every citizen of the United States to address serious faults in policy and to assist in the process of accountability.* » *in* J. R. APPELBAUM, *Communication in a world of pervasive surveillance*, *op. cit.*, p. VIII

Chapitre 2 - REGULER L'INTERNET DES OBJETS

Si la question de l'immunité concrète du privé des individus se joue effectivement à l'échelle de l'infinité écumante des microsphères des pratiques, une forme d'immunité collective se joue par la loi et les régulations à l'échelle des États, ou d'acteurs supranationaux comme l'Union européenne. La société civile est également impliquée à travers des associations ou des organisations parapubliques. L'implication d'acteurs d'échelle plus large permet ainsi de réduire la dissymétrie avec les acteurs économiques des TIC, et de sortir du débat sur le *privacy paradox* qui réduit la question de la vie privée à un choix individuel.

I - DE LA LOI INFORMATIQUE ET LIBERTES AU RGPD

La loi informatique et libertés et ses mises à jour

Dans l'approche contextuelle de Nissenbaum, les lois relèvent de ce qu'elle appelle la norme. Du fait de leur caractère écrit, elles sont les normes les plus explicites, et c'est en jouant sur leur caractère explicite qu'elles deviennent efficaces – face à une certaine forme de déloyauté, particulièrement des plateformes, quand elles ne sont pas explicitement régulées. Sans quoi, d'autres types de normes, « qui ne sont qu'implicitement comprises et acceptées », prennent le pas[443]. On l'a vu, c'est dans les années 1970, avec la montée en puissance de l'utilisation de bases de données informatisées par les États que les premières lois sur le sujet ont vu le jour, particulièrement la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés pour la France (voir « Une demande sociale ancienne autour de la vie privée », p. 47). Au-delà de la protection offerte au citoyen en matière d'inscription dans des fichiers de plus en plus souvent informatisés, on a vu que cette loi prévoyait également la création de la CNIL, dont les avis ont très tôt nourri la réflexion sur les usages nouveaux qui pouvaient être faits de l'informatique et de ces nouvelles données, comme dans le cas du projet AUDASS-Gamin. Plus largement, il faut rappeler que la loi informatique et libertés et la CNIL sont nées plusieurs années avant l'invention d'Internet, et même deux ans avant la sortie publique du Minitel. Il est donc tout à fait remarquable que cette loi et l'institution afférente

[443] « *Even with the focus narrowed to prescriptive norms, great variability in norm types remains. One dimension of variability that is relevant to contextual integrity is the degree to which norms are explicitly expressed in a given society, ranging from those that are* ***only implicitly understood and accepted****, to those that are explicitly formulated and sanctioned by authoritative individuals and institutions, to those that are explicit, formal, and enforced, such as norms embedded in formal legal systems*. », trad. pers., *in* H. F. NISSENBAUM, *Privacy in context*, *op. cit.*, p. 139

aient traversé la fin du XXe siècle et le début du XXIe sans évolution majeure. Quelques inflexions ont néanmoins été faites durant cette période.

La loi informatique et libertés elle-même est notamment modifiée et renforcée par la loi du 6 août 2004 transposant dans le droit français la directive 95/46/CE visant à harmoniser les droits européens en matière de protection de la vie privée. Elle est complétée par décrets le 20 octobre 2005 et le 25 mars 2007. Si la France avait été un des premiers pays d'Europe à se doter d'une loi informatique et libertés, elle est en revanche l'un des derniers à effectuer cette transposition. La directive européenne de 1995 introduit notamment la notion de « donnée à caractère personnel » en remplacement de la notion « d'informations nominatives » prévalant jusqu'alors en France. Cette nouvelle notion, encore utilisée aujourd'hui, a une portée plus large, qui vise à tenir compte du fait que la multiplication des fichiers et leurs croisements permettent d'identifier des individus par recoupements d'informations, y compris dans des bases anonymées. La directive repose plus largement sur trois principes :

- Proportionnalité : la collecte et le traitement ne doivent pas être excessifs et correspondre aux besoins effectifs pour lesquels ils ont été faits ;
- Transparence : la manière dont seront conservées et traitées les données fournies doivent être connues des personnes, qui doivent toujours pouvoir accéder aux informations les concernant ;
- Finalité légitime : typiquement, il est légitime de demander son adresse postale à une personne passant commande en ligne, mais pas forcément son lieu de naissance.

La directive abolit presque complètement les distinctions entre les collectes et traitements faits par des entités du secteur public ou du secteur privé présentes dans la loi de 1978. La possibilité pour les organismes privés de nommer un conseiller informatique et libertés (CIL) pour améliorer la relation avec les clients est aussi offerte contre des facilités de contact avec la CNIL, à l'image d'une pratique existant déjà en Allemagne, aux Pays-Bas et en Suède.

Une réglementation longtemps inefficace des services commerciaux en matière de vie privée

Pour autant, la portée de la loi informatique et libertés dans la protection de la vie privée des utilisateurs de services numériques en France est également grandement diminuée sur la période par divers biais. D'une part, une tendance forte à partir des années 1980 et surtout 1990

consiste pour les autorités nationales de divers pays à restreindre l'usage de procédés techniques de chiffrement permettant d'assurer techniquement la sécurité des communications en ligne pour les particuliers. Cette période est désignée sous le nom de *crypto wars*. Au cours des décennies 1980 et 1990, les États-Unis ont connu une vive polémique sur l'utilisation et l'exportation des solutions de chiffrement. Elle opposait les pouvoirs publics au secteur privé et à des associations de défense des libertés civiles. Le chiffrement a d'abord relevé de la catégorie juridique des armes et munitions soumises à autorisation pour l'utilisation et l'exportation, au nom de la lutte contre le crime et le terrorisme. Cette régulation s'est assouplie en deux temps. Le 15 novembre 1996, Bill Clinton limite par décret la rigueur du régime de déclaration aux pouvoirs publics pour l'utilisation et l'exportation des solutions de chiffrement[444], qui est ensuite pratiquement aboli le 10 janvier 2000[445] à l'initiative d'Al Gore[446], sauf à destination de certains États considérés comme soutenant le terrorisme, comme Cuba, l'Iran ou la Corée du Nord. La France connaît son propre pendant des « Crypto Wars » américaines durant les décennies 1980 et 1990, quoique sur un mode mineur[447]. Elle se dote dès 1986 d'une réglementation limitant de manière draconienne l'usage civil d'outils de chiffrement des échanges numériques avec le décret no 86-250 du 18 février 1986, portant modification du décret no 73364 du 12 mars 1973 fixant le régime des matériels de guerre, armes et munitions. Fondé sur un rapport de la DST et de la DGSE rédigé en 1985, le décret no 86-250 interdit l'exportation de logiciels de chiffrement, et oblige les sociétés agréées fournissant des services de chiffrement sur le territoire français à fournir au service central de la sécurité des systèmes d'information les clés de chiffrement employées. Le chiffrement de bout-en-bout, dans lequel seuls l'expéditeur et le destinataire d'un message disposent des clés de chiffrement et de déchiffrement, est donc interdit. Cette interdiction est reconduite dans l'article 28 de la loi no 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications. Ainsi, l'usage de Pretty Good Privacy (PGP), un des premiers logiciels de chiffrement disponibles sur l'Internet, était strictement interdit en France jusqu'en 1996, car il était considéré comme une arme de guerre de deuxième catégorie. Sous la pression de militants des libertés civiles et d'une partie des milieux commerciaux pressentant l'importance à venir du commerce en ligne, cette situation est modifiée par l'article 17 de la loi no 96-659 du 26 juillet 1996 de réglementation des télécommunications, qui dispose que « l'utilisation d'un moyen ou d'une prestation de cryptologie est libre », quoiqu'à certaines

[444] W. J. CLINTON, « Administration of Export Controls on Encryption Products », dans *Executive Order*, nº 13026, 1996
[445] R. R. MAJAK, « Revised U.S. Encryption Export Control Regulations », dans *RIN*, 2000
[446] F. TRÉGUER, *Pouvoir et résistance dans l'espace public*, *op. cit.*, p. 308
[447] *Ibid.*, p. 309

conditions notamment le recours à un tiers de confiance agréé par les pouvoirs publics. Cet assouplissement de la législation française a été confirmé à la publication des décrets d'application au cours des années suivantes. Le chiffrement sans déclaration aux pouvoirs publics avec des clés allant jusqu'à 128 bits pour usage privé est autorisé par le gouvernement Jospin en 1999 (décret n° 99-199 du 17 mars 1999)[448]. Mais ce n'est qu'avec la loi pour la confiance dans l'économie numérique du 21 juin 2004 que l'utilisation des moyens de cryptologie se démocratise. En revanche l'importation et l'exportation des moyens de cryptologie reste soumise à déclaration ou autorisation. Les moyens de cryptologie sont en effet toujours considérés comme des biens dits « à double usage » (civil et militaire), voire comme du matériel de guerre dans certains cas[449].

Si les services commerciaux en ligne ont été des acteurs majeurs des Crypto Wars jusqu'à faire accepter la libéralisation du chiffrement pour accompagner l'essor de l'économie numérique, ils ont aussi largement contribué dans les années 2000 et 2010 à enfoncer un coin dans la protection des données personnelles des internautes européens. En effet, la directive européenne 95/46/CE sur la protection des données personnelles d'octobre 1998 interdisait en principe le transfert de données personnelles de l'espace économique européen (EEE) vers des États leur appliquant un niveau de protection inférieur à celui en vigueur dans l'EEE. Ce niveau de protection étant particulièrement fort, les données personnelles des internautes de l'EEE ne pouvaient *de facto* être traitées presque que dans l'EEE. Du fait de l'importance considérable des services internétiques étatsuniens comme de la taille du marché européen, un cadre juridique bilatéral a rapidement été poussé par le département du Commerce étatsunien afin de garantir à environ 4 000 de ses entreprises la possibilité de traiter les données de leurs utilisateurs outre-Atlantique. Intitulé *Safe Harbor*, ce cadre assez peu contraignant mis en place entre 1998 et 2000 a donc assez largement limité la portée des mesures légales de protection de la vie privée en Europe. À la suite des révélations d'Edward Snowden en 2015 à propos de la surveillance de masse effectuée par les services de renseignement étatsunien sur les données des étrangers conservées sur leur sol à travers le programme Prism, « le très controversé Safe Harbor » a été annulé par la cour de justice de l'Union européenne (CJUE) le 6 octobre de la

[448] *Ibid.*, p. 313
[449] Pour l'information du lecteur : ce paragraphe est directement tiré d'un texte que j'ai rédigé et déjà mis en ligne sur Wikipédia.

même année[450]. Un nouvel accord est négocié en urgence par les États-Unis avec la Commission européenne entre 2015 et 2016, finalement accepté sous le nom de *Privacy Shield*. Légèrement plus protecteur, il prévoit notamment la nomination d'un médiateur entre les deux continents pour régler d'éventuels litiges. Contesté à son tour par des acteurs associatifs européens au nom de motifs similaires à ceux qui avaient conduit à la dénonciation de *Safe Harbor*, *Privacy Shield* sera lui aussi annulé par la décision C311-1812 du 16 juillet 2020 de la CJUE.

Ainsi, malgré l'importance historique de la loi informatique et libertés française de 1978, et l'engagement réglementaire des autorités et des CNIL européennes dans la protection des données personnelles en Europe, la Commission européenne a lancé dès janvier 2012 une réflexion sur la refonte des mesures de défense de la vie privée dans l'Union.

L'avènement du RGPD

Entre janvier 2012 et décembre 2015, un nouveau cadre légal pour la protection de la vie privée dans l'Union européenne a été élaboré sous le nom de règlement général sur la protection des données (RGPD). Il complète et remplace la directive 95/46/CE. Entré en vigueur le 24 mai 2016, il est définitivement applicable dans toute l'Union depuis le 25 mai 2018. Il a été transposé dans le droit français le 14 mai de cette année, soit assez tardivement. Un délai de deux ans était en effet laissé aux pays membres pour le transposer, afin de laisser du temps à leurs entreprises et institutions pour se mettre en conformité si nécessaire, ainsi que pour décider de certains paramètres à l'échelle nationale. L'âge minimal de consentement au recueil de ses données personnelles pouvait par exemple être fixé dans une fourchette comprise entre treize et seize ans – la France a retenu l'âge de quinze ans.

Ses principaux apports sont la transformation des conseillers informatique et libertés (CIL) en *data protection officers* (DPO) et le droit à la portabilité des données utilisateur. Ce dernier point est un développement du droit antérieur d'accès aux données personnelles, qui est désormais renforcé par le fait que ces données doivent pouvoir être transférées à un service équivalent dans un esprit de libre concurrence. Par exemple, il doit être possible de transférer ses messages d'une application à une autre. Si dans les faits ces transferts sont très hypothétiques (il n'est pas dit que mes interlocuteurs soient présents sur la nouvelle application où je voudrais transférer mes messages, ni d'ailleurs qu'ils soient identifiables de la première

[450] M. UNTERSINGER, « La justice européenne invalide le très controversé Safe Harbor, un accord sur les données personnelles », *Le Monde.fr*, 6 octobre 2015 (en ligne : https://www.lemonde.fr/pixels/article/2015/10/06/la-justice-europeenne-invalide-le-tres-controverse-accord-safe-harbor-sur-les-donnees-personnelles_4783262_4408996.html ; consulté le 12 juillet 2022)

application à la deuxième), ce principe a pour mérite de forcer les prestataires de services à fournir à leurs utilisateurs leurs données dans un format facilement lisible (mes messages seront ainsi téléchargeables dans un format textuel standard). Enfin, le RGPD assure une relative harmonisation entre pays européens quant à leurs lois Informatique et libertés, malgré le fait que certains paramètres puissent varier à l'échelle nationale, comme l'âge minimal requis pour le consentement au traitement des données personnelles.

*

Si la loi est le plus haut niveau des normes, et les usages courants leur forme la plus faible, il existe également des niveaux intermédiaires qui vont du standard ISO aux chartes en passant par les « bonnes pratiques » plus ou moins bien identifiées. Elles ont pour point commun de tirer leur principe d'une auto-régulation explicite, sans avoir le caractère contraignant du cadre légal. Dans le cadre d'Internet en particulier, des organisations d'auto-régulation très puissantes se sont très tôt mises en place pour assurer la gouvernance et le bon fonctionnement technique du réseau, en marge des gouvernements et des États. L'Internet Society fondée en 1992 est la première et la plus généraliste d'entre elles, mais d'autres organisations plus spécifiques ont également rapidement vu le jour ; par exemple, le World Wide Web Consortium (W3C), né en 1994, qui traite de la normalisation du Web, en élaborant notamment la documentation de l'*Hypertext Markup Langage* (HTML), le langage de balisage commun pour la création et la consultation de pages web. Existe-t-il une initiative comparable pour l'IoT ?

Internet Society

« L'internet Society (ISOC) est une organisation à but non lucratif créée en 1992 pour promouvoir et coordonner les développements des réseaux informatiques, en particulier les normes favorisant le fonctionnement de l'internet. Ces normes sont établies grâce aux travaux de l'IETF (Internet Engineering Task Force), qui regroupe des ingénieurs et des chercheurs du monde entier. (…) Avec des bureaux à Washington et Genève, l'ISOC est la plus importante autorité morale de l'internet. Elle comprend 28 000 membres répartis dans 80 sections (chapters) dans le monde entier et elle est dirigée par un bureau d'administrateurs élus par l'ensemble de ses membres. » (Niel & Roux, 2012)

II - L'ECHEC D'UNE LABELLISATION DES OBJETS CONNECTES SOUS L'EGIDE DE L'INTERNET SOCIETY

L'auto-régulation par des organisations professionnelles relativement indépendantes des pouvoirs politiques est fondamentale dans l'élaboration et la maintenance des technologies et protocoles numériques, et plus particulièrement en ce qui concerne les réseaux de communication impliquant une grande variété d'acteurs industriels. Cette auto-régulation a d'ailleurs bien souvent précédé les initiatives étatiques pour accompagner le développement des sociétés numériques. Pour autant, dans le domaine de l'IoT, il semblerait que cette dynamique horizontale, opérante pour Internet et pour le Web, ne le soit plus autant aujourd'hui pour la régulation du Web social et pour l'IoT. Nous allons le voir à travers l'exemple de l'échec d'une proposition de labellisation des objets connectés par l'Internet Society, pourtant « la plus importante autorité morale de l'internet »[451], proposition à laquelle j'ai participé dans une logique de recherche-action entre 2017 et 2019.

L'ambition maximale du groupe IoT était au départ de produire un label promouvant la sécurité et la vie privée des utilisateurs pour ce secteur d'activités. Cette ambition a été progressivement réduite à l'élaboration d'une charte, et a finalement abouti à la publication de « 22 recommandations » et d'un communiqué de presse. La sous-partie qui suit rend compte de cette évolution.

L'organisation parapublique de la régulation d'Internet

L'Internet Society est la plus ancienne et sans doute la plus puissante des autorités de régulation d'Internet. Fondée en 1992, l'historien Félix Tréguer souligne son importance en la présentant comme une « organisation co-fondée par Vint Cerf, Bob Kahn et d'autres « pères fondateurs » de l'Internet pour donner une assise juridique aux organismes de standardisation liés à Internet »[452]. Plus concrètement, l'ISOC encadre et finance les activités d'organisations-clés du développement d'Internet, dont les deux principales sont l'Internet Engineering Task Force (IETF) et l'Internet Research Task Force (IRTF). Elles comptent parmi les quelques *Standard Development Organizations* (SDO) qui établissent les standards et protocoles qui rendent possibles les échanges en ligne. La première traite du développement concret d'Internet à court et moyen terme, en élaborant des protocoles fondamentaux comme TCP/IP, ou des protocoles annexes comme TLS (qui permet le chiffrement des échanges sur Internet) ; la

[451] X. NIEL et D. ROUX, « Des évolutions permanentes », dans *Les 100 mots de l'Internet*, Paris (France), Presses Universitaires de France, 2012, vol. 3, § 15
[452] F. TREGUER, *Pouvoir et résistance dans l'espace public*, *op. cit.*, p. 326

deuxième a une fonction de plus long terme assimilable à de la recherche fondamentale – l'un de ses quatorze groupes de recherche actifs en 2022 traite par exemple des applications futures de l'informatique quantique à Internet. Au-delà de ces activités, l'ISOC est une forme de lobby et de *think-tank*, qui peut participer aux débats parlementaires comme produire des rapports ou organiser des évènements pour les acteurs du secteur. Il s'agit d'un organisme reconnu, au carrefour de multiples intérêts, tant institutionnels qu'économiques, dont la position est idéale pour impulser des initiatives d'auto-régulation du secteur.

Du reste, le quatrième des « *Global Internet Reports* » de l'Internet Society publié en 2017 pour les 25 ans de l'institution et intitulé *Paths to Our Digital Future* adoptait une approche résolument prospective dans laquelle la meilleure part était accordée à l'IoT et à la « convergence des mondes physique et internétique » parmi les six « moteurs de changement » (trad. pers.) identifiés pour les cinq années à venir, avant même la question de l'intelligence artificielle[453]. C'est donc sans surprise qu'une réflexion mondiale impliquant une grande partie des chapitres nationaux de l'ISOC a été initiée sur la question de la nécessaire régulation de l'IoT. En particulier pour le chapitre français de l'ISOC, cette réflexion était, de plus, encouragée aux articles 40 et 41 du RGPD qui suggèrent l'élaboration de « codes de conduite » précisant finement et par « secteur » d'activités comment appliquer au mieux le RGPD[454]. Ces deux articles mettent en œuvre un des principes de la préfiguration du RGPD selon laquelle il fallait prendre en compte le monde économique dans l'élaboration du droit sur les données personnelles et la vie privée. Quoiqu'il ait aussi pour but de mettre fin aux dérives longtemps observées dans les cadres législatifs précédents, notamment à travers des pénalités financières enfin dissuasives, le RGPD permet donc aussi de traiter les entreprises comme des partenaires possibles pour la puissance publique, plutôt que comme des antagonistes par défaut de l'intérêt général. Là encore, l'ISOC est idéalement placée en tant qu'association indépendante pour faire vivre cette ambition du RGPD, dans la mesure où ses intérêts ne sont directement ni ceux des régulateurs, ni ceux des entreprises, que ces acteurs soient ou non des partenaires techniques de l'ISOC à travers l'IETF ou l'IRTF.

C'est ainsi que l'ISOC a officiellement lancé en janvier 2019 un groupe de travail pour conduire une réflexion sur la régulation de l'IoT, le « groupe IoT », impliquant des acteurs très

[453] *Paths to Our Digital Future*, Internet Society, 2017, p. 8
[454] Le premier paragraphe de l'article 40 prévoit notamment que « Les États membres, les autorités de contrôle, le comité et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer à la bonne application du présent règlement, compte tenu de la spécificité des différents secteurs de traitement et des besoins spécifiques des micro, petites et moyennes entreprises. »

variés[455]. Selon les pratiques en vigueur dans les SDO associés à l'ISOC, la logique de travail mise en place était résolument collaborative et plutôt ouverte, sans aller jusqu'au principe de publicité des débats mise en œuvre dans les groupes de travail de l'IETF. Il était ainsi possible de proposer à participer au travail de réflexion directement depuis les pages du site de l'ISOC consacrées au groupe. En ce qui me concerne, c'est à travers les réunions publiques organisées mensuellement par la Quadrature du Net, les quadrapéros, que j'ai été informé de la création du groupe. Le 7 décembre 2018, un membre de la Quadrature au fait du sujet de la présente thèse m'y a convié, ainsi qu'un autre participant habituel des quadrapéros n'appartenant pas non plus formellement à la Quadrature, mais à l'association Franciliens.net.

Le projet m'a été présenté comme prometteur, mais encore relativement flou. Il s'agissait de prendre part à la réflexion collective dans deux directions :

- La production d'un texte, rapport ou charte, amené à synthétiser le travail conduit par le groupe ;
- Et, surtout, la préfiguration d'un éventuel outil d'information au public sous la forme d'un label comparable au Nutri-score dans le secteur alimentaire, qui aurait permis aux consommateurs de choisir en connaissance de cause à quels services souscrire et quels produits acheter selon des critères relatifs à leur vie privée et à la circulation de leurs données personnelles, critère qu'il nous revenait de définir.

L'intérêt du groupe était, en outre, de rassembler des acteurs de tous types, tant des institutions publiques (ARCEP, Agence du Numérique, ANSSI, CNNum) que des associations (gestionnaire de noms de domaine Afnic), des syndicats professionnels (MEDEF, UNAF), des entreprises (Nokia, pôle de compétitivité Systematic Paris-Region), et quelques autres chercheurs universitaires ou privés. La Quadrature du Net avait également accepté le principe de sa participation initialement, mais sans garantir de pouvoir y consacrer de moyens. Ma propre entrée dans le groupe en tant que chercheur a été confirmée par Lucien Castex, l'un des deux présidents du groupe, autrement dit des coordinateurs appartenant au chapitre français de l'ISOC, le 15 février 2019. Il est à préciser que la participation à ce groupe n'était pas rémunérée par l'ISOC, et relevait du *pro bono* pour les autres institutions participantes. La logique de ma participation relevait d'une logique de recherche-action, voire de recherche appliquée, dans la

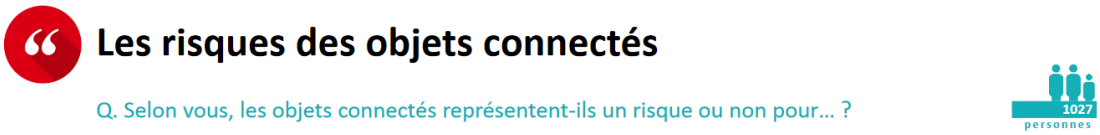
[455] « L'Internet Society fait progresser la sécurité des objets connectés », sur *Internet Society France*, 8 janvier 2019 (en ligne : https://www.isoc.fr/lancement-groupe-iot/ ; consulté le 13 juillet 2022)

mesure où les résultats de ce travail étaient amenés à être publics, et permettaient de mettre en application mes propres résultats préliminaires tout en m'ouvrant un nouvel axe de recherche plus fondamental. Par ailleurs, l'ISOC finançait le pilotage du groupe par un consultant extérieur et fournissait les moyens techniques pour les réunions et le travail collaboratif, à savoir une instance de visioconférence Zoom et un dépôt en ligne pour les documents de travail. Quelques réunions préliminaires ont eu lieu physiquement avant mon arrivée, puis le travail a été essentiellement effectué en ligne par la suite, au moins à ma connaissance.

Labellisation et *privacy by design*

Le principe de la création d'un label par l'ISOC avait été testé en amont de la création du groupe de travail à travers un sondage fait par l'institut OpinionWay[456]. Les intitulés choisis dans le sondage permettent d'abord de spécifier ce que l'ISOC entend par « objet connecté », à savoir ni un « smartphone », ni un « ordinateur », mais un objet du type « montre connectée/fitness, voiture connectée, caméra connectée pour bébés, enceinte connectée, etc. » La définition ne se réduit donc pas à la domotique quoiqu'elle soit associée à deux des quatre exemples. Les *wearables* et la voiture connectée sont également mis en avant. La première question thématique du sondage concerne la possession ou non d'objets connectés : seules 22 % des personnes du panel en possèdent, avec à chaque fois une légère surreprésentation linéaire selon l'âge (les jeunes sont plus équipés) et la CSP (les CSP+ sont plus équipées), avec des extrêmes d'équipement minimaux et maximaux de 15 % (pour les inactifs quel que soit leur âge) et 30 % (pour les jeunes entre 18-24 ans et 25-34 ans quelle que soit leur CSP). En l'absence de fichier détaillé, on peut donc supposer que les retraités pauvres sont les moins équipés, et les jeunes actifs riches les plus équipés. Aucune information n'est donnée sur les espaces de résidence des personnes.

[456] « Echantillon de 1027 personnes représentatif de la population française âgée de 18 ans et plus. L'échantillon a été constitué selon la méthode des quotas, au regard des critères de sexe, d'âge, de catégorie socioprofessionnelle, de catégorie d'agglomération et de région de résidence. L'échantillon a été interrogé par questionnaire auto-administré en ligne sur système CAWI (Computer Assisted Web Interview). Les interviews ont été réalisées du 27 au 28 juin 2018. Pour les remercier de leur participation, les panélistes ont touché des incentives ou ont fait un don à l'association proposée de leur choix. OpinionWay a réalisé cette enquête en appliquant les procédures et règles de la norme ISO 20252. Les résultats de ce sondage doivent être lus en tenant compte des marges d'incertitude : 1,5 à 3 points au plus pour un échantillon de 1000 répondants. » *in* F. MICHEAU, *Les Français et les objets connectés - Sondage OpinionWay pour ISOC France*, Paris (France), Internet Society France / OpnionWay, 2018, p. 3



		Sexe		Age					Statut			Possède un objet connecté	
	% OUI	Homme	Femme	18-24 ans	25-34 ans	35-49 ans	50- 64 ans	65 ans et +	CSP+	CSP -	Inactif	Oui	Non
Le respect de votre vie privée (protection des données personnelles)	**76%**	76%	77%	77%	76%	73%	77%	80%	74%	78%	79%	72%	79%
Votre sécurité physique	**44%**	39%	47%	41%	48%	47%	42%	39%	41%	51%	40%	40%	45%

Figure 22 - Les risques perçus concernant les objets connectés mesurés par OpinionWay pour l'ISOC (Micheau, 2018, p. 9)

La question des « risques » autour des objets connectés (voir Figure 22) est subdivisée en deux thématiques seulement : le « respect de [la] vie privée, et, plus étonnant, la « sécurité physique » des utilisateurs. À la première question, qui est évidemment la plus déterminante dans le cadre de la présente thèse, 76 % des sondés répondent que les objets connectés représentent un risque pour la vie privée. Sans que la question soit très spécifique, elle n'en confirme pas moins, d'une part, l'intérêt de ma thématique de recherche, autant que celui d'approfondir la question par des entretiens. D'autre part, elle confirme pour l'ISOC la pertinence de sa propre démarche de réflexion autour de la confiance envers les objets connectés. En ce qui concerne la question du risque physique, nous ne nous y attarderons pas : elle préoccupe visiblement moins les sondés (44 % de réponses positives), et concerne sans doute avant tout les voitures connectées ou autonomes : on peine à voir quel risque physique il y aurait à utiliser une enceinte connectée ou de la domotique, hors de cas très particuliers qui n'ont de toute façon guère été évoqués par mes propres enquêtés, y compris en ce qui concerne le compteur Linky, seul objet connecté domestique qui pourrait poser un problème de santé publique à travers l'émission d'ondes – inquiétude attestée médiatiquement, mais qui n'est significative chez aucun de mes enquêtés.

L'hypothèse d'une inquiétude envers les objets connectés quant à la vie privée des utilisateurs étant confirmée par cette première question, l'enquête pour l'ISOC s'attache ensuite à savoir si un « label » pourrait faire gagner les utilisateurs en confiance (voir Figure 23). La réponse est ici très partagée, et la distribution des réponses est presque symétrique, avec toutefois légèrement plus de personnes potentiellement plutôt plus confiantes que plutôt pas confiantes, et, réciproquement, légèrement plus de personnes pas du tout confiantes que tout à fait confiantes.

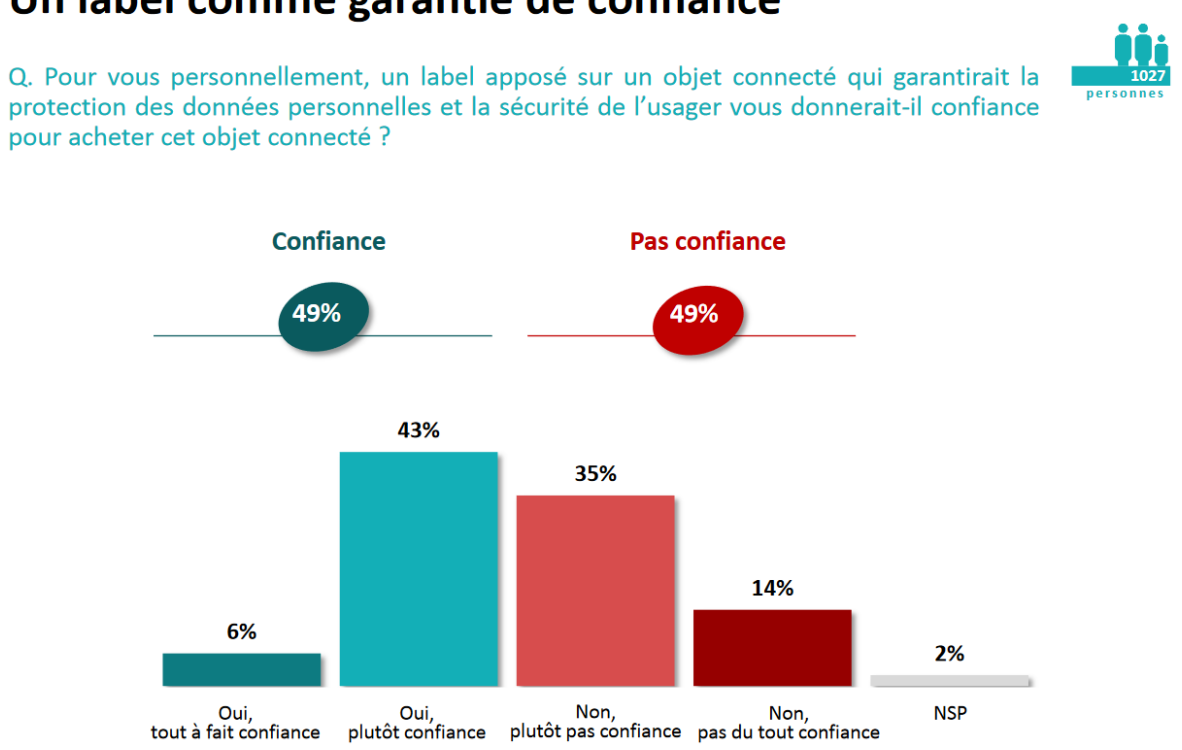


Figure 23 - La demande pour un label concernant les objets connectés mesurée par OpinionWay pour l'ISOC (Micheau, 2018, p. 10)

Si le principe d'une labellisation pour accompagner les utilisateurs n'est donc pas entièrement invalidé par le sondage, on peut tout de même constater qu'il ne répondrait pas à une attente extrêmement forte ou, si l'on s'en tient davantage à la formulation de la question, qu'une telle labellisation ne se verrait pas créditer d'un haut degré de confiance par défaut.

Du reste, si le principe fondant l'existence du groupe IoT était d'améliorer l'information aux utilisateurs potentiels de services et d'objets connectés, je fais l'hypothèse qu'il s'adressait avant tout aux producteurs d'objets et de services, qu'ils participent directement à l'atelier, ou qu'ils soient touchés ensuite par la communication externe de l'ISOC les invitant à s'emparer des outils créés par le groupe. C'est du reste une partie non-négligeable de la stratégie mise en œuvre par les promoteurs de l'indice Nutri-score dans l'alimentation, qui m'a été présenté comme une source d'inspiration pour le groupe de travail. Il est en effet assez bien établi que le Nutri-score n'a qu'une efficacité marginale sur les comportements d'achat en conditions

réelles[457], mais le label a également pour but affiché d'inciter les industriels à améliorer la qualité nutritionnelle de leurs produits ne serait-ce que par souci d'affichage, selon le rapport remis sur le sujet à la ministre de la Santé[458], et appuyé par la littérature scientifique[459,460]. Dans le cas d'un label sur des services numériques utilisant des données personnelles ou identifiantes, la logique aurait été de proposer une labellisation qui aurait permis aux utilisateurs potentiels de savoir comment leurs données seraient produites, collectées et traitées, mais aussi d'inciter les constructeurs à minimiser cette collecte de sorte à ne pas avoir à afficher un éventuel mauvais score, ou de trop nombreux pictogrammes indiquant quels types de données étaient collectés, par exemple. Il est difficile de dire si cette orientation qu'il m'a semblé identifier est le résultat de l'interprétation du sondage susdit, mais elle pourrait au moins expliquer pourquoi l'idée d'une labellisation a continué d'être à l'ordre du jour du groupe IoT sans demande sociale forte.

En cela, le groupe me semblait donc s'inscrire fortement dans une logique de *privacy by design*. Un paragraphe entier y était consacré dans la première page de la dernière version du projet de charte, ce qui pourrait indiquer que les initiateurs du groupe à l'ISOC avaient identifié cet axe comme majeur. Le *privacy by design* est un principe d'élaboration des matériels et logiciels autour de l'idée que la protection de la vie privée des utilisateurs doit être intégrée dès la conception, et pas uniquement après coup par des garanties sur l'utilisation qui sera faite des données récoltées. Selon Peter Hustinx, contrôleur européen de la protection des données[461] de 2004 à 2014, le *privacy by design* est un concept très proche des *privacy-enhancing technologies* (PET) et aurait d'ailleurs été présenté pour la première fois dans un rapport intitulé

[457] P. DUBOIS *et al.*, « Effects of front-of-pack labels on the nutritional quality of supermarket food purchases: evidence from a large-scale randomized controlled trial », *Journal of the Academy of Marketing Science*, vol. 49, nº 1, 1er janvier 2021, p. 119-138 (en ligne : https://doi.org/10.1007/s11747-020-00723-5 ; consulté le 17 juillet 2022)

[458] « Par ailleurs, les divers outils réglementaires proposés peuvent être utilisés pour inciter les firmes à reformuler leur offre alimentaire et innover dans ce domaine : en aidant la dimension « santé » des choix alimentaires à devenir un axe de différenciation essentiel des produits, on augmente les incitations à l'amélioration de leur qualité nutritionnelle. La réglementation ne doit pas être perçue uniquement comme une contrainte, mais peut jouer un rôle d'incitation à être plus compétitif sur le plan de la qualité et du prix, à développer l'innovation et à renforcer une image positive au niveau national et international. » *in* S. HERCBERG, *Propositions pour un nouvel élan de la politique nutritionnelle française de santé publique dans le cadre de la Stratégie Nationale de Santé - 1ère partie : Mesures concernant la Préventions nutritionnelle*, Paris (France), Ministère des Affaires Sociales et de la Santé, 2013, p. 28

[459] E. L. VYTH *et al.*, « Front-of-pack nutrition label stimulates healthier product development: a quantitative analysis », *International Journal of Behavioral Nutrition and Physical Activity*, vol. 7, nº 1, 8 septembre 2010, p. 65 (en ligne : https://doi.org/10.1186/1479-5868-7-65 ; consulté le 17 juillet 2022)

[460] R. DOBBS *et al.*, *Overcoming obesity : An initial economic analysis*, McKinsey Global Institute, 2014

[461] À savoir l'autorité indépendante chargée de la protection des données dans toute l'Union européenne.

Privacy-enhancing technologies: the path to anonymity en 1995[462]. Toujours selon Hustinx, deux personnes ont particulièrement inspiré ce projet de rapport bilatéral entre les autorités hollandaises et canadiennes, John Borking côté hollandais, et Ann Cavoukian côté canadien[463] - nous avons déjà évoqué cette dernière dans le récit de l'échec d'Alphabet à Toronto dans le projet d'aménagement du quartier Quayside (voir p. 29). L'expression n'apparaît pas telle quelle dans la révision du rapport en 2000, mais la question du design en lien avec la protection de la vie privée y reste fondamentale[464].

Si cette proposition a fait date, le *privacy by-design* est un principe assez général, dans l'application concrète duquel aucune solution technique précise ne permet de couvrir tous les cas de figure[465]. Typiquement, une des solutions récentes les plus remarquées a été mise en application, d'abord par Apple au niveau industriel, avec la généralisation du chiffrement différentiel pour obtenir des statistiques d'utilisation de son parc d'appareils et de logiciels sans avoir à connaître finement le profil de chaque utilisateur. Le chiffrement différentiel est une technique de cryptologie en développement depuis 2006, qui a parfois été présentée comme le « navire-amiral de la vie privée appliquée aux données »[466]. Le principe en est que, au moment de faire remonter la donnée de monitoring à Apple, comme de savoir si telle fonctionnalité d'un iPhone a été utilisée au cours du dernier mois, l'appareil introduit une certaine proportion d'informations fausses : au niveau de chaque téléphone particulier, 15 % par exemple des réponses envoyées seront un « non », quand bien même le service aurait bien été utilisé le mois précédent. Apple connaissant la proportion de réponses menteuses données par ses appareils, il lui suffit de redresser l'information en corrigeant ce biais statistique volontairement introduit. Le résultat est qu'Apple continue d'avoir des données assez fines à propos de l'agrégat constitué par l'ensemble de son parc, mais ne peut plus connaître le profil de chaque utilisateur,

[462] P. HUSTINX, « Privacy by design: delivering the promises », *Identity in the Information Society*, vol. 3, nº 2, 1er août 2010, p. 253-255 (en ligne : https://doi.org/10.1007/s12394-010-0061-z ; consulté le 18 juillet 2022)
[463] « *Two deputy commissioners—Ann Cavoukian at the Canadian side and John Borking at the Dutch side—played a key role in this project*. » *in Id.*
[464] R. HES et J. BORKING, *Privacy-Enhancing Technologies: The Path to Anonymity*, La Haye (Pays-Bas), Registratiekamer, 2000
[465] « *Different parties have proposed privacy-by-design methodologies that promise to be a holy grail for organizations collecting and processing personal data. These efforts aim at addressing the engineering aspects of privacy by design by pointing to design strategies, but fall short of relating how these strategies can be applied when building privacy preserving information systems*. » *in* S. GÜRSES, C. TRONCOSO et C. DIAZ, « Engineering Privacy by Design Reloaded », Amsterdam (Pays-Bas), 2015, p. 1 (en ligne : http://witdom.eu/content/engineering-privacy-design-reloaded ; consulté le 1er février 2018)
[466] « *Shortly after it was first introduced in 2006, differential privacy became the flagship data privacy definition*. », trad. pers. *in* D. DESFONTAINES et B. PEJÓ, « SoK: Differential Privacies », dans *Proceedings on Privacy Enhancing Technologies*, s. l., 2020, vol. 2, p. 288-313 (en ligne : http://arxiv.org/abs/1906.01337 ; consulté le 26 juillet 2022)

complètement faussé à l'échelle individuelle. Cependant, même cette solution très élégante et très commentée n'en nécessite pas moins de faire confiance à Apple dans l'implémentation du chiffrement différentiel, et elle ne peut être employée que sur des groupes d'utilisateurs suffisamment nombreux pour que la loi statistique des grandes nombres limite suffisamment la marge d'erreur dans l'interprétation des informations remontées. En termes de connaissance de la technique dans l'échantillon, seuls deux enquêtés parmi les plus technophiles y font explicitement référence [467]. D'autres pistes sont creusées aujourd'hui pour maximiser la confidentialité des informations personnelles dans l'utilisation de l'IoT, comme le recours à la technologie des chaînes de bloc[468], mais le chiffrement différentiel est aujourd'hui la plus perfectionnée à être déployée industriellement.

Quoique le *privacy by design* ne soit pas une martingale de la protection de la vie privée, il a permis l'émergence d'un principe à l'applicabilité directe plus forte, à savoir la minimisation de la collecte de donnée. Prenant en compte l'importance cruciale du design plutôt que de la seule protection *ex post* de données déjà collectées, il affirme qu'un service n'est jamais plus protecteur de la vie privée de ses utilisateurs que lorsqu'il fonctionne en collectant le moins possible de données au préalable, ce qui doit être logiquement pensé dès la conception du produit. Ce principe de minimisation a été très rapidement identifié comme majeur par les régulateurs [469] et précisé par des chercheurs, comme Gürses *et al.* qui affirment que la minimisation doit être comprise avant tout comme la limitation de la circulation des données vers des serveurs centralisés, sans par exemple exclure que des données soient produites et

[467] « JF: Et pour le coup, vous la considération, puisque certains me le disent, que... c'est sans doute pas faux, Apple protège mieux les données personnelles etc., ce qui expliquerait qu'il soit moins bon, justement parce qu'il te connaît moins.
E15: (acquiesce)
(…) E14: Avant de l'acheter, oui, j'ai regardé ce truc-là. Sur le fait qu'il envoyait pas tout non plus, et que... que normalement il s'arrête juste aux deux mots pour le déclencher et...
E15: (interrompant) Ca j'ai pas très bien compris leur truc. Apparemment ils injectent des... des faux... des fausses données dans ce qui récoltent pour du coup... ne pas forcément...
JF: (acquiesce)
E15: Pour ne pas pouvoir identifier absolument, heu... Pouvoir catégoriser absolument très bien la personne. Bon, après...
JF: Et ça...
E15: Je sais pas, enfin je sais pas, je suis pas assez connaisseur pour savoir si c'est juste du... si c'est juste de la poudre aux yeux ou... (petit rire)
JF: Alors pour le coup, c'est le chiffrement différentiel ? J'imagine ?
E15: Oui ! Il me semble que c'était ça.» (entretien 9, 20 min 40 s)

[468] N. DENIS, S. CHABRIDON et M. LAURENT, « Bringing Privacy, Security and Performance to the Internet of Things Through Usage Control and Blockchains », dans M. Friedewald *et al.* (éd.), *Privacy and Identity Management. Between Data Protection and Security*, [événement en ligne], Springer International Publishing, 2022, vol. 644, p. 57-72

[469] P. HUSTINX, « Privacy by design », *op. cit.*

stockées sur le terminal de l'utilisateur final[470]. Quoiqu'il ait surtout fait l'objet de discussions à partir du début des années 2010, le principe de minimisation a donc été implémenté jusque dans le texte du RGPD voté en 2016 : « Les données à caractère personnel doivent être : (…) c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) » dans l'article 5, « Principes relatifs au traitement des données à caractère personnel ». Cette prise en compte rapide et au plus haut niveau de norme souligne l'intérêt porté à ce principe.

L'option de la minimisation a de fait été évoquée dans les discussions du groupe IoT, ainsi que dans le projet de charte au volet de la vie privée, dans une formulation qui évoque quelque peu celle du RGPD en la précisant par l'évocation des serveurs distants (« cloud ») : « Les données collectées doivent être minimisées avant leur transmission au serveur cloud, conformes à celles prévues dans le contrat pour assurer le service (…) ». Cette recommandation vient en complément d'une pratique recommandée au volet sur la sécurité en amont dans le texte, qui invitait à ce que « Les données à destination et en provenance d'objets connectés doivent être chiffrées pour les rendre illisibles aux personnes non autorisées. Les entreprises doivent adapter leur sécurité pour minimiser, les risques de perte de données sensibles, leur exposition à la fraude et les interruptions de service. » Ce deuxième point est évidemment d'importance, et s'inscrivait dans un rappel sur l'importance du chiffrement des transmissions depuis les objets connectés, même s'il doit idéalement venir en aval de la minimisation de la collecte : il n'est pas nécessaire de protéger sur un serveur une donnée qui n'y a pas été transférée depuis un terminal. Au bout du compte, on ne peut que déplorer que le principe de minimisation n'apparaisse finalement pas dans les 22 recommandations publiées, qui s'en tiennent au rappel sur l'importance du chiffrement : « GARANTIR LA SÉCURITÉ DES COMMUNICATIONS par le renforcement du chiffrement ».

Ces choix entérinent malheureusement une option conceptuellement faible du point de vue de la défense et de la compréhension même de la vie privée, reléguée concrètement à un enjeu de sécurité informatique, au lieu de l'inscrire dans la logique immunitaire que je décris dans cette thèse. *In fine*, il ne s'agit pas de défendre la maîtrise sur ses données et ce qu'elles révèlent de lui pour l'utilisateur, mais simplement de s'assurer que ces données qui seront de

[470] « *In a system with a privacy-preserving design, the flow of sensitive data to a centralized entity (the service provider) is indeed "minimal", yet all the privacy-sensitive user data is captured and still stored on devices within the boundaries of the system. The difference to a "straightforward" implementation of a privacy preserving system is that the sensitive data only resides in components of the system under the control of the user.* » *in* S. GÜRSES, C. TRONCOSO et C. DIAZ, « Engineering Privacy by Design Reloaded », *op. cit.*, p. 1-2

toute façon collectées restent entre de bonnes mains. Nous verrons que ces choix reflètent plutôt des préoccupations évoquées par les représentants de l'industrie au cours des discussions (voir « Le risque du *privacy washing* », p. 240).

Labellisation et *privacy paradox*

En complément (et parfois à l'encontre) de cette logique axée sur le *privacy by design*, ma position générale dans les discussions a plutôt été de mettre en avant la lutte contre les effets du *privacy paradox*, c'est-à-dire de chercher à ce que le projet de charte et l'éventuelle labellisation qui aurait suivi cherche à gagner la confiance des consommateurs plutôt que de servir avant tout d'incitation pour les industriels. Il s'agissait de mettre mon principal résultat empirique du moment au service de la réflexion collective, quoique ma pensée sur le *privacy paradox* ait alors été plus simple et moins critique qu'aujourd'hui – il s'agissait alors d'entendre le malaise des utilisateurs prêts à céder des informations personnelles par fatalisme plutôt que par adhésion au design ou par reconnaissance de son adéquation à la fois à leurs besoins et à leurs valeurs et attentes[471]. Ainsi, j'insistais sur la nécessité de mettre en avant une information complète et loyale en plus de minimiser la collecte de données, dans le but de permettre aux utilisateurs de se sentir pleinement en maîtrise de leurs données et de leurs vies numériques, et de lutter contre le sentiment diffus mais récurrent dans les entretiens qu'on ne pouvait jamais vraiment savoir ce qui était fait de ses données, de ce qui était collecté, ou de la manière dont ces données étaient utilisées.

Auprès des industriels, cet argument n'était pas foncièrement différent de celui consistant à les inciter à améliorer leurs produits de sorte à gagner la confiance de clients potentiels. La manière de présenter l'approche diffère néanmoins subtilement : la lutte contre cette forme de *privacy paradox* avait pour moi l'intérêt de prendre en compte plus clairement les intérêts propres de l'utilisateur et de l'intérêt de la vie privée pour elle-même plutôt que de se focaliser sur le déclenchement de l'acte d'achat en magasin à travers le *packaging*. Autrement dit, il s'agissait également de jouer sur la manière dont l'utilisateur potentiel est perçu en partant du ressenti des utilisateurs, qui ressentent très nettement l'asymétrie d'information en leur défaveur quand ils utilisent des objets et des services qui sont pour eux comme des boîtes noires. Acquisti *et al.* identifient cette approche comme relevant d'un « *soft paternalism* »[472], à travers

[471] Pour rappel, je défends aujourd'hui l'idée que le *privacy paradox* dès sa première formulation a finalement été plutôt utilisé pour entériner une gestion inconséquente des données personnelles au nom de cette dissonance apparente entre les discours et les actes. Voir « Le chantage du privacy paradox », p. 184.

[472] A. ACQUISTI *et al.*, « Nudges for Privacy and Security: Understanding and Assisting Users », *ACM Computing Surveys*, vol. 50, nº 3, 8 août 2017, p. 3 (en ligne : https://doi.org/10.1145/3054926 ; consulté le 7 juin 2022)

lequel il est possible d'agir sur différents leviers pour amener les utilisateurs aux choix les plus pertinents pour eux en matière de consommation et de vie privée. Si un certain nombre de ces leviers portent sur des biais cognitifs inconscients (aversion à la perte, biais d'optimisme, préférence pour le *statu quo*…), l'« éducation » des utilisateurs fait aussi partie des actions prépondérantes identifiées par les auteurs, qui l'associent d'ailleurs eux aussi explicitement aux équivalents du Nutri-score outre-Atlantique[473]. Sans remettre en cause l'effectivité et la légitimité des autres « *nudges* » possibles dont Acquisti *et al.* font la synthèse, l'éducation me semble présenter l'intérêt d'être le moins paternaliste ou le moins descendant de cette compilation : l'utilisateur reste dans une posture d'information asymétrique, mais cette asymétrie est réduite. De fait, une telle asymétrie est de toute façon inévitable en cela qu'il serait illusoire de croire que tout utilisateur pourrait tout connaître de chaque système complexe qu'il utilise, qu'il soit numérique ou non. Enfin, axer la question autour de l'utilisateur et de son éducation auprès des industriels me semblait aller dans le sens d'une appréhension du consommateur potentiel plutôt comme un partenaire que comme une simple part de marché à conquérir.

Au bout du compte, si certaines inflexions ont pu être apportées en ce sens au texte du projet de charte, elles n'apparaissent pas dans les derniers textes effectivement livrés à l'été 2019, à savoir le communiqué de presse et les 22 recommandations.

Le risque du *privacy washing*

La diminution progressive des ambitions du groupe IoT, malgré la qualité des discussions auxquelles j'ai participé, révèle autant qu'elle résulte des difficultés à porter la question de la défense de la vie privée.

En ce qui concerne l'ambition initiale de porter une labellisation, elle me semblait déjà sérieusement battue en brèche dès les premiers temps de mon implication personnelle dans le groupe début 2019. Si la question était alors encore évoquée, elle n'orientait pas les discussions sur un mode prioritaire, alors même qu'un tel projet ne pouvait être mené à bien que sur la base d'une implication forte des participants. J'ai proposé en février 2019 une synthèse des labels ou propositions de labels existantes les plus convaincants à date pour nourrir cet axe de travail (voir en annexe, « Fiche synthétique sur les labels existants dans le cadre du travail pour le groupe ISOC/IOT », p. 431), sans qu'elle n'enclenche de discussion de travail plus concrète. Par ailleurs, la réflexion sur la labellisation graphique pour le paramétrage des services dans

[473] *Ibid.*, p. 13

l'IoT et pour l'information de leurs utilisateurs a continué à haut niveau dans d'autres contextes nationaux sur la période, ce qui accrédite la pertinence du sujet[474].

S'il semblait déjà assez peu probable que l'idée d'un label aboutisse début 2019, les efforts de la direction du groupe ont semblé plutôt tournés vers une présentation et une publication plus légère sous forme d'une charte le 4 juillet 2019 au Forum sur la gouvernance d'Internet porté par l'ISOC. Le projet de charte a davantage occupé le groupe, et fait l'objet principal de réunions en ligne et de demandes de retours sur le document partagée par les membres du groupe. Le consultant recruté par l'ISOC y a également concentré ses efforts de synthèse et de rédaction : il s'agissait du document pour lequel nous avions des points d'étape concrets, sous la forme de versions successivement arrêtées du document collaboratif en ligne. Ce projet de charte était l'objet principal des réunions qui ont eu lieu jusqu'en juin 2019. Il permettait des échanges d'assez bon niveau en cela que le texte, quoique synthétique, permettait des développements suffisants pour préciser les modalités d'application des principes défendus. La dernière version de la charte en juin 2019 comprenait ainsi neuf pages, soit un volume convenable pour préciser ce que pouvait signifier un mot de passe fort, quelles étaient les bonnes pratiques à retenir dans le cas de la divulgation de failles de sécurité, ou pour promouvoir le principe de minimisation évoqué plus haut.

Quoiqu'il n'ait alors pas été officiellement entériné à ma connaissance, l'abandon d'un projet de labellisation au profit d'un simple projet de charte a été le moment du retrait de la Quadrature du Net du groupe de travail. D'après les retours collectifs et discussions avec les membres de l'association impliqués, deux éléments ont entraîné ce retrait. D'une part, le principe d'une charte semblait, légitimement, beaucoup moins ambitieux, car il n'aurait relevé que de l'auto-régulation. Dans la culture juridique aujourd'hui très forte de LQDN, un tel niveau d'engagement, ni légal, ni même simplement contractuel, ne justifiait pas de consacrer plus d'effort militant à ce dossier. D'autre part, les membres de LQDN ayant eu accès aux documents de travail du groupe sur la charte ont réagi au mieux de façon neutre, et au pire avec d'importantes réserves sur de nombreux points, où certains ont considéré que le texte de la charte ne faisait souvent que reprendre des obligations par ailleurs légales, et disait parfois même moins que la loi existante, le RGPD notamment. Or, l'auto-régulation n'a de sens que si

[474] Une équipe de l'université Carnegie Mellon aux Etats-Unis a par exemple élaboré à la même époque une application pour smartphone, *IoT Assistant*, afin de faciliter les prises de décisions au niveau individuel dans l'usage de l'IoT. Voir Y. FENG, Y. YAO et N. SADEH, « A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things », dans *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, New York (ÉUA), Association for Computing Machinery, 2021, p. 1-16 (en ligne : https://doi.org/10.1145/3411764.3445148 ; consulté le 27 juillet 2022)

elle propose un mieux-disant par rapport à la loi, qui est de toute façon le minimum applicable. S'il n'était pas exclu que ces points puissent encore être améliorés au moment du retrait de LQDN, là encore le temps militant à consacrer à repartir de si loin n'aurait pas été bien alloué face à d'autres dossiers plus avancés ou susceptibles d'avancer. En octobre, au moment de la mise en ligne des documents synthétisant les propos tenus lors de l'événement de l'ISOC durant l'été sous la forme des « 22 recommandations », le consensus est même rapidement devenu qu'il fallait demander à l'ISOC que la participation initiale de LQDN au groupe ne soit plus mentionnée dans les documents publics – mention qui n'était toujours pas retirée début janvier 2023.

Pour autant, les discussions autour du projet de charte ont aussi permis d'identifier clairement des limites attendues de l'exercice. Ainsi, il y avait chez les représentants de l'industrie une certaine réticence vis-à-vis même de deux principes élémentaires de sécurité informatique ayant fait l'objet de débats, à savoir les mises à jour de sécurité, et le chiffrement des communications depuis les objets connectés. Ces questions ont par exemple cristallisé autour du petit scandale médiatique alors créé autour des robots de cuisine Monsieur Cuisine de la marque Silver Crest écoulés au cours de ventes éphémères par la marque de grande distribution Lidl. En juin 2019, deux particuliers relayés par le journal en ligne Numerama ont découvert que ces robots de cuisine étaient équipés de microphones invisibles, et non mentionnés dans la documentation associée[475]. Il faut signaler que tous les tenants et aboutissants de l'affaire n'étaient pas nécessairement connus à l'époque. Le consensus était néanmoins que le micro était présent par défaut dans la tablette sous Android servant d'interface au robot de cuisine, sans présager d'une intention malveillante. La question qui se posait était de savoir quel aurait été l'effet d'une forme ou d'une autre de label dans une telle situation. La position de l'un des acteurs industriels de la réunion allait malgré tout plus loin : il aurait été irréaliste car trop coûteux de faire retirer le microphone, qui pourrait peut-être servir après une éventuelle mise à jour permettant de l'exploiter dans l'interface, tout en ayant bien conscience que les mises à jour étaient peu probables pour un tel objet, vendu au cours d'une vente éphémère par un acteur généraliste qui n'en assurerait probablement pas le suivi. Sans en faire mystère, il s'agissait pour cet acteur de signaler ou de rappeler que la raison économique la plus triviale prévalait, que ce soit pour justifier de recourir à du matériel standard (ici, avec le micro non exploité et pas retiré), ou au contraire pour se laisser la possibilité d'un gain ultérieur en

[475] M. TURCAN, « Monsieur Cuisine Connect : micro caché, Android non sécurisé... les dessous du robot cuiseur de Lidl », *Numerama*, 13 juin 2019 (en ligne : https://www.numerama.com/tech/525214-monsieur-cuisine-connect-micro-cache-android-non-securise-les-dessous-du-robot-cuisine-de-lidl.html ; consulté le 23 juillet 2022)

valeur perçue (en activant peut-être une fonctionnalité de commande à la voix sans intervention sur le matériel, le micro étant déjà présent). Plus largement, il semblait aller de soi que des attentes fortes vis-à-vis des produits numériques n'étaient pas sérieusement envisageables sur des produits aux prix très faibles comme celui-ci, avec des marges bénéficiaires telles que la profitabilité ne pouvait être trouvée que dans la vente « flash », à savoir la vente rapide d'un stock important, pas forcément amené à être suivi dans le temps ou renouvelé. Pour le chiffrement, la logique était plus ou moins la même : l'achat de matériels en marque blanche (comme la tablette intégrée dans le Monsieur Cuisine), simplement assemblés pour créer un objet composite avec un effort ingénieurial d'intégration minimal, était présenté comme rendant irréaliste la prise en compte d'efforts de *privacy by design* supplémentaires et sans valeur ajoutée immédiatement monnayable, comme l'adjonction d'une nouvelle fonction à l'objet. Les tenants de la valeur supérieure de la vie privée et de la sécurité informatique dans le groupe pouvaient s'en émouvoir par principe, légitimement ou non, mais un tel produit, qui a connu un franc succès en l'occurrence, n'aurait simplement pas existé avec une marge bénéficiaire moindre, ou avec un prix de départ plus élevé et dissuasif. Valait-il mieux démocratiser ce type d'appareils en réponse à une demande par ailleurs forte des consommateurs, ou continuer de les réserver à des clients plus fortunés ?

L'épisode particulier du robot Monsieur Cuisine fut en tout cas le moment le plus révélateur de ce que le groupe IoT était une forme de microcosme des débats experts sur la sécurité informatique et la vie privée, un petit théâtre dans lequel se rejouaient évidemment des débats plus anciens et plus larges. Les acteurs eux aussi en étaient finalement assez stéréotypiques, tels que le chercheur du secteur public attaché à des principes jugés impossibles à mettre en œuvre dans l'état d'un marché mieux connu par un industriel habitué à raisonner dans un cadre commercial très contraignant.

En termes de dynamique des débats, les arguments les plus fortement défendus – au-delà des principes de base autour de la sécurité informatique et de la vie privée qui nous réunissaient – ont finalement été ceux de la nécessité économique de produire vite à et moins coût. Il n'était pas forcément si problématique que le cadre initial soit celui d'une charte plutôt que d'un label plus complet et contraignant, c'est d'ailleurs une des préconisations de Dominique Boullier dans « Rendre le numérique habitable » : il faut « Contraindre les développeurs via des labels et des assurances à adopter un principe de privacy-by-design et en

l'étendant. »[476] Il précise bien que cela doit se faire dans une logique de *privacy by design*, c'est-à-dire dès la conception, jusque dans le design du choix, et pas seulement *ex post* par un contrôle des données récoltées[477]. Quoiqu'il n'ait jamais été officiellement prévu de créer un cadre pour des audits à partir du label que nous aurions créé, le groupe IoT m'a longtemps semblé tout de même aller dans la direction préconisée par Boullier. Mais cette ambition a, entre autres choses, mais en grande partie, buté sur une limite également identifiée immédiatement après dans ce passage du texte de Boullier. Il affirme que « La priorité donnée à la sécurité sur la vitesse doit être réaffirmée, ce qui ne peut que ralentir tous les processus, mais c'est la condition »[478]. Cette condition, en l'espèce n'a pas été remplie. La priorité restant dans l'IoT, et en tout cas d'après les représentants du monde économique qui se sont exprimés dans le groupe IoT, à la vitesse de conception, de production et de vente de produits à la durée de vie généralement courte, les ambitions initiales portées par l'ISOC n'ont pas trouvé d'aboutissement à leur mesure.

Cette séquence de recherche-action est emblématique du risque permanent de *privacy washing* qui guette ce type d'initiative, par une transposition de l'expression *green washing* dans le domaine de l'écologie et de la protection de l'environnement. Il n'est pas difficile pour les entreprises d'accepter de participer à un groupe de réflexion, voire de le lancer, de signer des chartes, d'identifier de bonnes pratiques… et surtout d'en faire la publicité, que ce soit auprès des consommateurs ou, en l'espèce, sans doute aussi beaucoup aux représentants des pouvoirs publics et de régulateurs présents, comme l'ANSSI. Au sein même d'une entreprise, la participation à un tel groupe peut aussi servir la stratégie d'une équipe ou d'une autre simplement en interne, par exemple pour témoigner de son activité. Même dans le cas du groupe de travail IoT dont la publication actuelle n'a pas encore eu de retentissement particulier, le coût de participation était de toute façon minimal, et les engagements à prendre sans conséquence.

Au bout du compte, force est de constater que ce groupe fut un échec : la seule véritable production finale est un texte minimal pour le communiqué de presse associé à 22 recommandations très générales. Elles ne peuvent reprendre que la portion congrue des

[476] D. BOULLIER, « Rendre le numérique habitable : l'habitèle », *op. cit.*, p. 14
[477] En version plus longue : « Ce ne sont pas seulement les données personnelles qui doivent être récupérées et contrôlées mais aussi les traces de tous les comportements les plus élémentaires, avec un choix d'opt-in délibéré et non seulement de opt-out (avec l'option adoptée par défaut). Les architectes de choix numériques doivent être des contrôleurs algorithmiciens comme le proposent Mayer-Schoenberger et Cukier pour être certains que les principes déclarés sont effectivement mis en œuvre, ce qui suppose tests et validation, tout comme cela se fait pour la mise sur le marché des médicaments. Car ces architectures attentionnelles produisent des effets d'attachement à haut risque. »
[478] D. BOULLIER, « Rendre le numérique habitable : l'habitèle », *op. cit.*, p. 14

éléments évoqués lors des discussions sur le projet de charte, et le format très court de la publication ne permet plus d'entrer dans le détail technique de chaque mesure. Surtout, une charte n'a pas de caractère très contraignant, mais des recommandations n'en ont quant à elles absolument aucun. Jusqu'à l'été, les documents de coordination mentionnaient encore un « travail jusqu'à fin 2019 » qui laissait penser que des approfondissements ultérieurs auraient été possibles, mais il n'y a plus eu d'activité apparente du groupe au-delà de juillet 2019. La fin des travaux du groupe IoT a été actée fin 2019, avec donc une partie des bonnes pratiques identifiées dans le projet de charte réduites à 22 recommandations comme seul rendu final.

III - LA REUSSITE A VENIR DU CYBER-SCORE EN COURS D'ELABORATION EN FRANCE ?

Si le projet du groupe ISOC/IoT n'a pas abouti, une initiative de labellisation comparable a néanmoins vu le jour en France pour les services numériques à destination du grand public, le « CyberScore ». Il résulte d'une proposition de loi du sénateur UDI Laurent Lafon, président de la commission de la Culture, dont la première lecture a été faite au Sénat le 15 juillet 2020 avant d'être définitivement adoptée par les députés le 3 mars 2022[479]. Elle ajoute un article au livre premier du code de la consommation disposant que :

> *Alinéa 1 : « Les opérateurs de plateformes en ligne (…) et les personnes qui fournissent des services de communications interpersonnelles (…) réalisent un audit de cybersécurité, dont les résultats sont présentés au consommateur (…), portant sur la sécurisation et la localisation des données qu'ils hébergent, directement ou par l'intermédiaire d'un tiers, et sur leur propre sécurisation (…)*
>
> *Alinéa 4 : « Le résultat de l'audit est présenté au consommateur de façon lisible, claire et compréhensible et est accompagné d'une présentation ou d'une expression complémentaire, au moyen d'un système d'information coloriel. »*[480]

[479] Pour l'historique détaillé de la navette parlementaire de cette loi, voir le site du Sénat à l'adresse suivante : http://www.senat.fr/dossier-legislatif/ppl19-629.html

[480] Anon., « Loi n° 2022-309 du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public », dans *Code de la consommation*, 3 mars 2022 (en ligne : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045294275 ; consulté le 26 juillet 2022)

On retrouve ici les deux bases de la proposition antérieure du Nutri-score dans l'alimentation : une labellisation dont les données sont fournies directement par les industriels sous la forme de logos colorés sur l'emballage ou la page de présentation du produit. Cette filiation est complètement assumée par le législateur, et d'ailleurs souvent reprise dans les titres et manchettes de presse[481,482]. Les propos du sénateur Lafon recueillis par Marc Rees résument parfaitement cette ambition :

> *« Quand on utilise un outil numérique, on n'a pas connaissance du risque qu'il présente en termes de cybersécurité. Il fallait donc, à l'image de ce qu'il peut exister sur le plan alimentaire avec le Nutri-Score ou sur le plan immobilier avec le DPE, avoir une information synthétique, visuelle et accessible immédiatement à tous les usagers, quel que soit leur degré de connaissance et portant sur des risques qu'ils prendront à utiliser et livrer des données sur une plateforme »*

En somme, le Cyberscore accomplit la mission que s'était fixé le groupe ISOC/IoT en termes d'information au consommateur. Pour ce qui est des critères techniques et des modalités graphiques précises qui seront mises en œuvre, elles s'appuieront sur l'expertise technique de l'ANSSI pour l'homologation des auditeurs (ANSSI qui était, pour rappel, membre du groupe ISOC/IoT) et de la CNIL, selon le texte des alinéas 2 et 3 :

> *Alinéa 2 : « L'audit mentionné au premier alinéa est effectué par des prestataires d'audit qualifiés par l'Agence nationale de la sécurité des systèmes d'information.*
>
> *Alinéa 3 : « Un arrêté conjoint des ministres chargés du numérique et de la consommation, pris après avis de la Commission nationale de l'informatique et des libertés, fixe les critères qui sont pris en compte par l'audit prévu au même premier alinéa et ses conditions en matière de durée de validité ainsi que les modalités de sa présentation. »*[483]

---

[481] J. LAUSSON, « Après le NutriScore pour l'alimentation, voilà le CyberScore pour la sécurité des sites », *Numerama*, 25 novembre 2021 (en ligne : https://www.numerama.com/tech/758555-apres-le-nutriscore-pour-lalimentation-voila-le-cyberscore-pour-la-securite-des-sites.html ; consulté le 26 novembre 2021)

[482] M. REES, « Cyberscore : vers un vote conforme de la proposition de loi au Sénat », *Next INpact*, 18 février 2022 (en ligne : https://www.nextinpact.com/article/49887/cyberscore-vers-vote-conforme-proposition-loi-au-senat ; consulté le 18 février 2022)

[483] Anon., *Loi n° 2022-309 du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public*, *op. cit.*

En effet, la loi 2022-309 n'est pas d'application directe, mais rééquerrera que soient définies ses modalités d'application ultérieurement. Il n'est donc pas encore possible de savoir sous quelle forme se présentera le CyberScore. En outre, il n'est pas encore tout à fait exclu que cette loi ne soit finalement pas promulguée, faute de décrets d'application, mais le cas est aujourd'hui de plus en plus rare[484] et le CyberScore devrait voir le jour en 2022 ou 2023.

[484] J. MORIN, « Faute de décret d'application, un tiers des lois n'est pas promulgué », *BFM TV*, 12 juin 2015 (en ligne : https://www.bfmtv.com/politique/parlement/faute-de-decret-d-application-un-tiers-des-lois-n-est-pas-promulgue_AN-201506120073.html ; consulté le 26 juillet 2022)

Chapitre 3 - LE TRAITEMENT LOCAL DES DONNEES : UNE PRIVACY ENHANCING TECHNOLOGY ?

> *« Avec l'augmentation galopante des usages du numérique, de plus en plus de personnes prennent conscience des risques de divulgation de données personnelles. Un certain nombre de mécanismes, réunis sous le vocable de Privacy Enhancing Technologies (PETs), entendent apporter une réponse technique à ce problème. Construits selon les principes de Privacy by Design, ils permettent l'émergence de services ayant comme objectif de protéger efficacement la vie privée, dans des domaines et dans des environnements variés. »*[485]

Le *privacy by design* est un principe porté par les régulateurs publics depuis les années 1990 pour préserver au maximum la vie privée des utilisateurs d'outils numériques. Outre ses déclinaisons légales, le *privacy by design* peut également être mis en pratique dans l'élaboration même des objets et logiciels traitant des données personnelles. On parle alors de *privacy-enhancing technologies* (PET) ou de « technologies préservant la vie privée »[485]. Pour reprendre Laurent et Kaâniche, les PET sont la « réponse technique à ce problème » du *privacy by design*. Elles distinguent trois types de PET : les « techniques orientées utilisateurs », les « techniques orientées serveur » et les « techniques orientées canal de communication »[486]. Autrement dit, il est possible d'agir sur le terminal, le serveur ou le réseau. D'une certaine manière, les PET sont l'antithèse des *dark patterns*, qui visent au contraire à maximiser la collecte de données personnelles sans que l'utilisateur en ait forcément conscience (voir « Tromper l'utilisateur aujourd'hui », p. 207).

Pour reprendre Boullier et Sloterdijk, les PET seraient des outils architecturaux à destination des concepteurs d'objets et de logiciels, permettant d'ériger autour de l'utilisateur et de ses pratiques numériques des murs comparables à ceux qui compartimentent déjà le domicile : « Les candidats habitants du numérique réclament déjà un intérieur, par exemple grâce à la cryptographie car « une unité d'habitation réussie, du point de vue architectural, ne représente pas seulement un morceau d'air entouré de bâtiments, mais plus encore un système d'immunité psychosocial en mesure de régler selon ses besoins son degré d'étanchéité par

[485] M. LAURENT et N. KAANICHE, *Personnalisation de services : quelles technologies pour la préservation de la vie privée ?*, Paris (France), Chaire Valeurs et Politiques des Information Personnelles, 2019, p. 5
[486] *Ibid.*, p. 12

rapport à l'extérieur » (Sloterdijk, *Écumes*, p. 511). »[487] Nous allons voir que cette analogie du mur numérique, en matière de domotique connectée, n'est pas loin de faire coïncider comparant et comparé.

I - LE TRAITEMENT LOCAL DES DONNEES, MARTINGALE DE LA PROTECTION DE LA VIE PRIVEE DES UTILISATEURS ?

Dans le modèle actuel qui prévaut pour les enceintes connectées, la quasi-totalité des données est transmise aux serveurs du fabricant de l'enceinte, traitées à distance, avant qu'une réponse ne soit envoyée sur l'enceinte de l'utilisateur selon la commande initiale. Il peut s'agir par exemple de la lecture d'informations tirées de Wikipédia pour une question du type « qui est Barack Obama ? », de commandes envoyées à un appareil connecté pour une question du type « allume la lumière du salon », ou encore de la lecture d'un flux audio pour une requête musicale. Bien souvent, quand un appareil d'une marque tierce est impliqué, la circulation de la requête passe en outre par les serveurs de cette marque. Dans l'ensemble, les utilisateurs d'enceintes connectées semblent conscients de cet état de fait. Tous les utilisateurs interrogés en sont conscients, et quoique l'échantillon ne soit pas représentatif de la population générale, cette connaissance est vraisemblablement très largement répandue. Comme on le voit plus longuement dans la sous-partie « La question de l'écoute permanente » (page 266), même l'utilisateur le plus désinvolte ou le moins informé techniquement doit à un moment donné connecter son enceinte à son modem-routeur (« box » Internet) en Wi-Fi, ou constate bien vite que des problèmes de connexion à Internet rendent son appareil presque inutilisable.

L'un des principaux moyens offerts par les PET pour appliquer le *privacy by design* à la domotique connectée aujourd'hui est de traiter ces données localement, c'est-à-dire sans recourir aux serveurs des fabricants. Il s'agit à la fois d'une technique orientée utilisateur et orientée serveur en cela qu'elle confine les captats du logis au logis, et que les *feedbacks* sont eux aussi produits par un appareil au logis. L'enceinte connectée, comme *hub* domotique, est l'appareil tout indiqué pour centraliser ces captats et *feedbacks*.

Cette solution permet aussi de limiter la question du canal de communication au seul réseau domestique, puisque les données ne transitent plus vers les serveurs des fabricants. Les périphériques peuvent se connecter à l'enceinte par Wi-Fi ou par Bluetooth sans transmission supplémentaire à Internet, ce qui n'empêche que de les piloter *via* l'application du fabricant,

[487] D. BOULLIER, « Rendre le numérique habitable : l'habitèle », *op. cit.*

comme l'explique par exemple l'entreprise Konyks à propos de sa gamme d'objets connectés Easy (voir Figure 24, ci-dessous).

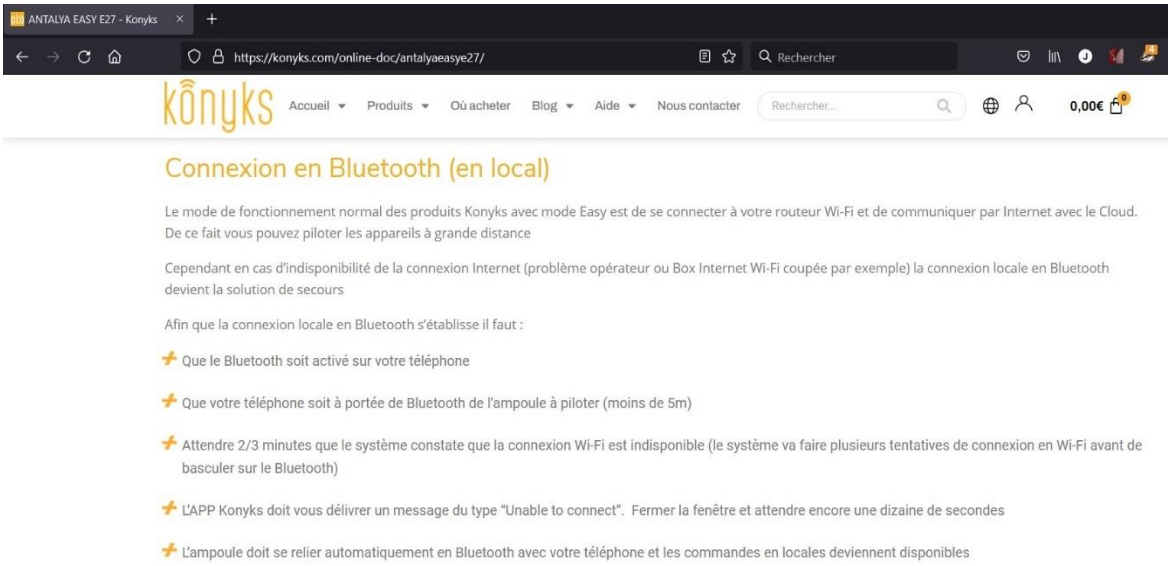


Figure 24 - Explication du mode de fonctionnement local sur le site de la marque Konyks (29/VIII/2021)

Il est par ailleurs techniquement facile de vérifier que le mode de fonctionnement local est effectif, ne serait-ce qu'en coupant l'accès à Internet de la box de l'utilisateur. Des solutions moins triviales ont par ailleurs fait l'objet de tout un pan de la recherche sur la vie privée numérique, par exemple avec le développement de l'outil *IoT Inspector* à l'université de Princeton, qui visait initialement à vérifier que les appareils connectés ne communiquaient bien avec des serveurs distants qu'aux moment désirés[488].

La base de l'argument pour le traitement local est que l'utilisateur garde la maîtrise sur ses données, argument qui a été évoqué directement par certains enquêtés ou lors des réunions du groupe de travail ISOC/IoT. Pour E19, médecin retraitée, ce principe était fondamental dans sa pratique professionnelle :

> « E19: Oui enfin moi je suis pas... alors si je prends le versant professionnel où bah maintenant au niveau des données médicales tout est saisi dans des gros systèmes, y compris le dossier partagé vanté par la sécurité sociale etc. où on nous dit que, bah, tout est verrouillé, tout çi, tout ça, moi j'y crois pas du tout ! En tant que professionnelle, moi je n'y crois pas, à ça ! Et je me suis toujours refusée... alors

[488] D. Y. HUANG *et al.*, « IoT Inspector: Crowdsourcing Labeled Network Traffic from Smart Home Devices at Scale », *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 4, nº 2, 15 juin 2020, p. 46:1-46:21 (en ligne : https://doi.org/10.1145/3397333 ; consulté le 18 novembre 2020)

bon, je suis partie aussi juste...
JF: ...au moment du basculement ?
E19: Oui. Parce qu'on avait évidemment un système informatique, mais je rentrais un minimum de données et je gardais mes dossiers papiers.
JF: Oui.
E19: J'ai pu m'accrocher à mon dossier papier jusqu'à ce que je parte. La fille qui a pris ma suite, elle saisit, hein, mais... moi, je fais pas confiance, en fait. Je suis d'une génération... Alors bon, il y a peut-être des gens qui ont notre âge qui font une confiance aveugle, mais moi je ne fais pas confiance (elle insiste) . Clairement, je ne fais pas confiance. Clairement je ne fais pas confiance à tous ces systèmes.
JF: Même en local ? C'est-à-dire sur votre ordinateur, vous savez ce qui...
E19: Sur le disque-dur ?
JF: Oui.
E19: Alors, pour mon usage professionnel je mettais quand même un certain nombre de choses sur mon disque-dur local. Heu... En local un peu plus, je dirais, mais: et encore.»
(entretien 12, 8 min 40 s)

Ce principe de travail était chez elle directement lié à la question de la confidentialité des échanges entre médecin et patient, et fait écho aux exemples médicaux couramment repris par Nissenbaum dans *Privacy in context*. Il est d'ailleurs à noter que E19 applique ce principe de manière plus souple dans le contexte de sa vie quotidienne. L'intérêt du traitement local des données a également été une question très évoquée dans le cadre du groupe de travail ISOC/IoT, cette fois plutôt dans le prolongement du principe de minimisation de la collecte de données à caractère personnel inscrit dans le RGPD.

D'un point de vue strictement technique, la quasi-totalité des enjeux de protection de la vie privée vis-à-vis des entreprises tient donc au lien internétique entre les terminaux et périphériques chez l'utilisateur avec les serveurs de leurs fabricants. Sans aucune connexion à Internet des enceintes et des éléments domotiques associés, les seules questions de vie privée qui pourraient être soulevées seraient liées à l'ingérence de personnes ayant accès eux-mêmes aux terminaux, par exemple un compagnon jaloux qui vérifierait l'historique d'utilisation de l'enceinte connectée pour vérifier si sa compagne avait bien allumé les lumières, ouvert un rideau roulant ou lancé de la musique *via* le Bluetooth à un moment où elle aurait affirmé être au domicile. En somme, les cas de figure des épreuves du privé liés à la *smart home* seraient infiniment moins variés. Le traitement en local des données peut donc apparaître comme la martingale permettant l'émergence du marché des enceintes connectées et de la domotique associée, sans pour autant compromettre le recours à ces technologies – et le modèle d'affaires de leurs fabricants.

Plus récemment, la question du traitement local des données a également été liée à celle de l'*edge computing*, qui désigne une logique proche : maintenir le contrôle de l'utilisateur sur des données stockées sur un ordinateur auquel il a accès, à l'*edge* ou au bord du réseau (comme l'enceinte connectée), et dont il maîtrise les communications externes, quand bien même ce ne serait pas directement le terminal ayant servi à collecter les données[489]. L'*edge computing* désigne plutôt un principe général d'action sur la topologie des réseaux qui consiste à rapprocher les terminaux traitant les données des appareils les collectant, et d'éviter ce faisant d'avoir recours à une architecture réseau très centralisée, d'autant plus pertinent avec l'émergence de l'IoT. Ce principe de portée générale ne vise pas forcément à la protection de la vie privée : d'un point de vue technique, il peut s'agir plus modestement d'assurer la robustesse d'un réseau en limitant le caractère critique d'un serveur central, par exemple en cas de panne. Il n'en est pas moins pertinent dans ce contexte, le rapprochement des points de contrôle des utilisateurs finaux assurant aussi leur plus grande maîtrise sur leurs données.

II - DES FONCTIONNALITES EN LOCAL FORCEMENT PLUS LIMITEES

Du point de vue de la protection de la vie privée et en considérant avant tout la question de la circulation de l'information, le traitement local peut sembler être une solution idéale, pour la domotique en particulier. Cette solution est d'ailleurs régulièrement évoquée par les fabricants d'enceintes connectées eux-mêmes. Cependant, il ne faut pas omettre que la question de la circulation des données n'est pas la seule à prendre en compte. Quoique les enceintes connectées soient de véritables ordinateurs, et donc capables de traitements, les utiliser sans connexion à Internet revient à les priver d'accès à des bases de données et à des capacités de traitement supérieures ou mises à jour en temps réel. Typiquement, cela implique qu'une enceinte connectée doive stocker localement les logiciels et données nécessaires au traitement du langage naturel comme à la synthèse vocale pour être opérante. Il faudra donc la doter de la mémoire *ad hoc* et elle sera presque forcément toujours en retard sur les dernières mises à jour de ces logiciels. De même, là où Google, Amazon et Apple s'appuient sur Wikipédia pour que leurs enceintes répondent aux questions de culture générale de leurs utilisateurs, il faudrait forcément distribuer à chaque appareils la base de données correspondante pour assurer le même niveau de service. Pour la question de la sécurité informatique, là où il est assez facile

[489] R. RIOS *et al.*, « Personal IoT Privacy Control at the Edge », *IEEE Security & Privacy*, vol. 20, janvier 2022, p. 23-32 (en ligne : https://www.computer.org/csdl/magazine/sp/2022/01/09516686/1watX9oWPe0 ; consulté le 23 mars 2022)

de mettre à jour un serveur central auquel des périphériques même datés adresseraient leurs requêtes *via* une API, il faudrait en revanche mettre à jour individuellement tous les logiciels de chaque application correspondant à telle ou telle marque pour assurer de la correction de chaque faille. Dans les faits, la question du traitement local des données est donc une excellente solution du point de vue de la transmission des données, mais beaucoup moins en termes de traitement.

Du côté des appareils eux-mêmes se pose également la question de leur pilotage en l'absence de véritables standards industriels. À titre d'exemple, les ampoules connectées de la marque Konyks sont capables de réagir à la musique diffusée par le *smartphone* sur lequel l'application permettant leur configuration a été installée, afin de créer une ambiance associant son et lumière. Cette fonctionnalité, étant liée à l'application sur smartphone, ne peut être retrouvée à travers un pilotage par une enceinte connectée, qui elle est seulement capable de paramétrages simples de l'intensité lumineuse ou de la température de couleur. En somme, l'intégration de fonctionnalités étant inégale selon les marques, et en l'absence de protocoles standards couvrant l'ensemble des usages, il y a toujours besoin du logiciel (et donc des serveurs) des fabricants d'objets connectés pour certains usages précis.

L'option semble néanmoins désirée par les utilisateurs… mais avant tout comme une option, et pas au détriment de la praticité. On le voit dans l'extrait suivant avec le discours de E15 et E14 :

> « Heu... est-ce que vous préfèreriez que les données... enfin, tout ce qui passe par l'enceinte, par exemple, reste en local. Qu'il y ait la possibilité d'avoir l'assistant et tout, mais que ce soit du local, sans passer par un serveur d'Apple à un moment ?
> E15: Bahhhh... (petite pause) Pourquoi pas.
> E14: (plus circonspect) Pour la même qualité de service, oui ?
> E15: Moi, pour la même qualité de service, oui, c'est sûr.
> E14: Je préfèrerais, ouais. Parce que...
> E15: (interrompant) Avoir son cloud à soi. Parce que maintenant on a des appartements qui sont... connectés en... en fibre optique, donc du coup c'est rapide (quel rapport avec un réseau local ?) donc... oui, c'est sûr. Ce serait du cloud interne, avec tous les services intégrés dedans, heu... (longue pause)
> JF: Mais du coup, ce serait pourquoi ? Qu'est-ce qui ferait que ce serait mieux ? Eviter d'avoir des données dans la nature ou... efficacité énergétique, ou...?
> E15: Bah que mes données personnelles restent personnelles et ne soient pas diffusées à d'autres.
> E14: Que ça reste physiquement ici.
> E15: Ouais.
> E14: C'est ça l'idée, en fait, je pense.

E15: Bah oui oui. » (entretien 9, 1 h 18 min)

Les deux sont favorables à l'idée sur le principe (E15 : « Bahhhh... (petite pause) Pourquoi pas », E14 : « Je préfèrerais, ouais. »). Lorsque je leur demande si cela pourrait être pour une question de dissémination des données ou d'écologie, dans le but d'élargir le champ argumentatif, ils n'en reviennent pas moins tous deux à la question de la vie privée (E15: « Bah que mes données personnelles restent personnelles et ne soient pas diffusées à d'autres » et E14 : « Que ça reste physiquement ici. »). Ils ont donc une véritable sensibilité à la question, qu'ils ont d'ailleurs techniquement mise en œuvre pour le stockage de leurs fichiers personnels du type photos etc. en installant chez eux un système de NAS assez élaboré, dont la redondance est assurée *via* Internet par la mise en commun avec un de leurs amis avec qui ils sécurisent mutuellement leurs données en cas de dommage physique de l'une ou l'autre unité de stockage[490]. Pour autant, et en ce qui concerne leur enceinte connectée, l'intérêt du traitement en local ne leur semble valoir qu'à la condition exclusive que cela se fasse « pour la même qualité de service », et « avec tous les services intégrés dedans ». Au moins pour leur enceinte connectée et leur domotique, il leur semble donc inconcevable de transiger avec les fonctionnalités offertes avec un traitement qui, pour l'heure, n'est possible qu'au moyen de serveurs distants.

Le constat est similaire avec E3, même en abordant la question simplement technique de la limitation des échanges au sein du réseau local, dont l'économie aurait pu séduire un profil d'ingénieur. E3 n'est absolument pas intéressé ni ne se sent concerné par cette limitation. Du point de vue technique, il lui importe surtout que les commandes soient exécutées rapidement. En fait, il est même d'autant plus impressionné de la réactivité de sa domotique qu'il sait que les captats ont été envoyés vers des serveurs distants où ils ont été interprétés, avant de revenir chez lui sous forme de commande pour ses appareils :

> [>E3]: Donc quand tu sais que tu envoies, ça va dans le cloud d'Amazon, c'est interprété, ensuite ça va chercher... là où ils stockent leurs skills ça s'appelle "lambda", et donc ça va dans "lambda", lambda va chercher la skill qui correspond bien, y a tout un cheminement. Ensuite ça répond, c'est renvoyé, là on est sur Philips, donc ça va interroger le site de Philips. Alors y a toute l'authentification qui est déjà

[490] Procédure dont il faut signaler qu'elle n'est pas systématiquement mise en œuvre même par des entreprises spécialisées à destination des entreprises, comme en témoigne les conséquences de l'incendie dans les locaux du premier hébergeur français, OVH. Voir J. LAUSSON, « Le terrible incendie chez OVH rappelle l'enjeu de la redondance pour les sites web », *Numerama*, 10 mars 2021 (en ligne : https://www.numerama.com/tech/695843-le-terrible-incendie-chez-ovh-rappelle-lenjeu-de-la-redondance-pour-les-sites-web.html ; consulté le 2 janvier 2023)

gérée parce que c'est toi au début qui dit "j'autorise machin tout le temps" et compagnie.

[27:20] [>JF]: Oui.

[>E3]: ...donc hop ça se connecte directement sur ton compte, ça récupère le truc, ça envoie l'information, lui après ça envoie le truc, ça retourne de l'autre côté pour dire "ok, d'accord".[27:32] Tout ça se fait hyper rapidement.

(entretien 1, 27 min)

J'observe même chez lui une certaine excitation technique à l'idée que sa commande vocale a justement circulé par beaucoup de points distants et qu'elle arrive pourtant si vite jusqu'aux ampoules de sa cuisine. En somme, il lui semble beaucoup plus important que la *magie* de la commande vocale opère (voir « Un fantasme technophile en cours d'actualisation », p. 368) plutôt que de limiter les communications de sa domotique avec des tiers dont il ne juge pas si grave qu'ils aient accès à ses données d'utilisation de leurs appareils.

III - L'ECHEC COMMERCIAL DE CETTE FONCTIONNALITE

Force est de constater que l'intérêt relatif manifesté par des utilisateurs de domotique connectée relativement à l'utilisation en local de leurs appareils se retrouve dans la timidité de la stratégie commerciale des principaux fabricants en la matière. Alphabet et Apple annoncent depuis des années le développement de telles solutions, sans qu'elles aient encore vu le jour. En France, seule une entreprise a déclaré son intention de fonder son modèle d'affaires sur la domotique en local, Snips :

> *« Ce n'est pas une enceinte connectée mais un module de calculs, une espèce de petit hub que l'on met dans un placard. À côté de ça, il y a des petits microphones, des petites télécommandes vocales que l'on place où l'on veut. Il n'y a rien qui sort de la maison. Nous garantissons à 100 % que personne ne peut vous surveiller. Nous vous garantissons l'absence de surveillance de masse. L'idée est que n'importe quel objet qui intègre l'assistant Snips puisse parler avec un objet ayant la technologie. »*[491]

[491] M. MOSCA, « Snips : "nous voulons détruire Alexa" Entretien avec Rand Hindi, son fondateur », *Les Numériques*, 26 août 2018 (en ligne : https://www.lesnumeriques.com/assistant-domotique/rand-hindi-snips-veut-detruire-alexa-a3897.html ; consulté le 7 décembre 2018)

Le discours de son fondateur, Rand Hinidi, se fondait en 2018 très clairement sur l'idée que l'utilisation en local était la meilleure garantie que « personne ne peut vous surveiller », jouant donc clairement la carte de la préservation de la vie de ses clients contre tout intérêt économique ou politique extérieur à « la maison ». S'y ajoutaient également d'intéressantes propositions techniques, comme le fait de pouvoir disséminer des micros dans l'espace domestique. L'idée de Snips était donc de jouer entièrement sur la carte du *hub* domotique plutôt que de chercher à vendre une enceinte connectée, avec une intelligence certaine de l'intérêt de ce type de dispositifs (voir « Le hub domotique », p. 304).

Malgré la volonté de son fondateur de concurrencer Amazon et Google, Snips n'a jamais produit de *hub* domotique en marque propre, ni réussit à s'imposer comme marque blanche dans le marché d'entreprise à entreprise souhaitant intégrer un assistant vocal fonctionnant localement, modèle d'affaires que mettait en avant Hindi en 2018[491]. Entre 2012 et 2019, la *start-up* aura levé 22 millions d'euros[492], avant d'être racheté pour 37,5 millions de dollars par Sonos, entreprise étatsunienne spécialisée dans le matériel hi-fi[493]. Sonos était la première entreprise à avoir intégré dans sa Sonos One les assistants Alexa et Google Assistant, avant de proposer une barre de son Sonos Ray dotée de son propre assistant vocal propriétaire fondé sur le logiciel de Snips[494]. Sans méjuger l'intérêt des produits de Sonos, on peut considérer ce rachat comme un échec commercial relatif pour Snips, dénotant un intérêt limité des investisseurs pour le modèle d'affaires d'un assistant vocal en local.

Du reste, certaines résistances persisteront chez les utilisateurs. E19 en est un cas paroxystique : elle explique être tout juste plus confiante dans le stockage de données en local, surtout pour ce qui concerne des données professionnelles qu'elle stockait malgré tout avec parcimonie sur son poste, lui préférant des « dossiers papier » :

> « E19: Oui enfin moi je suis pas... alors si je prends le versant professionnel où bah maintenant au niveau des données médicales tout est saisi dans des gros systèmes, y compris le dossier partagé vanté par la sécurité sociale etc. où on nous dit que, bah, tout est verrouillé, tout çi, tout ça, moi j'y crois pas du tout ! En tant que professionnelle, moi je n'y crois pas, à ça ! Et je me suis toujours refusée... alors

[492] M. NIZON, « L'ICO de Snips passée au crible des 3 critères de notre fiche d'analyse. », sur *Le Crowdfunding, ça vous chatouille ou ça vous gratouille ?*, 24 juin 2018 (en ligne : https://www.michelnizon.com/lico-de-snips-passee-au-crible-des-3-criteres-de-notre-fiche-danalyse/ ; consulté le 3 janvier 2023)
[493] Anon., « Sonos rachète Snips, qui développe un assistant numérique respectueux de la vie privée », *Next INpact*, s. d. (en ligne : https://www.nextinpact.com/lebrief/40641/10397-sonos-rachete-snips--qui-developpe-un-assistant-numerique-respectueux-de-la-vie-privee# ; consulté le 3 janvier 2023)
[494] Anon., « Sonos lance sa nouvelle barre de son Ray et son propre assistant vocal », *Next INpact*, 13 mai 2022 (en ligne : https://www.nextinpact.com/lebrief/69170/sonos-lance-sa-nouvelle-barre-son-ray-et-son-propre-assistant-vocal ; consulté le 16 mai 2022)

bon, je suis partie aussi juste...
JF: ...au moment du basculement ?
E19: Oui. Parce qu'on avait évidemment un système informatique, mais je rentrais un minimum de données et je gardais mes dossiers papiers.
(…)
JF: Même en local ? C'est-à-dire sur votre ordinateur, vous savez ce qui...
E19: Sur le disque-dur ?
JF: Oui.
E19: Alors, pour mon usage professionnel je mettais quand même un certain nombre de choses sur mon disque-dur local. Heu... En local un peu plus, je dirais, mais: et encore.»
(entretien 12 ; 9 min)

Malgré les garanties importantes fournies par la Sécurité sociale, elle est restée vent debout contre la télétransmission des données de santé de ses patients jusqu'à son départ à la retraite. Elle explique sa réticence par un effet de « génération »[495]. Elle craint notamment la possibilité d'un piratage, quand bien même ces données ne seraient pas amenées à circuler par construction, comme c'est le cas de données renseignées dans le fichier-patient de la Sécurité sociale. Il faut cependant préciser qu'elle n'a appliqué ce luxe de précaution qu'aux données de ses patients, qu'elle juge éminemment sensibles, mais qu'elle utilise parcimonieusement des logiciels comme WhatsApp pour communiquer avec sa famille.

Si l'on écarte le critère générationnel, même l'un des jeunes enquêtés, E5, extrêmement réticent lui aussi à la dissémination de ses données comportementales, déclare utiliser volontiers des machines non-connectées à Internet, sans crainte pour sa vie privée – y compris lorsqu'elles fonctionnent avec des logiciels en source fermée, comme son vieux Mac. Le point commun avec E19 reste sa grande méfiance quant à toute possibilité de voir des données être transmises à des tiers avec une machine connectée à Internet, même avec un logiciel supposé fonctionner localement. Si ce niveau de méfiance reste sans doute rare, il laisse malgré tout penser qu'une certaine frange de la population ne fera jamais totalement confiance aux promesses de conservation des données en local.

[495] L'évaluation de différences générationnelles dans le rapport à la vie privée n'est pas aisée, et en tout cas impossible à généraliser à partir du matériel empirique de la présente thèse. Dans une étude longitudinale de 2013 s'appuyant sur les cohortes du *General Social Survey* aux États-Unis ayant répondu à la question de l'approbation ou non des écoutes téléphoniques et de la simple collecte de données informatisées par le gouvernement, les résultats suggèrent en effet des différences générationnelles, mais qui pourraient tenir à d'autres facteurs requérant une analyse multivariée plus fine : « *Specifically we believe that multivariate analyses of income, familiarity with technology and gender might enable us to better understand the underlying explanations for generational variations*. ». P. M. REGAN, G. FITZGERALD et P. BALINT, « Generational views of information privacy? », *Innovation: The European Journal of Social Science Research*, vol. 26, nº 1-2, mars 2013, p. 98 (en ligne : http://www.tandfonline.com/doi/abs/10.1080/13511610.2013.747650 ; consulté le 7 juillet 2021)

Si aucun signal véritablement positif n'est venu de mes enquêtés quant à la possibilité d'utiliser des enceintes connectées en local, et même au contraire, il semble néanmoins que la solution soit de plus en plus sérieusement envisagée pour l'IoT. En témoigne par exemple le grand succès d'un article de prospective publié en 2016 dans le journal de l'Institute of Electronical and Electronics Engineers (IEEE) dédié à l'IoT, ayant été déjà été cité 2 515 fois[496], et traitant du *edge computing*[497]. Les auteurs défendent l'idée que le modèle actuel du *cloud computing*, très centralisé, ne serait pas pérenne, ni du reste que sa pérennité soit souhaitable. Ils défendent entre autres choses l'idée que l'*edge computing* serait plus compatible avec la préservation de la vie privée des utilisateurs finaux, quoique dans un cadre qui dépasse largement la domotique connectée.

*

En somme, le *privacy paradox* présente un véritable intérêt historique dans le développement des questionnements sur la vie privée à l'ère numérique. Il a en particulier contribué à ancrer un principe méthodologique capital dans le champ, à savoir le fait d'inscrire les réflexions dans des situations concrètes, là où le caractère philosophique et/ou légal de la notion de vie privée menait souvent à des développements plutôt théoriques. Il doit cependant être dépassé aujourd'hui, dans la mesure où ce paradoxe n'est qu'apparent.

La notion de *privacy paradox* me semble tenir au fond sur deux piliers insatisfaisants. D'une part, sur un plan moral, elle oppose le sérieux apparent de la protection de la vie privée, érigée comme valeur cardinale qui devrait être absolue à l'apparente désinvolture des individus lorsqu'il leur est proposé de ne pas en tenir compte pour un bénéfice minime. D'autre part, elle méconnaît le fait que les individus sont dans un rapport de pouvoir asymétrique avec les entreprises qui collectent et utilisent leurs données. Étant admis que des pans entiers de nos vies sont placés sous le régime de médiations numériques, le *privacy paradox* ne tient plus : il n'y aurait paradoxe que s'il y avait véritablement un choix à faire. Deux enquêtés en particulier qui sont extrêmement soucieux de protéger leurs données personnelles, E5 et E20, ont ainsi toutes les peines du monde à mettre en œuvre leurs principes malgré des dispositions mentales, des capacités et des moyens remarquables par comparaison avec la population générale. Le *privacy paradox,* qui semble être une contradiction dans les pratiques effectives des individus, est en fait un problème à résoudre au niveau de la régulation – étant entendu que les projets de société

[496] Au 29 septembre 2021.
[497] W. SHI *et al.*, « Edge Computing: Vision and Challenges », *IEEE Internet of Things Journal*, vol. 3, nº 5, octobre 2016, p. 637-646

des GAFAM ne permettent pas de laissez-faire des régulateurs dans le domaine, sauf à accepter le bien-fondé de ces projets, et de renoncer aux principes de liberté individuelle aujourd'hui en vigueur dans beaucoup d'esprits, et surtout dans les lois.

CONCLUSION PARTIELLE

Nous avons vu dans la partie précédente qu'il fallait se départir progressivement de l'imaginaire territorial strictement axé sur l'espace qui a prévalu jusqu'alors, et assurait la protection de la vie privée par l'architecture concrète des domiciles. La numérisation en cours du monde a d'abord porté sur l'augmentation des espaces publics, puis des spatialités des individus à travers le smartphone plus particulièrement. Les espaces privés domestiques en tant que tels sont d'une certaine manière le front pionnier actuel de cette tendance pour les industriels, même s'ils étaient déjà quelque peu ouverts aux circulations de données numériques à travers l'ordinateur personnel connecté à Internet ou le smartphone utilisé au domicile. L'enjeu actuel est de questionner la manière dont des types de données nouvelles seront produites et collectées par et depuis la smart home augmentée d'un nombre croissant de capteurs et d'objets du quotidien capables de communications de machine à machine.

Le droit et la régulation proposent déjà des outils puissants pour encadrer ces pratiques déjà anciennes et bien connues, quoiqu'elles s'étendent à des espaces nouveaux où des enjeux spécifiques sont mobilisés. La législation européenne s'est plus particulièrement dotée du RGPD en 2016, dont les principes inspirés des *privacy-enhancing technologies* s'appliquent tout à fait à l'IoT domestique. Pour autant, il reste beaucoup à faire en ce qui concerne l'information et l'encapacitation des utilisateurs : la critique savante du *privacy paradox* doit s'accompagner de mesures concrètes pour la résorption de ce qui est avant tout une asymétrie d'information voire de maîtrise d'usage entre les utilisateurs et les producteurs d'objets ou de services connectés. La recherche-action à laquelle j'ai participé pour ce travail de doctorat a été un échec opérationnel qui aura au moins eu l'intérêt d'éclairer les risques susceptibles d'obérer le succès de telles initiatives.

En tout état de cause, s'il faut envisager les nouvelles limites augmentées des espaces domestiques non comme de strictes barrières mais plutôt comme de nouvelles frontières plus ou moins poreuses à la circulation des données, il est très clair que la gestion de cette porosité doit revenir aux habitants de ces espaces domestiques augmentés. Le sentiment d'absence de maîtrise sur ses données personnelles qui prévaut aujourd'hui dans l'utilisation de la plupart des services numériques ou augmentés ne doit pas s'étendre à l'espace domestique et aux pratiques qui s'y font, ce qui serait un recul important du point de vue du droit et de l'habitabilité du monde, dans lequel le domicile a été largement sanctuarisé au cours des deux derniers siècles

et au moins pour l'Europe et l'Amérique du Nord. L'apparent paradoxe d'une « topographie réticulaire » articulant l'espace tangible du domicile et l'espace internétique doit devenir une réalité dans laquelle les habitants exercent leur légitimité sur un espace plus ouvert, à la manière dont le *megatrend* de la mondialisation a permis l'interconnexion des espaces à l'échelle mondiale sans pour autant remettre en cause les souverainetés nationales légitimes.

Nous allons donc maintenant nous attacher à voir dans la finesse des pratiques quotidiennes les plus élémentaires comment les individus interagissent déjà avec l'IoT domestique et plus particulièrement les enceintes connectées, afin d'identifier quels sont les enjeux pratiques spécifiques en matière de vie privée dans l'habitation de la *smart home*.

Partie 4 - VIVRE CHEZ SOI AVEC LES OBJETS CONNECTES : LE CAS DE L'ENCEINTE

L'émergence d'Internet et de la domotique connectée a considérablement complexifié l'architecture technique de l'espace domestique. L'eau et l'électricité, parfois le gaz, et plus récemment le téléphone ont été durant une grande partie du XXe siècle les seuls réseaux techniques desquels les résidents avaient à se soucier. Et encore s'agissait-il essentiellement de savoir ouvrir ou couper un point d'arrivée général au domicile, effectuer un occasionnel relevé de compteur, et savoir « brancher » ses appareils - ce qui peut demander un peu de travail pour l'eau et le gaz, mais ne pose aucune difficulté à une personne valide pour l'électricité ou le téléphone. Les personnes qui avaient à se *soucier* de leur rapport à ces réseaux dans un pays développé étaient finalement très peu nombreuses : un chef d'entreprise souhaitant préserver le secret industriel pouvait éventuellement juger utile de faire attention à une écoute téléphonique, un cultivateur de cannabis en armoire intérieure pouvait s'inquiéter du fait que la consommation électrique de ses lampes trahisse son activité… et tout un chacun pouvait, bien sûr, s'inquiéter de dysfonctionnements plus ou moins graves allant du dégât des eaux à l'explosion d'une conduite de gaz. Mais, dans l'ensemble, l'essentiel de nos rapports à ces réseaux étaient fonctionnellement simples, et n'introduisaient guère d'enjeux pour leurs utilisateurs finaux.

Il en va bien autrement à l'ère numérique, en ce qui concerne le « branchement » aux réseaux numériques et singulièrement à Internet, et même aujourd'hui pour ce qui touche aux anciens réseaux, dont les nouveaux compteurs connectés posent à leur tour des questions nouvelles d'immixtion dans la vie privée domestique des abonnés. Comme on l'a vu, le point de départ de cette thèse est justement d'interroger une première réaction récurrente des personnes confrontées à la question de l'utilisation potentielle ou effective des enceintes connectées : le fait qu'elles soient d'abord vues comme des objets intrusifs, de véritables micros-espions du phonotope domestique (chapitre 1). Je fais l'hypothèse que le microphone est un capteur sonore inquiétant pour beaucoup de personnes, au même titre que la

vidéosurveillance dans l'espace public, mais avec des modalités évidemment spécifiques au captat sonore et au design de ces enceintes conçues pour s'intégrer à nos domiciles et à s'interfacer avec un nombre toujours plus grand de nos appareils.

Si l'on *habite*, évidemment, l'espace de son domicile, mais aussi les pratiques que l'on y déploie et qui nous transforment en retour, la question de savoir comment vivre avec les objets connectés devient une question aussi capitale que celle de savoir comment évoluerait notre rapport à l'espace public au moment de l'émergence de la vidéosurveillance. Si les objets connectés, même très élaborés, ne peuvent au mieux que singer l'acteur à travers leurs fonctions conversationnelles et d'activation de nos objets connectés, il ne fait en revanche aucun doute qu'ils sont des actants de plus en plus puissants de nos vies, et singulièrement de nos vies domestiques en ce qui concerne Alexa, Google Home ou HomePod, et la myriade d'objets-satellites qui gravitent autour de ces *hubs* techniques agissant comme de véritables maîtres d'orchestre domotiques (chapitre 2). Selon la manière dont les utilisateurs construisent leur rapport affectif à l'enceinte connectée, elle pourra être considérée comme un simple assistant, un concierge, voire un quasi-membre de la famille, une gouvernante sans corps (chapitre 3).

Au-delà du rapport à l'enceinte connectée comme objet technique se pose la question du statut de l'enceinte comme un objet interlocuteur. Les fabricants d'enceintes connectées recherchent en effet un certain niveau d'anthropomorphisme de ces objets, dont les capacités à converser avec les utilisateurs en langage naturel ainsi qu'à répondre à des requêtes ou à des questions parfois assez complexes, voire à fonctionner de manière automatique, les ramènent au niveau de quasi-acteurs, de quasi-personnages dans la vie familiale et domestique.

Chapitre 1 - L'ESPIONNE

De toutes les réactions possibles à l'évocation des enceintes connectées, le réflexe de rejet face à l'idée d'avoir un micro connecté à Internet à l'écoute de tout ce qui se passe dans son salon est l'un des plus constants. Ce, que la question soit posée à de potentiels enquêtés, dans une conversation banale… ou aux diverses personnes avec qui j'ai vécu ces dernières années au moment de leur proposer d'installer chez nous l'Amazon Echo dont je disposais pour me familiariser moi-même à la vie avec ces appareils. C'est le premier réflexe des opposants à ces objets, et même souvent une réticence initiale qu'on retrouve chez les personnes plus ouvertes. L'enceinte est généralement considérée d'abord comme un espion actif : on la craint pour elle-même. À ce titre, la réaction d'E19 à l'évocation de Google Home ou d'Alexa, dans les débuts de notre entretien, est exemplaire :

> « Je pense que... a priori je ne pense pas que vous en ayez, mais peut-être que vous connaissez des gens qui en ont une ? Tout ce qui est Google Home, Amazon Alexa...
> E19: Mais ça c'est se mettre un espion dans sa maison, quoi.
> François: Ouais ouais !
> JF: Ah moi je... (levant les mains de l'air de dire que je n'en dis rien)
> E19: Clairement ! Je trouve ça... rigo... enfin, entre guillemets rigolo, mais si on réfléchit un tout petit peu plus, enfin... On a les heures d'allées, de venues, de rentrée, de sortie, d'habitudes, allumer la télé, écouter de la musique, quelle radio... Enfin...! Tout quoi.
> François: Ouais. »
> (entretien 12 ; 16 min 10 s)

L'idée est ici exprimée dans sa forme la plus directe : une enceinte connectée, c'est un « espion dans sa maison », un mouchard rendant ou pouvant rendre compte de la totalité de faits et gestes jugés importants, qu'il s'agisse de la présence au domicile (« les heures d'allées, de venues (…) ») ou de la manière de s'informer (« allumer la télé, (…) quelle radio… »). Quant au reste des périphériques domotiques (caméra, serrure…), nous allons voir qu'ils sont plutôt envisagés comme des points de vulnérabilité, de possible intrusion dans l'espace domestique : les enquêtés craignent ce qui pourrait en être fait plutôt que ce qu'ils font directement. Ils sont en cela alignés avec la littérature scientifique en sécurité informatique.

L'enceinte connectée a d'abord été plutôt l'association d'une enceinte et d'un microphone connectés. C'est donc d'abord la question de la captation audio qui a cristallisé les réticences motivées par la protection de la vie privée à l'égard de ces objets. Pour autant, la captation vidéo est rapidement devenue elle aussi un sujet de préoccupation, que ce soit par

l'intégration de webcams dans l'IoT domestique, ou plus récemment par l'adjonction d'écrans et de webcams dans les enceintes connectées elles-mêmes. Les dernières expérimentations des fabricants d'enceintes connectées laissent à penser que des fonctions de captation de mouvement, même sans instrument de captation optique, permettront à terme même aux enceintes les plus simples de pouvoir visualiser les intérieurs domestiques.

I - LA QUESTION DE L'ECOUTE PERMANENTE

La fonction de base des enceintes connectées et, plus largement, des assistants vocaux, est de fournir une interface vocale interactive entre des utilisateurs et des logiciels – logiciels qui pourront eux-mêmes actionner des équipements connectés ou interagir à terme avec d'autres humains. L'intérêt technique singulier de l'enceinte connectée est donc d'introduire dans un phonotope moins une enceinte qu'un micro s'appuyant sur une fonction logicielle de traitement automatisé du langage naturel (TALN). Dans la vaste majorité des cas, cette fonction logicielle n'est pas opérée localement, c'est-à-dire dans l'enceinte, mais sur des serveurs distants opérés par le fabricant de l'enceinte. Cette réalité, techniquement triviale, ne l'était cependant pas pour le grand public dans les premiers temps du déploiement de cette nouvelle gamme d'objets, et elle n'a longtemps pas fait l'objet de communications grand public de la part des fabricants d'enceintes connectées. La véritable publicisation de cet état de fait a eu lieu à l'été 2019, deux ans après les premières sorties d'enceintes connectées en France, été durant lequel les acteurs majeurs du secteur ont fini par devoir communiquer à ce sujet après une série de scandales médiatiques[498]. Elle s'inscrit dans la suite directe d'une série de révélations et de scandales qui permettent de faire l'inventaire des réactions et des craintes liées à la captation audio des sons du domicile.

Des microphones toujours activés par défaut

La question de l'écoute permanente par les enceintes a sans doute été la première des menaces perçues contre la vie privée des / par les utilisateurs. Dans son expression la plus basique, elle consiste à se demander si les micros de l'enceinte écoutent en permanence leur environnement sonore, ou phonotope. La question est devenue un marronnier persistant jusqu'à aujourd'hui, particulièrement dans la presse spécialisée. Elle est devenue un sujet de conversation courant, ainsi que la question spécifique qui m'a sans doute été le plus

[498] M. BIERI et F. VALLET, *À votre écoute - Exploration des enjeux éthiques, techniques et juridiques des assistants vocaux*, Paris (France), CNIL, 2020, p. 41

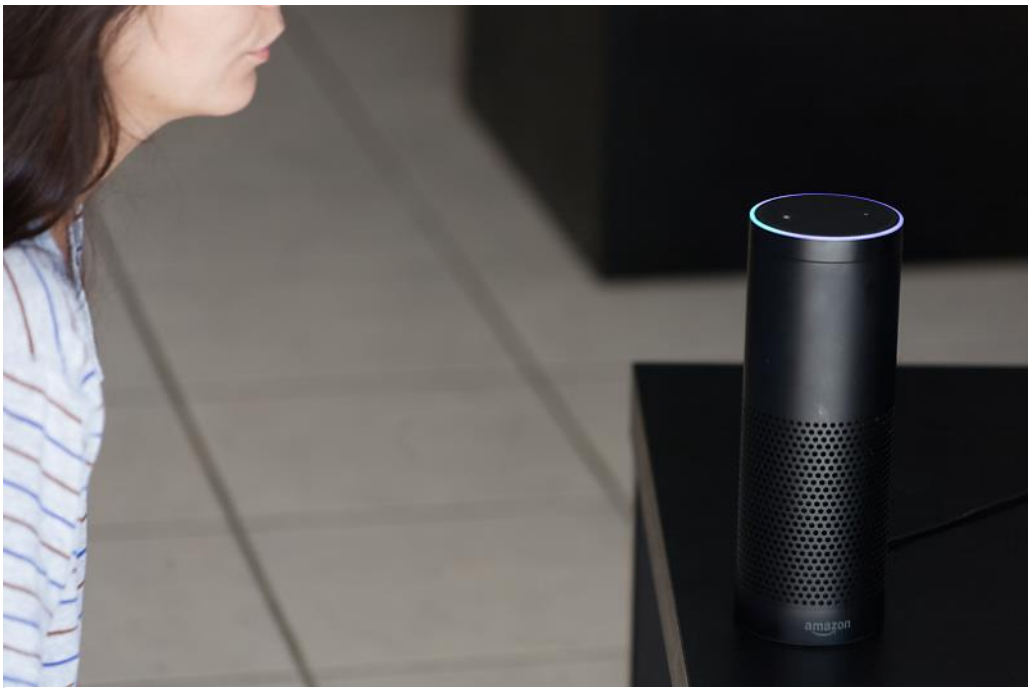
régulièrement posée par des enquêtés potentiels ou par des personnes apprenant quel était mon sujet de travail dans des conversations plus banales. Elle a même donné lieu à une publication dédiée du laboratoire LINC de la CNIL en juillet 2021, dont le titre humoristique évoquant une conversation dans un couple, « Chéri(e), mon smartphone m'écoute ?! »[499], suggère bien sa récurrence banale. Bien qu'elle ait déjà été d'usage pour les *smartphones*, elle est beaucoup plus centrale dans le cas des enceintes connectées, dont la fixité, l'alimentation filaire plutôt que par batterie, et la connexion permanente à Internet a pu inquiéter davantage les utilisateurs. La réponse sur le plan technique a donc été apportée par les fabricants plus particulièrement à l'été 2019, dans leur communication institutionnelle comme dans leurs tutoriaux et conditions d'utilisation : oui, les micros de l'enceinte sont toujours activés par défaut, puisqu'elle doit pouvoir être activée à la voix à tout moment. Pour autant, tout n'est pas durablement enregistré par l'enceinte, et encore moins systématiquement téléversé sur les serveurs du constructeur. La communication des constructeurs à ce propos semble avoir été assez bien comprise, tant par mes enquêtés que dans les commentaires des groupes d'utilisateurs sur les réseaux sociaux.

> « Alors que si elle t'écoutait sans avoir posé la question, là ce serait grave.
> JF: Alors il y a des cas de petites erreurs...
> E6: Oui.
> E7: Oui oui.
> JF: Mais ça tu considères que...
> E6: C'est pas grave.
> E7: Ben après techniquement non, sinon elle s'allumerait, si elle t'écoutait (pas compris) A moins qu'elle soit prévue au contraire pour avoir un usage... sous-marin !
> E6: Ca ça me dégoûterait complètement. Je la couperais le lendemain.
> E7: Je pense pas ! Ce serait pas dans l'intérêt de la société. » (entretien 3 ; 47 min 30 s)

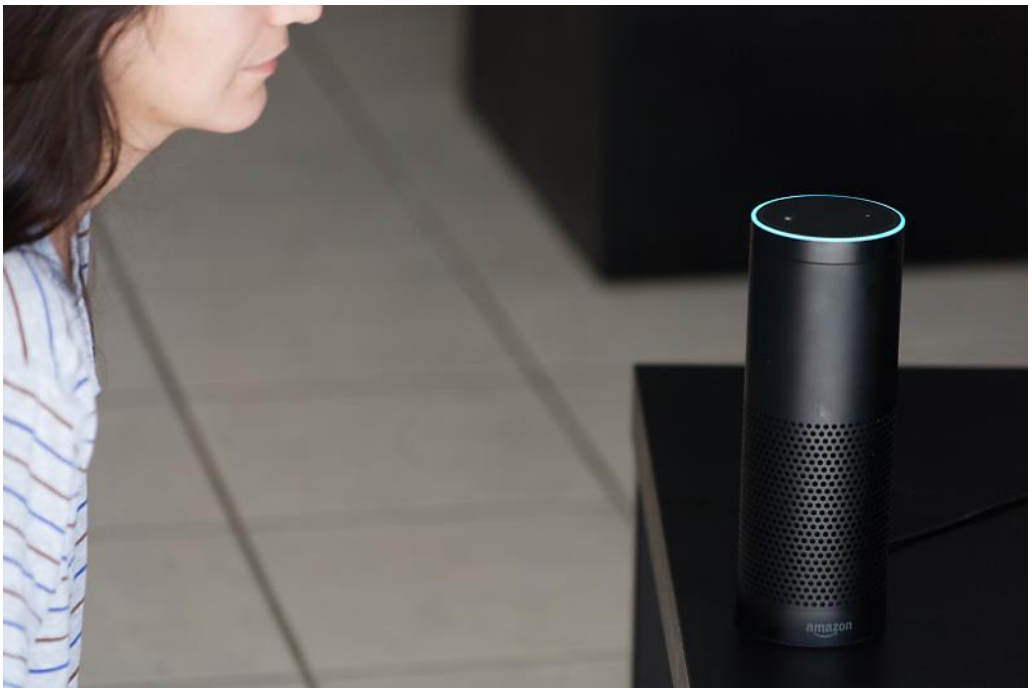
Au-delà de la seule communication des entreprises, le design même des enceintes a sans doute facilité la compréhension de leur mode de fonctionnement. En tout premier lieu, le fait de devoir recourir à un mot de réveil (« Alexa », « Okay Google », « Dis Siri »…) fait office d'interrupteur vocal : sans ce mot de réveil, l'enceinte ne déclenche aucune action. Bien que le microphone soit effectivement activé en permanence par défaut, c'est le mot de réveil qui fait qu'un captat audio est enregistré, transmis, traité, puis déclenche l'action souhaitée. La plupart des enceintes sont également équipées de diodes lumineuses qui signalent le fait qu'elles passent à une écoute active. Sur le modèle Echo d'Amazon, équipé d'une diode circulaire, le

[499] F. VALLET, « Chéri(e), mon smartphone m'écoute ?! », 2 juillet 2021 (en ligne : https://linc.cnil.fr/fr/cherie-mon-smartphone-mecoute ; consulté le 30 août 2021)

témoin lumineux s’allume même d’une lumière blanche plus vive dans la direction de la source de son écouté après une activation de l’enceinte par son mot de réveil (voir Photographie 13), à la suite de quoi une animation circulaire de la diode signale à l’utilisateur que l’enceinte est en train de transmettre la séquence audio ou de recevoir la réponse attendue de la part du serveur (voir Photographie 12). Un bouton physique pour désactiver le microphone est souvent présent également.



Photographie 13 - Une utilisatrice active une enceinte Amazon Echo avec le mot de réveil "Alexa" et prononce sa requête. La diode circulaire s'allume en bleu et affiche une zone lumineuse blanche en direction de la source vocale (JFP, 2021)



Photographie 12 - L'utilisatrice s'étant tue, l'enceinte Echo signale qu'elle est en train de traiter la demande par un témoin lumineux faisant le tour de la diode circulaire, avant de donner sa réponse (JFP 2021)

Ces éléments de design apportent à l'utilisateur un *feedback* qui le renseigne sur le fonctionnement de l'enceinte. Plus indirectement, ce sont aussi les dysfonctionnements de l'enceinte qui permettent de comprendre son fonctionnement. Par exemple, lorsque l'enceinte réagit à une « fausse » sollicitation : prononcer une phrase comme « qu'est-ce que c'est que ça ? » activera ainsi bien souvent une enceinte d'Amazon dont le mot de réveil est « Alexa ». L'enceinte ne va alors pas forcément répondre, ne pouvant pas interpréter d'ordre, mais l'activation du témoin lumineux informe l'utilisateur que l'écoute active aura été brièvement enclenchée. *A contrario*, les enceintes ne réagissent pas toujours aux véritables sollicitations, forçant l'utilisateur à répéter le mot de réveil, parfois à plusieurs reprises, éventuellement à se rapprocher de l'enceinte pour formuler sa commande. Ces interactions fonctionnelles ou dysfonctionnelles renseignent sur les capacités techniques de l'objet et permettent à l'utilisateur d'intérioriser une forme de proxémie avec l'objet, et en particulier de savoir quelle est la portée efficace de ses micros.

Il est également possible de consulter son historique d'interactions avec l'enceinte pour constater soi-même ce qui est archivé sur les serveurs du fabricant. E8 décrit bien la démarche, qu'il a effectuée :

> « E8: Donc je pense que l'impact est assez limité, par rapport à ça. Heu... alors est-ce que tout fonctionne comme ça, je ne sais pas. Est-ce que c'est aussi une réalité, je sais pas. Après c'est vrai que quand on va dans l'historique, où on peut voir tout ce qui a été entendu par la machine, on a quand même cette... on voit effectivement vraiment tout ce qu'on a pu dire et tout ce qu'on a pu demander, mais que depuis le moment où le mot de réveil a été prononcé. Pas avant, pas après. » (entretien 4, 37 min 40 s)

Conscient du fait qu'il ne peut pas savoir avec certitude si Amazon est sincère dans l'affichage de l'historique (« alors est-ce que tout fonctionne comme ça, je ne sais pas. Est-ce que c'est aussi une réalité, je sais pas »), il semble néanmoins convaincu du fait que l'activation au moyen du mot de réveil est bien nécessaire pour qu'un enregistrement soit effectué et transmis aux serveurs d'Amazon. La transparence de l'entreprise sur les données collectées, sous forme de captats audio consultables et de la transcription de la séquence telle qu'elle a été comprise par le logiciel, lui semble un gage de bonne foi. Il évoque d'ailleurs ensuite les cas où ces informations ont été réclamées par la police dans le cadre d'enquêtes aux États-Unis comme un argument supplémentaire : il n'y avait *a priori* pas d'enregistrements supplémentaires disponibles d'après ce qu'il a retenu de l'affaire, à raison – du moins, aucun qui ait été

officiellement évoqué et retenu dans la procédure judiciaire. Si l'on consulte attentivement un historique de navigation Alexa, ici sur le modèle installé dans mon propre logement, on peut d'ailleurs constater que l'interface distingue même les captats considérés comme des activations accidentelles par le message « L'audio n'était pas destiné à Alexa », alors qu'une interaction normale comme « Alexa volume down » est directement transcrite (voir Figure 25).

Figure 25 - Extrait d'un historique de commandes vocales sur Alexa, avec le cas d'une activation accidentelle (JFP, 2022)

D'une certaine manière, cette transparence de l'historique est rassurante pour l'utilisateur, qui peut constater quand son enceinte s'active, y compris quand elle s'active à tort. En l'espèce, c'est la phrase « Alex ça a eu l'air de lui plaire » qui a été interprétée à tort comme un mot de réveil, alors qu'il s'agissait d'un prénom (« Alex ») phonétiquement proche du mot de réveil de cette enceinte (le mot de réveil par défaut, « Alexa »), prononcé dans une phrase sans rapport avec l'enceinte au cours d'une conversation. On peut ajouter que l'interface permet la suppression de tout ou partie de l'historique vocal, et même de corriger ou de préciser quelle était le sens d'une requête pour contribuer à l'amélioration du logiciel de transcription automatique d'Amazon. Google et Apple proposent des historiques à l'interface très similaires pour leurs propres produits.

Il reste à noter que les faux positifs sont tout de même légion. En outre, la reconnaissance de la signature vocale des utilisateurs étant encore peu aboutie, il est également possible pour d'autres personnes que les utilisateurs légitimes de l'enceinte de la déclencher à l'envi, comme l'illustre cette planche dessinée de l'illustrateur XKCD, malicieusement signalée par E5 (voir Figure 26), où un invité arrivant chez des amis disposant d'une enceinte connectée Echo commande de butte en blanc sur Amazon « deux tonnes de maïs façon crème » (trad. pers.).

Figure 26 - «Listening » par XKCD, https://xkcd.com/1807 [en ligne], consulté le 30/X/2020

Si ce cas de figure est fictionnel, la possibilité d'activer à la voix des enceintes connectées de tiers a été utilisé à dessein *via* l'un des médias ayant un accès privilégié au phonotope domestique, à savoir la télévision. Une mise en application réelle de l'ajout de produits dans le panier Amazon d'utilisateurs d'Alexa a ainsi été faite massivement le 13 septembre 2017 lors de la diffusion du premier épisode de la vingt-et-unième saison de la série animée étatsunienne *South Park*.[500] L'épisode se présentait comme une satire de ces nouveaux objets et des utilisateurs tendant à se reposer toujours plus sur eux dans le moindre aspect de leurs vies. Au prétexte de montrer un personnage s'adressant à des enceintes connectées dans le cadre du récit, le but des créateurs de la série était évidemment d'activer les enceintes réellement possédées par les téléspectateurs dans une remarquable démonstration de bris du quatrième mur. La commande volontairement grotesque de « *hairy balls* » (« roubignoles » dans la version française) ne s'est pas faite seulement au détriment des parents de l'un des

[500] C. MACDONALD, « "I never knew Alexa had such a potty mouth": South Park episode activates viewers' Alexa and Google Home devices, creating "erroneous alarms" and shopping lists for "hairy balls" », *Daily Mail Online*, DMG Media Limited, 14 septembre 2017 (en ligne : http://global.factiva.com/redir/default.aspx?P=sa&an=DAMONL0020170914ed9e0093x&cat=a&ep=ASE ; consulté le 31 août 2021)

Figure 27 - Capture d'écran à 1 min 10 s de l'épisode 1 de la saison 24 de la série animée mettant en scène des personnages passant des commandes loufoques sur leur enceinte Echo, provoquant l'activation de celles des téléspectateurs

personnages, mais bien également à celui des téléspectateurs possédant réellement une enceinte Echo.

Dans un registre plus convenu, l'entreprise Burger King avait déjà exploité le procédé en avril de la même année, cette fois à une fin promotionnelle. [501] Un acteur costumé comme un caissier de la marque de restauration rapide s'adresse ainsi au téléspectateur pour lui faire la promotion du burger historique de la marque, le Whopper, en précisant immédiatement que les quinze secondes du *spot* publicitaire ne lui permettraient pas d'en énumérer tous les ingrédients. Il fait alors mine d'avoir une idée, et lance une commande « Ok Google » pour que les enceintes de la marque poursuivent l'énumération des ingrédients elles-mêmes à partir de la fiche Wikipédia du produit.

Si l'exemple de *South Park* a un intérêt critique certain, celui de Burger King est une démonstration *marketing* au premier degré, et qui vise un intérêt avant tout commercial. Elle a, à ce titre, été très contestée comme une pratique à réprouver. D'un point de vue commercial, il s'agit d'une forme de concurrence déloyale, puisque cette exploitation du matériel des téléspectateurs concernés permettait de faire durer la publicité au-delà du temps imparti. Ce, au détriment de la publicité suivante, pour ainsi dire parasitée par celle de Burger King, et sans que Google ait été prévenu ou rémunéré – une requête de ce type est considérée comme « naturelle » et non comme un « contenu sponsorisé » pour Google, le moteur de recherche y apporte une réponse sans contrepartie financière. Plus important sans doute : bien que certains aient trouvé la publicité innovante et audacieuse, la plupart des personnes ont surtout vécu l'activation contre leur gré de leur enceinte comme une intrusion pure et simple dans le phonotope de leur domicile. Cette sollicitation commerciale imprévue a dépassé le cadre plus

[501] B. F. RUBIN, « Ads for voice assistants are here and they're already terrible », *CNET News.com*, CNET Networks Inc., 21 avril 2017 (en ligne : http://global.factiva.com/redir/default.aspx?P=sa&an=CNEWSN0020170421ed4l00003&cat=a&ep=ASE ; consulté le 31 août 2021)

ou moins admis du visionnage passif d'une publicité pour entraîner une action concrète dans leur domicile. Dans ce cas de figure, Google Home n'a pas seulement été un potentiel espion collectant discrètement des informations, mais il a été détourné pour devenir un véritable intrus infiltré dans l'espace domestique au moyen du médium sonore.

La transmission prévue de captats audio au fabricant

Pour autant, au-delà de ces cas limites, l'écoute permanente du phonotope domestique par les enceintes (ou l'exploitation commerciale ou humoristique de la mise sous écoute permanente du phonotope) répond le plus souvent à des règles prévues et plus ou moins clairement affichées par les fabricants. E8 résume succinctement un avis partagé par la majorité des enquêtés, y compris les plus critiques :

> « E8: Alors je pense qu'il y a aussi une psychose, entre guillemets, qui peut se faire, où les gens peuvent avoir l'impression d'être écoutés en permanence. Mais faut quand même garder, toute raison garder, ne serait-ce qu'avec un aspect purement, heu, purement pratique du système, où potentiellement on ne peut pas stocker des milliers... des journées entières d'enregistrement concernant des millions d'utilisateurs. C'est pas jouable. » (entretien 4, 38 min 50 s)

Ses termes sont forts, puisqu'il parle de « psychose » (et plus classiquement, à d'autres moments de l'entretien, de « paranoïa ») pour désigner cette crainte qui lui semble irraisonnée d'imaginer que l'ensemble des conversations non-adressées à une enceinte ou un smartphone soient enregistrées et conservées. De fait, cette crainte n'apparaît chez aucun des enquêtés dont le modèle de menace est banal.

Pour les captats audio transmis de façon attendue au fabricant, la reconnaissance vocale ou TALN des assistants vocaux recourt au *machine learning* (une branche de l'intelligence artificielle) pour transcrire et interpréter la parole humaine. Ce processus est automatisé pour une large part, et la qualité des agents conversationnels croît à mesure qu'ils sont utilisés. Néanmoins, une partie de cet apprentissage requiert une intervention humaine, particulièrement en début de développement : il faut d'abord que des humains « éduquent » l'algorithme, puis qu'ils contrôlent tout ou partie des résultats ultérieurs. L'apprentissage-machine est dit « supervisé ». En juillet 2019, Google déclarait ainsi que 0,2% des requêtes vocales à son Assistant étaient réécoutées par des humains[502]. Quoique cette proportion soit infime, ce

[502] D. MONSEES, « More information about our processes to safeguard speech data », sur *Google*, 11 juillet 2019 (en ligne : https://blog.google/products/assistant/more-information-about-our-processes-safeguard-speech-data/ ; consulté le 18 novembre 2020)

processus de vérification permet tout de même de reconstituer des conversations ou des dictées assez complètes, selon un témoignage d'une ancienne sous-traitante de Microsoft ayant travaillé sur l'assistant Cortana en français.

Dans son livre *En attendant les robots*[503], Antonio Casilli décrit combien sont nombreux les personnels de l'ombre derrière l'apparente automaticité des logiciels et robots dans notre quotidien. Ces « travailleurs du clic » effectuent notamment un grand nombre de tâches d'étiquetage pour les jeux de données utilisées par les logiciels d'intelligence artificielle[504], quand ils ne pilotent pas eux-mêmes parfois directement certains effecteurs – par exemple, dans le cas de voitures autonomes où un opérateur humain à distance prend la main sur le logiciel. L'auteur, membre de la Quadrature du Net, a d'ailleurs publié sur leur site un entretien avec une « travailleuse du clic » ayant contribué à l'entraînement du logiciel de reconnaissance vocale UHRS (*Universal Human Relevance System*) utilisé par Microsoft pour son assistant vocal Cortana[505]. Son travail consistait à écouter de courts extraits de requêtes audio pour vérifier qu'elles avaient été bien interprétées. Elle rapporte que la principale mesure de protection de la vie privée des utilisateurs était le découpage des requêtes en séquences de quelques secondes, mais que certaines duraient « plusieurs minutes », et qu'il n'était pas rare d'avoir à traiter suffisamment de bribes d'une même requête pour inférer le profil ou l'humeur de l'utilisateur[506]. Dans un texte de synthèse ultérieur, Casilli et Tubaro affirment que, contrairement aux promesses des industriels, et même avec des logiciels de reconnaissance vocale mâtures, le besoin de recourir à des vérificateurs reste élevé, et que ces « travailleurs du clic » devraient même devenir de plus en plus nombreux avec l'accroissement des usages et des dispositifs connectés[507]. Si des activistes comme LQDN et une partie de la presse ont assez largement

[503] A. A. CASILLI, *En attendant les robots : enquête sur le travail du clic*, Edition augmentée de l'essai « Le travail à inégales distances »., Paris (France), Points, 2021

[504] Il s'agit dans un premier temps de dire au logiciel ce qu'il doit comprendre de telle donnée dans la phase d'entraînement (par exemple, lui indiquer la présence d'un arbre ou d'un visage dans une image donnée), puis de vérifier dans un second temps si les interprétations automatiques du logiciel sont exactes, pour le corriger au besoin.

[505] « Derrière les assistants vocaux, des humains vous entendent », sur *La Quadrature du Net*, 18 mai 2018 (en ligne : https://www.laquadrature.net/2018/05/18/temoin_cortana/ ; consulté le 9 février 2023)

[506] « Nous n'avions jamais l'intégralité des conversations évidemment, elles étaient découpées en petites pistes ; cependant on pouvait tomber sur plusieurs morceaux d'une même conversation dans une même série de transcriptions (c'était suffisant pour dresser un profil basique de l'utilisateur ou de son humeur du moment par exemple). » *in Id.*

[507] « Even when a new voice-activated technology is sufficiently mature and no longer needs human impersonators, the need for workers to prepare datasets and, more importantly, to perform quality checks on outputs remains high. It can even be expected to grow as more and more applications of voice technologies emerge, from home automation to industrial production and even health services (where, for example, nurses can simultaneously provide care to patients and dictate notes about their condition). » *in* P. TUBARO et A. A. CASILLI, « Human Listeners and Virtual Assistants: Privacy and Labor Arbitrage in the Production of Smart Technologies », dans M. E. Graham et F. Ferrari, *Digital Work in the Planetary Market*, Cambridge (États-Unis) et Londres (Royaume-Uni), MIT Press, 2022, p. 188

relayé ces informations sur le mode du scandale, le témoignage de la travailleuse du clic ayant travaillé sur UHRS n'a pas choqué les enquêtés-utilisateurs du panel auxquels je l'ai présenté. La pratique est perçue comme une nécessité technique, et la confiance envers les fabricants est assez forte pour la rendre contextuellement intègre. Ce n'est en revanche pas ou moins le cas dans le cas de transmissions intempestives de captats audio (voir ci-dessous) ou dans des cas de détournement (voir « Le voyeur numérique », p. 283).

La transmission intempestive de captats audio au fabricant

Si le fait que les micros des enceintes soient activés en permanence ne pose donc pas nécessairement problème, plus gênants sont les cas de transmission intempestive de données. Dans le modèle actuel, toute activation par un mot de réveil entraîne l'enregistrement et le téléversement des captats audio. Il n'est pas sûr que ce mécanisme soit tout aussi bien compris des utilisateurs en général, quoiqu'il ait été connu des personnes interrogées pour ma thèse. Là encore, le design et les dysfonctionnements de l'enceinte rendent compte de cet état de fait : la connexion au réseau Wi-Fi domestique est généralement la première étape de configuration d'une enceinte connectée, suivie de l'identification du profil Amazon, Google ou Apple. En outre, en cas de déconnexion ou de mauvaise connexion à Internet, le dysfonctionnement de l'enceinte apparaît en toute évidence et est signalé par un message d'erreur. Le fait que les modèles d'enceinte actuels dépendent très fortement d'une connexion Internet reste donc assez clair.

En revanche, il est plus difficile de maîtriser la transmission des données échangées entre l'enceinte et les services distants. Le journaliste Artem Russakovskii en octobre 2017 a ainsi fait état de l'un des premiers bogues très commentés à propos des enceintes connectées, en l'espace une Google Home Mini dont la gamme venait alors de naître[508]. La situation a été jugée suffisamment sérieuse par Google pour que l'entreprise dépêche un ingénieur chez le journaliste dans les heures suivant son signalement de bogue au service de relations publiques. Un défaut de fabrication des boutons physiques des premières Home Mini entraînait en effet l'envoi presqu'ininterrompu de séquences vocales à Google. Artem Russakovskii s'était bien aperçu que les diodes de son enceinte tendaient à se déclencher très souvent, mais c'est surtout en allant voir l'historique de ses requêtes à son assistant dans son compte Google qu'il s'est

[508] A. RUSSAKOVSKII, « Google is permanently nerfing all Home Minis because mine spied on everything I said 24/7 [Update x2] », sur *Android Police*, 10 octobre 2017 (en ligne : https://www.androidpolice.com/2017/10/10/google-nerfing-home-minis-mine-spied-everything-said-247/ ; consulté le 6 juillet 2021)

aperçu du fait que son enceinte l'enregistrait en permanence. Le bogue a été rapidement résolu par la désactivation (logicielle) pure et simple des boutons défectueux.

En matière d'intempestivité des transmissions de données, se pose enfin la question de la confiance à accorder aux concepteurs mêmes des enceintes pour ne pas récupérer de données subrepticement. Une approche « paranoïaque » consiste à ne pas leur faire confiance du tout… et à remplacer jusqu'aux micros des enceintes, physiquement. Une approche plus modérée a consisté pour des chercheurs à monitorer le trafic réseau sortant des enceintes pour vérifier que les transferts de données correspondaient bien aux moments d'activation de l'enceinte et que peu ou pas de données étaient échangées à d'autres moments – typiquement, pour une mise à jour[509,510,511,512]. Pour autant, même cette démarche a pour limite que ces tests ne valent que sur les enceintes testées et au moment des tests : le logiciel des enceintes étant propriétaire et compilé par les fabricants, il est impossible de garantir totalement la loyauté de leur fonctionnement.

Enfin, il faut signaler que les enquêtés ne craignent pas seulement l'enceinte connectée ou leur *smartphone* pour eux seuls. Si ces appareils sont forcément le vecteur physique de la collecte, de nombreuses craintes sont exprimées vis-à-vis d'applications ou de programmes déloyaux, qui peuvent aussi bien être installés sur des appareils ne surveillant pas leurs utilisateurs par défaut. Il s'agit d'un marronnier journalistique et d'un sujet de conversation extrêmement récurrent, souvent évoqué par mes enquêtés également, et absolument réfuté par un couple seulement du panel[513]. Un article tout à fait représentatif du genre a par exemple été publié dans l'*ADN* en juin 2021, et intitulé de façon quelque peu outrancière « « Chuuut,

[509] M. MORGENSTERN, « Careless Whisper: Does Amazon Echo send data in silent mode? », sur *AV-TEST Internet of Things Security Testing Blog*, 8 juin 2017 (en ligne : https://www.iot-tests.org/2017/06/careless-whisper-does-amazon-echo-send-data-in-silent-mode/ ; consulté le 19 novembre 2020)

[510] A. GHADIRY, « Is My Google Home Spying On Me? », sur *SogetiLabs*, 5 avril 2017 (en ligne : https://labs.sogeti.com/google-home-spying/ ; consulté le 19 novembre 2020)

[511] R. FRAWLEY, « Logging and Analysis of Internet of Things (IoT) Device Network Traffic and Power Consumption », *Master's Theses*, 1er juin 2018 (DOI : 10.15368/theses.2018.60 consulté le 19 novembre 2020)

[512] S. A. ALATKAR, *Detecting Smart Home Activity Through Network Traffic Signatures*, mémoire de master, New York (ÉUA), State University of New York, 2020

[513] « E6: Après peut-être que si on lui demandait explicitement comment c'est Madrid... Ça se trouve, peut-être... En tout cas, elle nous a jamais entendu dire quelque chose, je crois, sans qu'on lui demande, c'est ce que je veux dire.
JF: (j'acquiesce)
E6: On n'a jamais parlé d'aller à Londres et elle nous a jamais fait de pub qu'on lui demandait pas.
E7: Moi je me suis jamais sentie ciblée par les pubs.
E6: Ou alors c'est très subtil (rire).
E7: Ou alors on voit pas. Ouais, non.
E6: Je crois pas. » (entretien 3, 20 min 40 s)

Instagram nous écoute » : retour sur une théorie pas si complotiste que ça » [514]. Le point commun à ces articles et retours d'expérience individuels est la surprise ressentie par nombre d'internautes ayant pu constater qu'un sujet qu'ils venaient d'évoquer à l'oral et à proximité de leur smartphone avait fait presque immédiatement apparition dans les sujets des publicités qui leur étaient destinées en ligne, sujet à propos duquel ils jurent leurs grands dieux n'avoir effectué aucune recherche préalable qui aurait pu guider les algorithmes publicitaires. *Ipso facto*, nous serions donc tous sous écoute permanente afin que soient captés nos sujets d'intérêt monétisables, comme nous le sommes déjà effectivement sur Internet à partir de nos recherches et de notre navigation. Mathieu Cunche, chercheur de l'INRIA de Lyon, interrogé par des journalistes à ce propos résume les raisons consensuelles dans le milieu de la sécurité informatique pour lesquelles ce scénario est improbable : ce serait très coûteux en capacités de stockage, peu efficace à partir d'appareils fonctionnant sur batterie qui se déchargeraient donc extrêmement vite ; et même si ces défauts peuvent être techniquement contournés, ce serait de toute façon aussi illégal qu'inutile en comparaison de la masse considérable d'informations qui peuvent être captées ou inférées beaucoup plus facilement à partir de nos autres pratiques, géolocalisation et navigation en tête. Un chercheur de l'entreprise Kapersky affirme également sur le blog de son entreprise que la coïncidence entre diffusion de publicités et évocation orale du sujet des publicités à proximité d'un *smartphone* n'est pas autre chose qu'une coïncidence, ou le résultat d'une activation involontaire de l'assistant vocal du téléphone[515]. L'intérêt de cette anecdote récurrente est essentiellement qu'elle concerne un public beaucoup plus large que les utilisateurs d'enceintes, qui constituaient une population très faible dans les premiers temps de la thèse, tout en s'appliquant aussi bien et peut-être même davantage encore aux enceintes connectées.

Enfin, il est à signaler plus largement que davantage d'inquiétudes ont été exprimées par mes enquêtés à propos de leurs téléphones portables que de leurs enceintes. Là où l'enceinte a une présence physique et une localisation manifestes, le smartphone se fait en revanche beaucoup plus facilement oublier. Deux enquêtés interrogés dans des entretiens distincts m'ont ainsi rapporté la même anecdote du déclenchement de l'assistant vocal de téléphones au cours d'une réunion professionnelle.

[514] D.-J. RAHMIL, « « Chuuut, Instagram nous écoute » : retour sur une théorie pas si complotiste que ça », *L'ADN*, 30 juin 2021 (en ligne : https://www.ladn.eu/media-mutants/reseaux-sociaux/pourquoi-impression-instagram-ecoute-conversations/ ; consulté le 1er juillet 2021)
[515] A. MALANOV, « Smartphones sur écoute : mythe ou réalité ? », sur *Kapersky Daily*, 6 août 2019 (en ligne : https://www.kaspersky.fr/blog/smartphones-eavesdropping/12070/ ; consulté le 9 janvier 2023)

E3 : Ou alors ils sont sur leur téléphone, et sur leur téléphone sans le savoir « Ok Google » il est déjà activé… Enfin moi ce qui est assez rigolo c'est que le nombre de collègues que j'ai en réunion où t'as le truc qui se déclenche alors que personne n'a dit « Ok Google » mais le téléphone a cru comprendre qu'il y avait ça, du coup il commence à parler. [29:09] Enfin c'est… (entretien 1 ; 29 min)

Au-delà du fait que le phonotope de leur entreprise leur semblait un enjeu important et rendait ces activations plus gênantes, le caractère plus nettement intempestif de ces activations tenait également au fait qu'un iPhone posé sur la table ou glissé dans une poche n'est pas attendu et bien identifié comme activable vocalement. Selon l'enquêté E3, qui travaille pourtant dans le secteur informatique, beaucoup de ses collègues n'ont pas conscience du fait que l'assistant vocal de leur téléphone est activé, là où une enceinte connectée ne laisse presque pas de doute à ce sujet et permet plus simplement une gestion proxémique de la question.

Le risque de piratage des enceintes connectées

Au contraire de la crainte quant à l'utilisation commerciale subreptice de l'accès à leur phonotope domestique par les fabricants d'enceintes connectées, la crainte de piratage par un tiers inquiète beaucoup moins les utilisateurs. La perspective que leur enceinte ou leur réseau domotique soient piratés leur paraît lointaine, voire ridicule :

« E3: Ca écoute en permanence juste pour détecter le mot-clé, et ça écoute en permanence.
E4: Oui mais qu'elle enregistre en fait.
E3: Ca enregistre pas.
E4: Pour moi elle enregistre pas ce qui est dit...
E3: Ca enregistre pas.
E4: ...et je vois mal un mec ou une nana avec un casque "alors vas-y, qu'est-ce qu'ils disent..." (nous rions tous) Tu imagines le job de merde !
E3: Mais c'est des ordinateurs qui font ça aujourd'hui, chérie.
E4: Non mais c'est ça que je veux dire, c'est que je vois pas l'intérêt en fait. » (entretien 1, 1 h 09 min)

Tous deux ont bien conscience que l'écoute de leur phonotope domestique *via* leur enceinte est possible, et ils évoquent d'ailleurs directement ensuite le fait qu'ils aient conscience qu'un acteur puissant comme une agence de renseignement puisse mettre en œuvre de telles pratiques. Mais cette perspective pour un individu isolé les fait rire : « ...et je vois mal un mec ou une nana avec un casque "alors vas-y, qu'est-ce qu'ils disent..." (nous rions tous) Tu imagines le job de merde ! ». De manière plus générale, quand les questions de piratage sont évoquées, c'est avant tout quant aux serrures connectées ou aux volets ouvrants que le niveau de vigilance des

enquêtés remonte (voir « La serrure connectée : une réticence provisoire ? », p. 359), mais pas ou très peu quant à leur phonotope.

De ce point de vue, la seule enquêtée utilisatrice d'une enceinte connectée dont l'insouciance vis-à-vis de l'écoute potentielle de son phonotope ait baissé est E21. Néanmoins, dans son cas particulier, ce changement est dû à l'évolution de son modèle de menace dans lequel c'est moins la perspective de l'aléa en soi que l'accroissement des enjeux dans son phonotope qui a changé la donne, à travers l'entrée en politique potentielle, au moment de l'entretien, d'une partie des membres de sa famille.

Étonnamment, les spécialistes en sécurité informatique sont souvent beaucoup plus critiques voire alarmés quant à la domotique et aux enceintes connectées en tant que failles potentielles de sécurité. Dans un article de son blog consacré à la RFC 9124 sur les mises à jour logicielles dans l'IoT qui concerne plutôt les périphériques domotiques que les enceintes connectées elles-mêmes, Stéphane Bortzmeyer commence clairement par rappeler qu'« On le sait, la sécurité des gadgets nommés « objets connectés » est abyssalement basse. Une de raisons (mais pas la seule, loin de là !) est l'absence d'un mécanisme de mise à jour du logiciel, mécanisme qui pourrait permettre de corriger les inévitables failles de sécurité. Le problème de la mise à jour de ces machins, souvent contraints en ressources, est très vaste et complexe.[516] ». Mais cette inquiétude technique n'a pas de véritable résonnance parmi les enquêtés utilisateurs d'enceintes, sauf chez un couple d'enquêtés dont l'un est informaticien, E15 et E14. Ils sont les seuls à manifester une conscience aigüe de sécurité de leur réseau informatique domestique : quoiqu'ils soient les enquêtés les plus équipés en objets domotiques de mon échantillon, ils ne sont pas allés jusqu'à installer une serrure connectée ou même une sonnette connectée à l'entrée de leur appartement car elle aurait constitué un point d'entrée physique extérieur à leur réseau.

En tout état de cause, aucun piratage ou détournement massif des capacités des enceintes connectées n'a été observé à ce jour. La preuve de concept la plus élaborée d'une possible exploitation des enceintes connectées pour l'écoute subreptice du phonotope domestique a été proposée par des chercheurs du Security Research Labs (SRLabs), Luise Frerichs et Fabian Bräunlein, qui ont découvert qu'il était possible de prolonger l'écoute par une enceinte Alexa très largement au-delà du temps normal en introduisant un caractère spécial spécifique

[516] S. BORTZMEYER, « RFC 9124: A Manifest Information Model for Firmware Updates in Internet of Things (IoT) Devices », sur *Blog de Stéphane Bortzmeyer*, 15 janvier 2022 (en ligne : https://www.bortzmeyer.org/9124.html ; consulté le 1er février 2022)

(U+D801 dans la norme Unicode) dans le code d'une application[517]. Même alors, il faut que l'utilisateur ait installé l'application en question sur le compte lié à son enceinte, que le mot d'appel ait été entendu, et la diode indiquant que l'enceinte est en train d'enregistrer reste allumée (voir Photographie 13). Autrement dit, le risque identifié, même dans cette faille *zero-day* (c'est-à-dire non identifiée au préalable par le fabricant), reste très faible.

II - L'IMAGE CONSIDEREE COMME PLUS CRITIQUE QUE LE SON

Si l'accès au phonotope n'est pas un enjeu extrêmement fort pour l'essentiel des personnes de l'échantillon, leur paysage domestique visuel leur semble en revanche nettement plus critique. Il s'agit nettement d'une ligne de force des propos recensés dans le corpus.

Une surveillance plus difficile à déjouer

Dans la mesure où les enceintes connectées équipées de webcam n'étaient pas encore commercialisées au début de la campagne d'entretiens et qu'elles sont restées assez rares même après cela, c'est plutôt à travers des exemples d'autres technologies de captation vidéo embarquées que l'on appréhendera cette question. Notre cadre analytique de la vie privée comme activité immunitaire permet néanmoins de circonscrire utilement la question à défaut de pouvoir finement approcher les enjeux liés à la captation vidéo par les enceintes connectées en elles-mêmes.

Ainsi, E5, très critique envers les enceintes connectées, n'a jamais été confronté à des modèles équipés de caméras. Pour autant, il évoque spontanément le cas des Google Glass pour relater la force de sa réaction quand il a été confronté à une captation vidéo à laquelle il ne s'attendait pas, en l'occurrence dans la rue. Les Google Glass étaient des lunettes équipées de webcam, connectées et alimentées par batterie, lancées par Google en 2011 avant que leur production et leur vente soient suspendues début 2015 faute de succès et du fait de fortes réticences, entre autres choses vis-à-vis de la vie privée. Depuis 2017, seuls des modèles à destination des entreprises industrielles ont continué à être développés et vendus. Leurs caractéristiques techniques les inscrivent en tout cas très bien dans le champ de l'IoT et des *wearables*. Même s'il n'est pas beaucoup plus indulgent vis-à-vis de la captation audio seule, E5 fait une gradation entre les deux pratiques de collecte de données, en défaveur de la vidéo.

[517] C. CIMPANU, « Alexa and Google Home devices leveraged to phish and eavesdrop on users, again », *ZDNet*, s. d. (en ligne : https://www.zdnet.com/article/alexa-and-google-home-devices-leveraged-to-phish-and-eavesdrop-on-users-again/ ; consulté le 24 mai 2021)

Dans les raisons qu'il mobilise, il semblerait que le fait qu'il soit beaucoup plus difficile d'échapper « [gentiment] » à la vue qu'à l'ouïe semble prépondérante :

> « E5: Non, parce que les Google Glass sont un outil d'enregistrement de capture d'information, de numérisation de ce qui se passe. Que tu es en train d'imposer aux autres. Juste parce que tu es en face de lui. L'autre a deux possibilités, soit s'échapper, soit te... te... [1167,9] de manière plus ou moins gentille et pacifique... j'ai l'impression qu'il y avait une certaine hostilité, une hostilité marquée, à l'époque de Google Glass, vis-à-vis de ça.
> JF: (acquiesce)
> E5: Oui. Moi ça m'est arrivé une fois de voir quelqu'un dans la rue avec des Google Glass, j'ai pas l'impression que... bon. Ça n'a pas été un succès commercial. Et j'avais eu une réaction forte, vraiment. Vraiment épidermique. Soudain, voir quelqu'un et me dire que c'était pas anodin et... je... voilà, je réagissais mal. » (entretien 3 ; 19 min 05 s)

Il décrit sa réaction comme « forte, vraiment épidermique » lorsqu'il a croisé une personne équipée de Google Glass dans la rue, ce qui ne lui a semblé « pas anodin ». Au regard de ses postures déjà très critiques mais nettement plus froides quant aux autres pratiques de surveillance, ce récit m'a semblé particulièrement remarquable dans son entretien. Il décrit même le port de Google Glass comme une pratique « hostile » envers les personnes présentes dans le champ de vision du porteur, dans la mesure où elles sont pour ainsi dire piégées par lui. Le problème n'est pas en soi d'être pris en photo ou télésurveillé : au moment de l'entretien, E5 vit dans un quartier central de Paris depuis plusieurs années déjà, il est déjà accoutumé au fait d'être pris en photo dans la rue ou surveillé par des caméras. C'est donc autre chose qui se joue ici. La surprise face à un dispositif de captation nouveau et très rare, même à l'époque, influe en partie sans doute dans la dimension forte et « épidermique » de sa réaction, terme dont l'implicite signale bien une forte réticence due à une faible sensibilisation préalable, comme s'il s'était brûlé en touchant par inadvertance un objet trop chaud. Pour autant, E5 connaissait déjà largement le dispositif d'un point de vue technique, il ne s'agit donc pas d'une simple réaction de rejet face à l'inconnu ou à la nouveauté. Je retiendrai ici deux axes explicatifs :

- D'abord, il s'agit d'un outil Google, une entreprise dont il mesure et dont il craint l'influence et les capacités techniques de tout premier ordre en matière de collecte et d'organisation de l'information. Le captat résultant cette rencontre impromptue ne sera pas une photographie ou même une petite séquence vidéo qui finira oubliée dans une carte SD au fond du tiroir d'un particulier. Les Googles Glass permettent de classer rigoureusement cette information (horodatage, géolocalisation) après traitement et

conservation sur des serveurs distants, information qui servira ensuite probablement à entraîner des algorithmes de *machine learning* et pourront être corrélées à la pléthore d'autres informations collectées par Google. Cela était d'autant plus vrai sans doute avec une technologie encore en développement de ce type, et donc gourmande en retours d'expérience.

- Ensuite, il n'y a pas *d'échappatoire* (« s'échapper ») facile au regard d'une Google Glass, elle « s'[impose] aux autres ». Il ne finit pas vraiment sa phrase au moment où il évoque la chose, mais on peut supposer qu'il signale ici qu'il serait difficile ou en tout cas malcommode d'avoir à demander de ne pas être objet de captation vidéo au porteur. Eu égard à d'autres moments de l'entretien avec E5, on devine qu'il est gêné par le fait de ne pouvoir lui-même se soustraire à cette forme de surveillance. Là où il pouvait, par exemple, déjouer partiellement le traçage cellulaire de son téléphone portable en ne l'ayant pas systématiquement sur lui de sorte qu'on ne puisse systématiquement corréler la position de son téléphone portable et la position de son propre corps, la présence d'une Google Glass dans son entourage lui donne la sensation d'être acculé et de ne pouvoir mettre en œuvre aucune mesure simple d'évitement.

Plus largement, il semble apparaître en filigrane du discours des enquêtés que l'image serait plus identifiante d'un corps, ou que l'image de soi et l'intimité s'appliquent bien davantage à l'image qu'au son. Ils craignent donc une certaine forme de voyeurisme, y compris algorithmique pour E5 par exemple.

Le voyeur numérique

Dans le langage courant, les termes voyeur et voyeurisme sont très péjoratifs :

> *« Personne, généralement un homme, qui tire son plaisir de la vue de la nudité, des fonctions excrétoires, des rapports sexuels d'autrui. (…) Personne qui se plaît à découvrir des choses intimes, cachées, qui est d'une curiosité malsaine. (…) Trou dissimulé dans une cloison qui permet d'assister, sans être vu, à des scènes de caractère érotique ou obscène (d'apr. Esn. 1965). »*[518]

[518] « Voyeurisme », dans *Trésor de la Langue Française informatisé*, Nancy (France), CNRS & Université de Lorraine, 1994 (en ligne : https://www.cnrtl.fr/definition/voyeurisme ; consulté le 9 août 2022)

La réaction vis-à-vis de la webcam équipant des Google Glass, une enceinte connectée, ou un dispositif de vidéosurveillance est très comparable à la gêne ressentie face au voyeur, qui regarde ce qui est « intime » ou « caché », voyeur qui désigne dans un dernier sens plus rare mais ici très opportun un « trou » permettant de regarder « sans être vu ». La grande différence avec la vidéosurveillance numérique est que le voyeur est généralement un logiciel, envers lequel la relation n'est pas la même qu'envers l'œil d'un humain, et que ce voyeur plus souvent numérique n'est généralement pas dissimulé.

Ainsi, nous avons approfondi dans la sous-partie précédente l'exemple extrême d'E5 qui est de toute façon très critique de toute forme de captation vidéo, y compris de la vidéosurveillance de l'espace public. E3 et E4, eux, ne sont absolument pas opposés à cette dernière, qu'ils estiment être un outil de sécurité efficace et nécessaire, à plus forte raison depuis les attentats de Paris en 2015 qui ont particulièrement marqué E4. Relativement insensibles à une vidéosurveillance publique qu'ils estiment légitime, on a déjà vu qu'ils vont jusqu'à s'amuser qu'un éventuel malfaiteur parvienne à surveiller leur phonotope domestique en détournant leur Echo Dot :

> E4: ...et je vois mal un mec ou une nana avec un casque "alors vas-y, qu'est-ce qu'ils disent..." (nous rions tous) Tu imagines le job de merde ! (entretien 1, 1 h 09 min)

Malgré cette posture qui peut sembler extrême, et qu'on devine malgré tout bravache, ils sont par contraste étonnamment réticents à l'installation de caméras connectées en permanence dans leur domicile :

> [>E4]: Après moi honnêtement je pense que ça ne me dérangerait pas qu'on m'écoute.
>
> [1:09:18] [>E3]: Moi ça me...
>
> [>E4]: Par contre qu'on me voit. [1:09:21] Ouais, je serais plus... moi, ça ça m'embêterait. Par contre, qu'on m'écoute... (entretien 1 ; 1 h 9 min 10 s)

E4 hiérarchise ici sans ambivalence aucune la gravité de la diffusion de captats audio ou vidéo de son espace domestique. Elle explicite assez peu cette différence, et singulièrement sa gêne particulière à être vue : l'argument de la « banalité » de leurs conversations vaut aussi pour l'essentiel de leurs actes visibles dans leur salon, où est déjà installé leur Echo Dot. Il y a donc bel et bien un point de blocage spécifique par rapport à la vue, qu'elle n'a pas (ou beaucoup moins) vis-à-vis de l'ouïe. Dans le cas d'E3, il est à préciser que cette réticence, qu'il partage,

tient sans doute également au fait qu'il rapporte avoir déjà lui-même piraté un réseau de vidéosurveillance. Il s'agissait de rendre service à son père, désapprouvant l'installation de caméras dans les locaux de l'entreprise qui l'employait, et qui avait demandé à son fils de lui indiquer à tout le moins ce qui était effectivement vu par ces caméras. Il ne s'est pas étendu sur la question, mais il a probablement eu recours à un moteur de recherche pour l'IoT comme Shodan, et il est probable également que le réseau de cette entreprise ait été très peu ou mal sécurisé. Les webcams déployées dans les derniers modèles d'enceinte connectées par des acteurs comme Google, Amazon ou Facebook sont probablement beaucoup plus difficiles à pirater à distance, mais les webcams de constructeurs tiers interfaçables avec le reste de la domotique domestique ne le sont pas nécessairement. En tout état de cause, cette expérience de première main explique sans doute sa faible confiance dans de tels dispositifs. Enfin, il est à signaler qu'ils sont également très précautionneux quant à la diffusion de l'image de leur petite fille, alors même qu'il s'agit d'un bébé au moment de l'entretien : s'ils mobilisent l'argument du consentement qu'elle ne peut pas encore exprimer, ils ajoutent également qu'il leur semblerait gênant pour elle que son image et plus particulièrement des photos nues soient disponibles en ligne, y compris dans ses premières années.

Même si la captation vidéo devait être essentiellement algorithmique ou chez des enquêtés qui n'éprouvent pas *a priori* de pudeur particulière relativement à leur phonotope domestique, il y a donc une gêne spécifique vis-à-vis de l'image. Cette gêne est cependant plus marquée encore lorsqu'il y a certitude de visualisation du flux vidéo par un œil humain, même d'un familier – et ce, y compris éventuellement pour celui qui regarde. L'exemple d'E16 est ici éclairant : la question de la surveillance vidéo de son domicile revêt un caractère particulier du fait de son handicap et de l'inquiétude de son père quant à sa sécurité physique. Pour autant, et bien que cette surveillance ait été perçue plutôt comme une supervision assez légitime par E16 lui-même, c'est son père qui a très rapidement choisi de renoncer aux caméras installées dans le salon :

> « JF: Oui, c'était peut-être plus au début, qu'il s'inquiétait ?
> E16: Voilà, il y avait ce côté un peu... Et puis une fois, deux fois, et ça l'a gêné plus lui.
> JF: Ah oui ?
> E16: Son, son ressenti de... voilà, je, je... de me regarder, c'était pas malsain, mais il y a un côté malsain, quand même, dans la vidéo, un côté un peu voyeur. Et puis si j'avais un souci, il savait que j'avais mon téléphone, j'appelais, le côté surveillance, c'était... c'était quelque chose qui l'a fait rigoler au début devant la caméra mais qui

> est devenu après un peu... un peu malsain, quoi. Enfin, malsain...» (entretien 10 ; 53 min 50 s)

C’est bien ici la vidéo comme medium de supervision qui a spécifiquement posé problème. Un peu plus tard dans cette séquence, E16 précise bien leur réticence partagée quant à la vidéo elle-même :

> « Du coup voilà, maintenant, ces caméras, c'est toujours un peu le problème de la vidéo, est-ce que c'est de la sécurité, est-ce que c'est du voyeurisme... C'est un peu gênant, ouais, je trouve, dans l'espace vraiment privé.
> JF: Tu trouves ça gênant par rapport aux soignants, où tu te dis que c'est pas agréable pour eux, ou par rapport à toi ? Parce que tu m'as pas dit si ça te gênait que ton père puisse te voir dans le salon, ou quoi que ce soit.
> E16: (inspire) Bah moi qu'il puisse regarder la caméra dans le salon dans la journée, ça me gêne pas. J'aimerais pas par contre qu'il y ait une caméra dans ma chambre, pendant qu'on me fait des soins, une toilette, que je suis tout nu... Même si je sais qu'il l'allumera jamais, imaginons qu'il ait mis ça, qu'il l'allumera jamais aux horaires où j'ai ce genre de soins, quoi. Mais ouais, avoir une caméra qui puisse potentiellement me surveiller, je trouverais ça particulièrement gênant, ouais.» (entretien 10 ; 55 min 18 s)

Le terme de « voyeurisme » est ici très fort, et directement employé par l’enquêté lui-même. Il mobilise la notion d’intimité, entendue dans l’un de ses sens les plus univoques, jusqu’à la nudité. La présence même d’une caméra dans la partie de la maison où il pourrait « [potentiellement] » être vu nu pendant ses soins est la limite minimale qu’il pose, quand bien même il aurait toute confiance en son père pour respecter cette intimité. Pour autant, il accepte très bien qu’une caméra soit présente dans le salon, un espace où sa nudité ne sera *a priori* pas exposée (« qu'il puisse regarder la caméra dans le salon dans la journée, ça me gêne pas »). C’est d’ailleurs cette option qu’ils ont un temps retenue, et son père a effectivement installé une caméra dans le salon. Dans cette configuration, c’est en fait son père qui a été le plus rapidement gêné par le dispositif au point de le retirer après quelques jours d’utilisation. Du côté d’E16, il y avait quand même une petite gêne, provenant plutôt du sentiment de surveillance active qu’il associait au bruit du moteur électrique de la caméra commandée à distance. Il n’était pas forcément gêné par la vidéo comme medium de surveillance en général, mais il l’était quelque peu par le bruit qui lui signalait cette surveillance, même bienveillante, en train de se faire. D’une certaine manière, ce bruit de moteur transformait le simple voyeur (compris comme « trou dissimulé dans une cloison qui permet d'assister, sans être vu » à une scène intime), acceptable dans cette configuration familiale, en un véritable surveillant, peut-être plus infantilisant et en tout cas plus intrusif. Le parallèle peut ici être fait avec la vidéosurveillance

dans l'espace public, généralement assez bien acceptée ou jugée peu gênante par la majorité en cela que, même en sachant qu'une caméra est présente dans la rue, ses opérateurs sont légitimes, et surtout que la caméra est le plus souvent trop en hauteur pour que les individus passant dans son champ de vision puissent savoir si un zoom est fait sur eux ou si la caméra les suit. Il est probable que, même dans un espace public, les passants auraient les mêmes réticences envers une caméra manifestement tournée vers eux, qu'ils la voient ou qu'ils l'entendent.

Un seul couple d'enquêtés utilise finalement systématiquement la vidéosurveillance de leur domicile, du moins quand ils quittent leur appartement. Il s'agit là d'un vrai voyeur, puisqu'une webcam est dissimulée dans un objet du mobilier. Au moment où ils me signalent cet usage lors de l'entretien, ils s'amusent même à me faire deviner où pourrait être ladite webcam, que je ne parviens pas, du reste, à trouver en détaillant visuellement la pièce de vie[519]. Il faut rappeler que ce couple d'enquêtés très équipés en domotique connectée présente la particularité d'avoir à la fois une grande confiance dans la sécurité de leurs installations et un faible degré de pudeur réciproque – déjà évoqué à travers le fait qu'ils partagent la géolocalisation de leur smartphone en continu. Ils constituent donc un cas rare, et même unique dans l'échantillon, mais qui pourrait être un signal faible de pratiques plus générales à l'avenir. Pour autant, même dans leur cas, E14 signale qu'il faudrait la couper quand ils ne sont « pas là » :

> « E14: Voilà. Faut que je la coupe, quand on rentre.
> E15: Quand on désactive l'alarme, ouais.
> JF: Parce que du coup, c'est pour...
> E14: C'est quand on n'est pas là.
> JF: Ouais.
> E14: Si jamais il y a un voleur. Comme il y a eu tellement, tellement, tellement de cambriolages ici.»
> (entretien 9, 10 min 40 s)

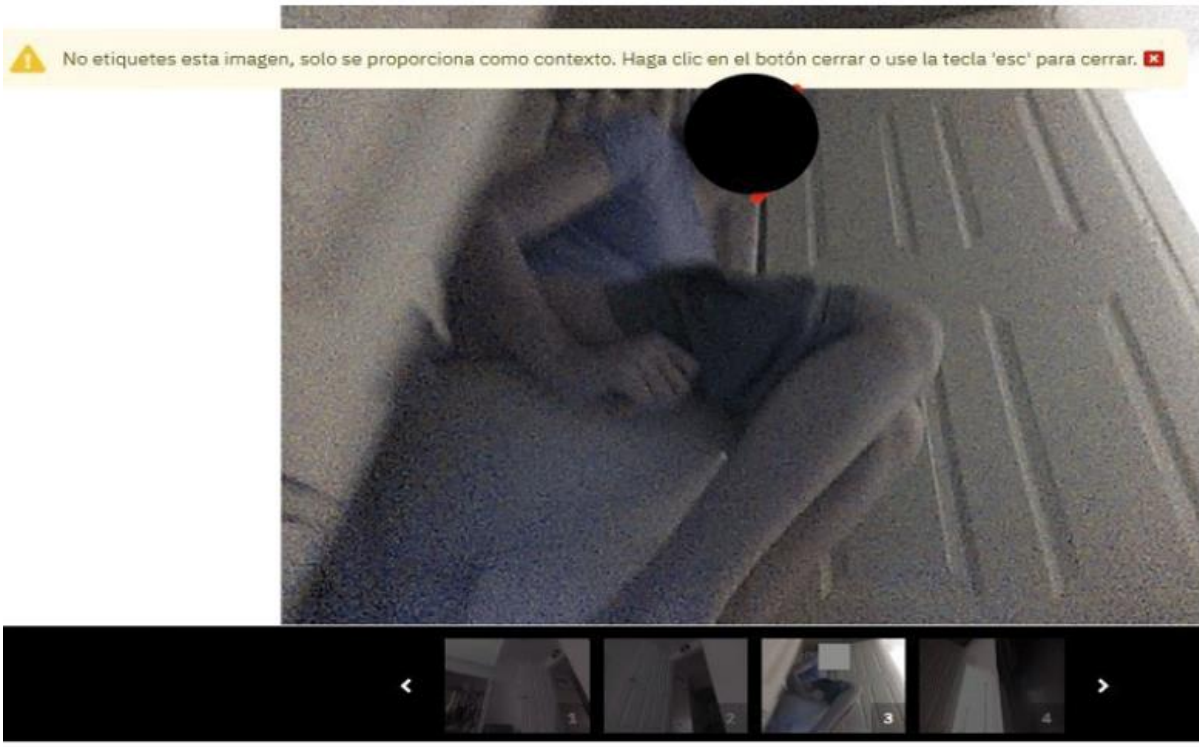
[519] « Ah si ! Caméra de surveillance, aussi.
JF: Ouais ?
E14: Il y en a une dans la pièce, là, si tu la trouves.
JF: (je cherche) Ca y est maintenant je suis en parano ! Où est-elle ! (rires)
E15: On l'oublie vite, hein !
[602,4] JF: Mais elle est visible ?
E14: (pause) Elle est... cachée dans...
E15: Elle est décorée ! (éclat de rire)
E14: Elle est décorée. Made in E15. (je continue de chercher) Ça va, c'est que tu ne l'as pas vue tout de suite.
JF: Je pense que je sèche. Là non, c'est un détecteur de... (mouvement) Dans le pot, là ?
E15: (rire)
E14: Non. Elle est là-bas, là.
E15: C'est le (élément de décoration) .
JF: Oh ! Ahhh... Habile, oui ! (ils rient d'un air entendu) Habile.» (entretien 9, 9 min 40 s)

Cette simple remarque révèle deux faits. D'abord, s'il faudrait qu'il la coupe, c'est qu'elle fonctionne par défaut en permanence après activation. Ce n'est pas une fatalité technique, semble-t-il : son compagnon ajoute d'ailleurs aussitôt qu'il faudrait corréler son activation à celle du système d'alarme, ce qui serait probablement un effort de configuration minimal pour ce couple d'enquêtés. Ce, à plus forte raison qu'ils disposent de cette caméra depuis plusieurs mois au moins : ils m'ont signalé que leur dernière acquisition domotique était leur HomePod, et la personne qui m'a mis en relation avec eux en vue de l'entretien me signalait déjà alors comme un fait marquant qu'ils disposaient d'une webcam dissimulée chez eux. E15 le dit lui-même un peu plus tard : « Bon, là ça filme en continu parce qu'on n'a pas bien configuré ça, mais... Il faudrait qu'on le fasse. » Ensuite, il semble nécessaire à E14 de préciser qu'il faudrait qu'il la coupe « quand on rentre ». La vidéosurveillance de leur domicile est donc conçue comme un moyen de veiller sur leur espace domestique depuis l'extérieur, thématique sur laquelle nous reviendrons plus loin (voir « Maîtriser son domicile depuis l'extérieur », p. 349), mais aussi qu'il ne leur semble pas souhaitable que leur paysage domestique soit monitoré en permanence, et en l'occurrence quand ils y sont. Cette revendication est plutôt celle de E15, et c'est E14 qui n'a pas encore fait la configuration – il faut cependant préciser que tous ont accès au flux vidéo. En tant que couple, ils présentent donc un cas intéressant : aucun des deux n'est fondamentalement gêné par cette captation vidéo en continu, y compris d'eux-mêmes, mais elle ne leur semble vraiment pertinente que lorsqu'ils ne sont pas là. Si ce n'est pas explicitement dit par E15, il se peut également qu'il soit agacé par le fait de ne pas avoir la maîtrise du flux vidéo. On peut faire l'hypothèse que le véritable cas-limite concernant la vidéo-surveillance n'est pas dans l'opposition binaire entre les moments de présence ou d'absence à deux du domicile (l'activation de la caméra n'est alors pas utile en cela que chacun peut directement voir de ses yeux ce que fait l'autre et ce qui se passe dans l'appartement), mais dans la situation où l'un seulement est présent, et que l'autre peut le regarder sans être vu lui-même. En somme, et même dans le cas de ce couple adhérant pleinement au principe de ces technologies surveillantes, et dans lequel il est tout à fait accepté que chacun dispose de « voyeurs » l'un sur l'autre, il subsiste *in fine* une gêne à ce que ce voyeur se fasse voyeuriste, autrement dit qu'il ne soit pas parfaitement réciproque (comme avec leurs géolocalisations qu'ils partagent mutuellement en gardant chacun le contrôle sur le paramètre) et donne à l'un une forme d'ascendant sur l'autre, si petite qu'elle soit.

Signalons enfin que la présence d'un voyeur humain derrière la machine, risque finalement peu craint par les utilisateurs d'appareils connectés, n'en reste pas moins possible.

Le lanceur d'alerte Edward Snowden a permis au grand public de s'apercevoir que des privilèges système élevés, même possédés par de rares individus, permettaient des fuites de données massives y compris pour une des plus puissantes agences de renseignement au Monde (voir « La prise de conscience de la surveillance de masse : de la publicité ciblée aux révélations Snowden », p. 295). L'accès aux données des utilisateurs de dispositifs connectés est elle aussi beaucoup plus triviale qu'on pourrait le penser pour les employés et sous-traitants des fabricants d'objets connectés, comme nous l'avons vu en ce qui concerne l'entraînement des modèles d'intelligence artificielle pour la reconnaissance vocale (voir « La transmission prévue de captats audio au fabricant », p. 274). Un scandale récent a jeté une lumière crue sur cet accès à des images domestiques voire intimes des employés et sous-traitants des fabricants d'objets connectés équipés de caméras. Dans un article fouillé du magazine *MIT Technological Review*, la journaliste Eileen Guo explique ainsi comment des photographies annotées d'intérieur vues du sol ont été diffusées *via* Facebook, montrant tantôt un chien, tantôt un garçon de huit ou neuf ans allongé sur le ventre et fixant l'objectif, et le plus souvent des éléments de mobilier comme une télévision ou une applique lumineuse[520]. Prises par des aspirateurs-robots de marque Roomba, ces photographies auraient été diffusées en cercle fermé par des travailleurs du clic chargés de les annoter, avant d'être diffusées de façon virale sur Facebook puis dans la presse. Il est à préciser que la branche d'Amazon produisant ces aspirateurs affirme que ces images proviennent de modèles de développement dont les utilisateurs étaient volontaires et conscients de ce type de captations, et non de modèles commerciaux présentés comme plus sécurisés. Le cas reste très intéressant en cela que sur la quinzaine d'images diffusées, c'est celle d'une femme assise sur la cuvette de toilettes faiblement éclairées qui a été la plus reprise, notamment dans la presse (voir Photographie 14).

[520] E. GUO, « A Roomba recorded a woman on the toilet. How did screenshots end up on Facebook? », *MIT Technology Review*, 19 décembre 2022 (en ligne : https://www.technologyreview.com/2022/12/19/1065306/roomba-irobot-robot-vacuums-artificial-intelligence-training-data-privacy/ ; consulté le 20 décembre 2022)



Photographie 14 – Image tirée d'une fuite de données d'aspirateurs Roomba (source : MIT Technological Review, 2022)

Même en retenant la défense de l'entreprise selon laquelle un modèle commercial classique n'aurait pas rendu cette situation possible, le cas est des plus révélateurs.

D'une part, il permet de considérer que les personnes dont l'intérieur a été photographié et montré sur Internet sont victimes d'une atteinte à leur vie privée autant que l'entreprise iRobot est victime d'une infraction de leur secret industriel. Les conséquences sont bien sûr différentes pour des individus ou une entreprise, mais toutes deux sont ici victimes de cette malveillance, et ce n'est qu'indirectement que le fabricant est responsable. Si l'on reprend la terminologie de Nissenbaum (voir p. 69) décrivant les contextes de problèmes de vie privée à travers les notions de « rôles », d'« activités », de « normes » et de « finalités », iRobot a opéré logiquement envers ses testeurs (rôle assumé et rémunéré) avec une finalité de captation claire (la recherche et développement) et encadrée par une norme (contractuelle et de design, avec de gros autocollants verts indiquant « Prise de vidéo en cours » sur les appareils concernés). iRobot n'a pas dérogé à l'intégrité contextuelle de la captation de données chez les testeurs, mais a été elle-même victime d'une atteinte à son secret industriel qui a mené à un « *privacy problem* » d'ordre plutôt juridique. Si l'on reprend donc cette fois la taxonomie du juriste Daniel Solove (voir Tableau 2, p. 63), les testeurs ont été victimes, à travers l'utilisation frauduleuse de données intimes légitimement collectées par iRobot, d'une dissémination d'information

(« *information dissemination* ») et plus précisément d'une rupture de confidentialité doublée d'une diffusion non sollicité (« *breach of confidentiality* » et « *disclosure* »).

D'autre part, et une fois cette situation précisément définie du point de vue de l'atteinte à la vie privée dont elle est porteuse, il est tout aussi intéressant de s'attarder sur la manière dont elle a été perçue qu'au déroulement même de l'événement. Le fait le plus saillant est que l'image la plus partagée sur la quinzaine de photographies diffusées est celle de la femme dans ses toilettes. Plus que l'image d'un intérieur, du chien de la famille ou même d'un enfant, elle est en quelque sorte le pire de ce que la plupart des individus craignent de voir diffuser d'eux-mêmes par des objets connectés. Il s'agit tout à la fois d'une image d'intimité, de relative nudité, et d'une fonction corporelle peu valorisante, le tout visage visible. L'image a en outre les caractéristiques d'une photographie réaliste, prise sur le vif dans de mauvaises conditions de visibilité dont témoigne le grain de l'image et la désaturation des couleurs, mais avec un cadrage largement suffisant pour identifier la personne. Seule peut-être une image d'ébat sexuels aurait pu la supplanter. En somme cette image est exceptionnelle en cela qu'elle est le paroxysme pris en conditions réelles, sans détournement du logiciel ou du matériel (quoique dans un cadre de recherche et développement) et effectivement diffusé à large échelle de ce que les individus craignent de leurs objets connectés.

III - LA CAPTATION DE MOUVEMENT

Dans l'ordre de l'observation, voire de la surveillance de l'espace physique, la vue et l'ouïe, dans cet ordre, sont sans conteste les sens qui reviennent le plus souvent comme étant les plus efficaces. Il en va de même quand ces sens sont délégués à des machines opérant ces captations vidéo et audio. On a vu que tous les enquêtés étaient plus sensibles à la captation de leur image que des sons qu'ils produisaient. Pour ce qui est de l'observation du monde physique, l'imaginaire de l'espionnage est d'abord celui de la caméra-espion ou de la vidéo-espion, comme l'illustre la belle affiche du film *La vie des autres* de Florian Henckel von Donnersmarck sorti en 2006, dans laquelle un espion de la Stasi regarde et écoute dans l'ombre l'appartement du couple d'intellectuels est-allemands contestataires à la surveillance duquel il est affecté (voir Figure 28).

Figure 28 - Affiche du film La vie des autres (Florian Henckel von Donnersmarck, 2006)

Une raison pratique évidente de ce primat de la vue et de l'ouïe pour la surveillance est qu'il s'agit des deux sens de la distance, par lesquels on peut acquérir des sensations nous informant sur un objet même assez lointain, et avec un engagement minimal du corps – voire un engagement nul pour l'ouïe, qui ne requiert pas même d'exposer son oreille, contrairement à l'œil qui doit être en ligne directe avec cet objet. En comparaison, l'odorat, le toucher et surtout le goût, semblent d'une efficacité très inférieure pour l'espion en cela qu'ils réclament une certaine proximité, sinon un contact, pour opérer – en plus d'être assez peu informatifs du fait de leur faible développement chez l'être humain.

De fait, la question de ces autres modalités sensitives de possible surveillance n'a pas été abordée par les enquêtés, qui ne sont pas non plus les axes de développement les plus importants pour les industriels du logis connecté. Ces derniers se concentrent avant tout sur les captations audio et vidéo, cette fois dans l'ordre inverse, probablement pour tenir compte de la

plus grande méfiance bien comprise des utilisateurs pour la diffusion de leur image[521]. Il n'en existe pas moins un courant de recherche et développement consacré à la captation du mouvement des individus, embryonnaire aux débuts de cette recherche, mais qui semble de plus en plus significatif.

La première utilisation triviale, ancienne et bien connue, en est la captation de mouvement qui permet par exemple l'activation d'une lumière ou d'une caméra de surveillance en cas de mouvement dans une pièce ou un jardin. Mais les développements récents vont plus loin que cette fonction, au fond, de simple interrupteur, pour permettre de produire des données relatives à un individu. Kröger *et al.* ont par exemple consacré un court papier aux usages possibles de l'accéléromètre pour obtenir des informations sur les individus, accéléromètre qui constitue selon eux un risque très sous-évalué dans la réflexion sur la protection de la vie privée[522]. Aujourd'hui présents dans la vaste majorité des smartphones et des montres connectées, les accéléromètres permettent ainsi de mesurer ou d'inférer l'activité physique des personnes, le poids d'une charge portée dans les bras, le style de conduite, la géolocalisation (en complément du GPS, par exemple pour continuer à suivre les déplacements d'une personne à l'entrée d'un lieu souterrain), le style de conduite automobile, l'âge, ou encore les émotions et la personnalité plus généralement[523].

Dans l'espace domestique, une application récurrente de ce type de captations fondées ni sur le son, ni sur l'image concerne la mesure du sommeil et plus largement l'espace de la chambre. Il peut s'agir d'une surveillance assez basique, comme celle qui a été projetée très brièvement dans la literie d'une résidence du CROUS de Nantes afin de mesurer l'usure de lits amovibles dits « connectés », à l'initiative de l'entreprise Espace Loggia[524]. Trois capteurs avaient été installés pour mesurer « l'usure des câbles, l'état des fixations murales et la présence

[521] C'est du moins l'hypothèse de Joseph Turow dans The Voice Catchers, qui écrit : « *Marketers have approached voice as exploitable part of the human body that doesn't have the negative associations of facial recognition. This relatively blank slate, they believe, offers an opportunity to cultivate trust. Yet the voice profiling activities that already happen every day raise many ethical issues*. » J. TUROW, The Voice Catchers: How Marketers Listen In to Exploit Your Feelings, Your Privacy, and Your Wallet, New Haven, Yale University Press, 2021, p. 8

[522] *« accelerometers are less well-understood in terms of their privacy implications, and also much less protected [6, 7]. Even scholarly literature has largely ignored potential issues in this field, with researchers describing accelerometer data as "not particularly sensitive" [8] or even "privacy preserving" [9]* » *in* J. L. KRÖGER, P. RASCHKE et T. R. BHUIYAN, « Privacy implications of accelerometer data: a review of possible inferences », dans *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy - ICCSP '19*, Kuala Lumpur (Malaisie), ACM Press, 2019, p. 81 (en ligne : http://dl.acm.org/citation.cfm?doid=3309074.3309076 ; consulté le 22 mai 2021)

[523] J. L. KRÖGER, P. RASCHKE et T. R. BHUIYAN, « Privacy implications of accelerometer data », *op. cit.*

[524] C. PAISTEL, « Étudiants à Rennes. Dormez, vous êtes surveillés... », *Ouest-France*, 6 septembre 2017 (en ligne : https://www.ouest-france.fr/bretagne/rennes-35000/etudiants-rennes-dormez-vous-etes-surveilles-5227294)

de parties déformées »[525]. Face au tollé provoqué par certains étudiants et relayé dans le quotidien local *Ouest-France*, les lits ont finalement été retirés. Ce projet a été d'autant plus décrié qu'il concernait le lit, meuble intime par excellence et micro-lieu symbolique du relâchement, du repos et de la sexualité, et qu'il concernait une population plus ou moins captive d'étudiants en résidence universitaire – donc hors d'une logique d'*opt-in*.

La mesure du sommeil en elle-même est plus récente. Testée au cours d'un projet de recherche dans la Aware Home, c'est finalement Google qui en a proposé la première application industrielle à travers les capteurs Soli, à savoir un radar miniature à même de mesurer les mouvements à proche distance pour en inférer des données sur la durée ou la qualité du sommeil de l'utilisateur, à plus forte raison en association avec une enceinte connectée – qui peut, en complément, enregistrer les phases de ronflement, par exemple. La recherche et développement d'Amazon a rapidement suivi le coche avec l'autorisation des autorités étatsuniennes[526]. Son produit n'est en revanche pas encore disponible.

En somme, quoique ces dispositifs soient encore assez confidentiels, il reste intéressant de mentionner que des pistes alternatives à la captation audio ou vidéo au sens strict sont explorées aujourd'hui par les fabricants. On peut faire l'hypothèse que l'utilisation d'un radar plutôt que d'une webcam pour des usages de ce type pourrait même, à l'avenir, être convoqué comme un argument de défense de la vie privée : il est plus aisé de proposer à l'utilisateur de mesurer ses mouvements nocturnes ou autres à travers un nuage de points non-texturé obtenus par un radar plutôt que par l'analyse d'images vidéo nettement plus identifiables et identifiantes. Une première confirmation de cette hypothèse se retrouve déjà dans la communication de Google autour de ses micro-radars Soli (voir Figure 29), dont le quatrième item indique clairement que le fait que Soli ne soit pas un appareil photographique le rend plus « privé » (« *private* »).

[525] « Big Brother dans des lits connectés d'étudiants ? La réponse du concepteur, le retrait du Crous », s. d. (en ligne : https://www.nextinpact.com/article/27165/105122-big-brother-dans-lits-connectes-detudiants-la-reponse-concepteur-retrait-crous ; consulté le 17 août 2022)

[526] D. LAZARUS, « Column: Amazon wants to use radar so Alexa can watch as you sleep », *Los Angeles Times*, 16 juillet 2021 (en ligne : https://www.latimes.com/business/story/2021-07-16/column-amazon-radar-sleep ; consulté le 4 octobre 2021)

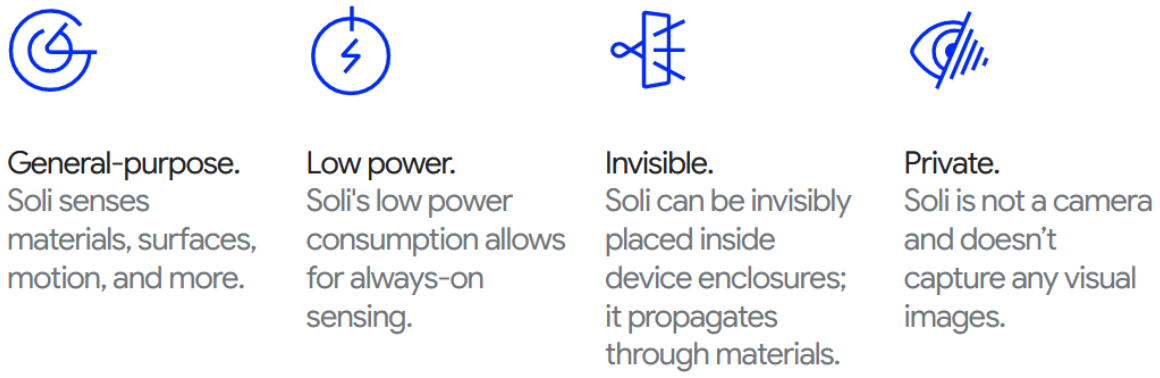


Figure 29 - Les quatre intérêts industriels de ses mini-radars Soli selon Google (source : https://atap.google.com/soli/, 2022)

IV - L'ESPIONNAGE, DU DELIRE PARANOÏAQUE AU FATALISME

En toile de fond de l'émergence des enceintes et objets connectés, on a vu que la plupart des enquêtés manifestent une approche fataliste face à cette nouvelle forme de progrès technique : il est souvent jugé inévitable, et dès lors à accompagner bon an, mal an. Rencontrée dans une FNAC à côté du rayon des enceintes connectées où elle flânait sans avoir nécessairement la volonté d'en acquérir une, E10 me déclare par exemple :

> « E10: Je suis une personne déjà... bien... bien dans mon coin, je suis pas extravagante, je suis bien... (geste de la main pour dire "posée, tranquille", cela m'arrache un petit rire) S'il fallait que je me cache pour (incompréhensible), je me cacherais. C'est vraiment... c'est tout... je sais pas. Après de toute façon au bout d'un moment on sera obligés, parce que c'est l'évolution, c'est ça. » (entretien 6, 30 s)

Ni spécialement technophile, ni pour autant technophobe, elle résume bien l'idée que « l'évolution » technique vers plus de traçage ou de collecte numérique des pratiques quotidiennes lui semble être incontournable. Elle se cachera si besoin, mais son attitude est emblématique d'un fatalisme qui se retrouve peu ou prou chez tous les enquêtés, y compris chez les plus technophiles.

La prise de conscience de la surveillance de masse : de la publicité ciblée aux révélations Snowden

La prise de conscience globale relativement à la surveillance de masse est la grande nouveauté de l'époque par rapport aux précédents travaux d'importance sur la vie privée menés

par Rey, Nissenbaum ou Solove. Si les discours des activistes de la vie privée pouvaient facilement passer pour excessifs ou paranoïaques jusqu'au début des années 2010, les révélations d'Edward Snowden en 2013, peu avant le début de ce travail de doctorat, ont complètement changé la donne.

Snowden est un ancien administrateur système qui a fait carrière comme agent de la National Security Agency (NSA) des États-Unis puis comme consultant dans des entreprises-écran de la Central Intelligence Agency (CIA). Issu d'une famille de militaires et de fonctionnaires de l'État américain depuis plusieurs générations, il s'engage au tournant des années 2000, peu après les attentats du 11 septembre à New York. Cet évènement exceptionnel a précipité l'émergence de nouveaux outils de contrôle anti-terroristes d'une portée encore inconnue dans le secteur public, y compris pour les puissantes agences de renseignement des États-Unis. Dans cette époque particulière, des profils comme celui de Snowden ont pu émerger à grande vitesse pour construire ces outils. Dans sa dernière affectation à Hawaï, à seulement 29 ans, Snowden raconte avoir « enfin été dans la position de voir tout l'effet de [son] travail en un coup d'œil, assemblée comme les mécanismes d'une immense machine formant un système de surveillance de masse à l'échelle mondiale. » Au fond d'un bunker creusé sous un champ d'ananas lors de la Deuxième guerre mondiale, il raconte : « j'étais assis devant un terminal depuis lequel j'avais un accès pratiquement illimité aux communications de presque n'importe quel homme, femme ou enfant sur Terre qui aurait un jour passé un coup de fil ou touché un ordinateur. »[527]

Après avoir fait la révélation aux journalistes Laura Poitras et Edward Greenwald de l'ampleur de ce système de surveillance en « complète contradiction avec la constitution des États-Unis mais aussi avec les principes élémentaires de n'importe quelle société libre »[527], Snowden a pris la fuite à travers le monde avant d'obtenir l'asile en Russie en 2013 et d'en devenir un résident permanent en 2020. Ces révélations, richement documentées et explicitées par l'un des techniciens les plus en pointe sur ces programmes de renseignement comme X-Key Score ou Prism, ont eu un retentissement mondial. Tous les enquêtés avec lesquels le nom d'Edward Snowden a été évoqué connaissaient au moins son nom. E5 est celui qui connait le mieux l'affaire. Il a lu l'autobiographie du lanceur d'alerte, *Permanent Record*, et il avait eu une forme d'épiphanie avant cela en voyant une interview de l'homme :

> « E5: La nouvelle en soi, au début, c'était les données téléphoniques. C'est ça le premier article qui est sorti sur Snowden. (il imite un ton désabusé:) "Ouais, mais

[527] Trad. pers. E. J. SNOWDEN, *Permanent record*, *op. cit.*, p. 3

on le sait, des trucs comme ça". Ce que je me suis dit. Mais c'est quand je suis tombé sur les vidéos que ça a fait écho, oui, à.… j'étais absolument... conscient... j'étais complètement en phase avec tout le message, c'est ça.
JF: (acquiesce) Une épiphanie, quoi?
E5: Parce que l'enjeu n'est pas technique.
JF: (acquiesce)
E5: L'enjeu est de société. Ce que je dis quand je parle de... pourquoi je suis dans Franciliens.net, à faire un fournisseur d'accès à Internet, bénévole, alors qu'on a des choses à côté pour gagner de quoi manger le soir, heu... C'est que nous croyons qu'Internet n'est pas un fait technique. Internet est un fait social. Internet construit les citoyens que nous sommes. Internet modifie les rapports, les échanges, les communications... Et Internet construit, donc, la société. C'est vrai pour Internet, et le numérique. Ce qui a fait écho en moi c'est la question de la société qu'on construit. C'est ça qui est la question fondamentale posée par Snowden. » (entretien 2, 2 h 35 s)

Lui-même informaticien et connaisseur des enjeux liés au numérique, il commence par estimer « on le sait, des trucs comme ça » à propos de la surveillance des données téléphoniques. Mais en continuant de creuser l'affaire, il prend conscience de l'ampleur du système de surveillance du renseignement étatsunien, et la figure de Snowden devient un catalyseur de sa propre action militante à propos d'Internet.

E5 est bien sûr un cas assez exceptionnel dans le panel. La réaction de E17 à ma question de savoir s'il connaît Edward Snowden est sans doute plus emblématique de l'attitude fataliste courante :

« E21: Oui. Oui. C'est, heu... Alors... heu... (longue hésitation) Les services de renseignement ou autre, américains, surveillaient.. enfin, avaient accès aux données, ils prélevaient des données et... bon. C'est comme je dis, je... Je suis à la fois effrayé, et je m'en moque. Je sais pas comment on peut dire ça, c'est-à-dire que je me dis que je suis impuissant. Je sais vers où on va, finalement ça ne me surprenait pas. » (entretien 11, 1 h 46 min)

Il connaît les grandes lignes de l'affaire, et il en est à la fois « effrayé » et indifférent. Le sentiment qui prévaut chez lui est « l'[impuissance] » face à des moyens techniques qu'il sait démesurés.

Ainsi, quoique les révélations de Snowden n'aient pas forcément entraîné de profonds changements dans les pratiques numériques de tout un chacun ni bien sûr un engagement aussi fort que chez E5, il est patent que 2013 est une année charnière dans la prise de conscience générale sur les moyens de surveillance déployés par les États, et qu'elle a départi la thématique

de la défense de la vie privée numérique de son image de lubie d'informaticiens paranoïaques pour devenir un sujet tout à fait consensuel.

« N'avoir rien à cacher » : criminalité et surveillance

Il n'en reste pas moins qu'un principe de désinvolture déjà bien identifié avant les révélations Snowden continue d'être exprimé par un certain nombre d'enquêtés, qui peut se résumer à l'expression « je n'ai rien à cacher ». Solove lui-même y a consacré un ouvrage entier, *Nothing to hide*[528], et l'expression est devenu un trope rhétorique parmi les activistes cherchant à convaincre leurs contemporains d'adopter des mesures de protection de leur vie privée numérique.

Le fond de l'argument des personnes qui déclarent n'avoir rien à cacher est que seuls des criminels auraient à craindre la surveillance policière ou les services de renseignement. Il n'y aurait pas lieu pour des individus banals et sans histoire de craindre pour leurs communications ou leurs pratiques numériques générales. E6 et E7 développent ce discours rassurant à l'évocation de la possibilité de suivre les mouvements d'un individu, ici grâce à son passe de transports en commun :

> « E7 : Sauf si tu étais un individu recherché ! (…)
> E6: Oui, c'est aussi parce qu'on est des gens... qui n'ont pas de problème, quoi. Ça joue ! (sourit)
> JF: (acquiesce)
> E6: Je pense que si on était des criminels, on aurait plus de problèmes avec ça. » (entretien 3, 36 min 40 s)

L'idée est clairement exprimée : il n'y a rien à craindre d'un tel suivi pour qui n'est pas un « individu recherché » ou un « criminel ». Le dessinateur du *New Yorker* Pat Byrnes reprend cette idée dans une caricature présentant justement des criminels se méfiant des appareils électroménagers dans une cuisine (voir Figure 30, ci-dessous) :

[528] D. J. SOLOVE, *« I've Got Nothing to Hide » and Other Misunderstandings of Privacy*, *op. cit.*

Figure 30 - Caricature "Faites attention à ce que vous dites. L'électroménager a des oreilles" (auteur : Pat Byrnes, 20/VIII/2019)

Cette idée est plaisamment présentée à travers des personnages d’allure patibulaire, mal rasés, aux lunettes noires, cigare ou cigarette à la bouche, dont deux sont assis à une table de cuisine devant une montagne de billets de banque tout en jouant aux cartes. Cette ambiance de tripot clandestin sur la partie en bas à droite de l’image contraste nettement avec le reste du décor, qui est celui d’une cuisine occidentale proprette équipée de divers appareils ménagers métallisés et munis d’écrans. Ce contraste fonde le ressort comique de l’image, que vient appuyer la tirade du personnage sur la droite : « Faites attention à ce que vous dites. L'électroménager a des oreilles ». Derrière leur apparente banalité, les appareils sont en effet présentés comme des mouchards potentiels pour ces personnages visiblement impliqués dans des activités illégales. La tirade est, en outre, une variation sur l’expression commune « les murs ont des oreilles », qui enjoint habituellement à la méfiance moins envers les murs qu’envers d’éventuelles personnes dissimulées ou proches d’interlocuteurs désirant rester discrets. Si l’évolution de la

domotique connectée devait mener à l'intégration des microphones nécessaires aux assistants vocaux dans le bâti des espaces domestiques, il se pourrait à terme que l'expression « les murs ont des oreilles » finisse par devoir être prise au premier degré. Je fais néanmoins l'hypothèse que cette évolution possible reste encore assez improbable et qu'elle ne devrait pas se généraliser dans un futur proche (voir « Converser avec un objet », p. 392).

En poussant la logique du « rien à cacher », les possibilités offertes par l'IoT pour la surveillance policière semblent même désirables à certains enquêtés qui y voient la possibilité de renforcer leur sécurité. À mon grand étonnement, ce discours a même parfois été repris à la suite de la question du guide d'entretien portant sur les lunettes de reconnaissance faciale développées pour la police chinoise. Si E3 manifeste la réticence que j'attendais face à cet exemple généralement présenté comme liberticide et propre à un régime autoritaire, E4 est littéralement enthousiasmée par les possibilités de repérage de criminels :

> [>JF]: (…) C'est sur la question justement de ce qui est fait actuellement mais en plus poussé par la police chinoise. Je sais pas si vous avez vu que certaines unités de police chinoises avaient maintenant des caméras de reconnaissance faciale. Je ne sais pas s'ils les mettent dans des lunettes type Google Glasses, ou si c'est une caméra... Enfin, en tout cas, la reconnaissance faciale, dans la rue, ils savent si telle personne est suspectée de tel truc.
>
> [2:15:06] [>E4]: C'est bien, ça ! (l'air vraiment étonnée et enthousiaste)
>
> [>JF]: C'est-à-dire qu'on te croise, le problème étant que...
>
> [2:15:10] [>E3]: (indiscernable) ... tout, quoi.[2:15:12]
>
> [>JF]: ...ils savent qui est où, etc. Enfin, le problème, ou pas.
>
> [>E4]: Ben c'est bien, ça.[2:15:14] Franchement, si ça peut permettre d'arrêter des gens, c'est bien (elle rit) .
>
> [2:15:18] [>E3]: Il me semble qu'il y avait quelques travers...
>
> [2:15:20] [>E4]: Il y en a toujours, de toute façon.[2:15:23] (entretien 1, 2 h 15 min)

De fait, E4 avait manifesté son vif souci de la sécurité dans l'espace public quelques minutes auparavant :

> [>E4]: Sinon on ne sortirait plus de chez nous (je ris nerveusement) , enfin moi je ne sortirais plus de chez moi.[2:13:24] Heu... Surtout depuis qu'on a notre petite fille. Et c'est vrai que... ben... je pense que quelque part, d'être surveillés ça peut être un gage de sécurité supplémentaire (j'acquiesce) Après... voilà. Je pense que quand on nous surveille dans la rue c'est pas pour nous spammer ou à des fins

commerciales (en riant)
(entretien 1, 2 h 13 min 20 s)

Si ce discours sécuritaire est en soi assez classique, l'enthousiasme de E4 reste étonnant. Elle finit par admettre une véritable obsession, manifestée par les nombreuses allusions qu'elle aura fait aux attentats de Paris en 2015 à plusieurs moments de l'entretien :

> [2:16:50] [>E4]: Ben en fait moi le truc c'est...[2:16:52] enfin…[2:16:55] j'ai une obsession pour la sécurité, ces derniers temps.[2:16:55] C'est devenu un peu mon obsession du moment, donc je me dis que si c'est utilisé à des fins... pour arrêter des personnes recherchées et...[2:17:06] ça peut être... pour moi c'est un moyen supplémentaire en fait de. Parce qu'on a du mal à les avoir ces gens-là finalement. Parfois c'est des gens qui sont recherchés pendant des années.
> (entretien 1, 2 h 16 min 50 s)

Certains enquêtés n'en restent pas moins critiques face à la généralisation de la surveillance, et manifestent plutôt un sentiment de gêne diffus. La force de l'argumentaire du « rien à cacher » rend en effet difficile pour beaucoup d'enquêtés n'ayant eux non plus rien à cacher d'expliquer en quoi cette surveillance les affecterait. On le voit ici chez E2 :

> « E002: Qui te pousse à encore plus de vigilance, et qui instaure un climat de peur, plutôt que d'essayer de, de, de... d'exterminer le problème de fond, tu vois. De criminalité, ou tu vois qui passe par plus d'éducation, de moyens dans les hôpitaux, les écoles, tout ça. Je trouve que c'est pas un bon investissement, en fait. Je trouve que le côté sécuritaire se résout pas par plus de vigilance, par plus... d'intrusion ?
> JF: (acquiesce)
> E002: Ca va pas résoudre le problème, de la sécurité, tu vois, qu'il y ait moins de violences, de vols, ou de disparitions. De viols. C'est pas en surveillant les gens que ça va baisser. Ca va permettre de retrouver peut-être plus de criminels, mais ça va pas enrayer la criminalité. »
> (entretien 02, 1 h 21 min 50 s)

Face à l'évidence apparente de chercher à faciliter le travail légitime d'appréhension de criminels, elle cherche ses mots pour définir ce qui la gênerait dans le fait d'être surveillée, avant de proposer de manière hésitante sa réticence envers une « intrusion ». Elle évoque également un « climat » de peur et de vigilance que produiraient ces pratiques. Il lui faut plus de temps pour finir par trouver une formule qui traduit une pensée plus construite (« Ca va permettre de retrouver peut-être plus de criminels, mais ça va pas enrayer la criminalité ») qui la ramène à l'opposition classique dans les débats sécuritaires entre la répression et la prévention de la criminalité.

Certains enquêtés poussent cet argumentaire plutôt vers la question politique des effets potentiellement délétères de la restriction des libertés et du renforcement des pouvoirs de la police :

> « Plus ça va, moins on a de libertés. Tu crois que t'es libre, mais en fait, t'es, t'es comme un mouton, bien cloisonné. Et ça, ça me gêne un peu. Après, si ça a une utilité pour retrouver des gens... Pffff... J'ai jamais réfléchi à la question. Je pense que ça me gêne un peu, en fait. De (incompréhensible) surveillé, partout. (petite pause) S'ils le justifient par des... des, des... problèmes de criminalité, des choses comme ça, ça me gêne, mais bon, je me ferais à cette idée que c'est nécessaire.
> JF: Et du coup, la gêne, elle tient à quoi ? Genre, une espèce de pudeur, de crainte par rapport à une mauvaise utilisation de ces informations...? C'est quoi qui te gêne.
> E16: C'est plus une réutilisation, je sais pas, moi... Manif pour les je-sais-pas-quoi, bah les gens vont être fichés. "Vous appartenez à tel type d'association, tel type de truc..." »
> (entretien 10, 2 h 37 min)

Là aussi, E16 peine à exprimer d'abord autre chose qu'un sentiment spontané d'aversion à la surveillance, et souscrit même à l'idée qu'il soit utile d'appréhender des criminels (« S'ils le justifient par des... des, des... problèmes de criminalité, des choses comme ça, ça me gêne, mais bon, je me ferais à cette idée que c'est nécessaire. »). La crainte que les technologies de surveillance présentées comme des moyens de lutte contre la criminalité puissent être utilisées dans un second temps contre des groupes politiques ou des mouvements contestataires est bien représentée dans l'échantillon. Outre E16, elle est également exprimée par E2, E17, E20 et E5. De fait, il est avéré en France que l'extension de la notion de « terrorisme » censée limiter le champ d'application de la loi Renseignement de 2015, qui prévoit des mesures extraordinaires de restriction des libertés individuelles, a fini par s'appliquer également à des militants écologistes, à des manifestants ou à des supporters de football[529]. Quoi qu'il en soit, beaucoup d'enquêtés n'en restent pas moins suffisamment confiants dans la régulation des pouvoirs de police dans un contexte démocratique pour ne pas juger alarmante ou problématique cet ensemble de possibilités techniques et judiciaires, comme E3 et E4, ou E15 et E17 (voir

[529] Comme l'explique l'avocat Arié Halimi dans une interview pour *Libération* : « C'est par exemple ce qui s'est produit peu de temps après les attentats du 13 Novembre, avec les interdictions des manifestations à l'occasion de la COP 21 à Paris. Ce fut aussi le cas avec le bannissement de certaines personnes des cortèges anti-loi travail, ou encore des interdictions de déplacement de supporteurs de football. Le texte de transposition fixe la limite d'une application aux actes terroristes mais c'est une notion malléable. » *in* E. FANSTEN, « Etat d'urgence : « Une inscription dans le droit commun qui annule toute contestation » », *Libération*, 9 juin 2017 (en ligne : https://www.liberation.fr/france/2017/06/09/etat-d-urgence-une-inscription-dans-le-droit-commun-qui-annule-toute-contestation_1575516/ ; consulté le 2 janvier 2023)

aussi « Les différences perçues entre les différents acteurs publics et privés de la collecte de données », p. 215).

*

Les réactions fortes contre les enceintes connectées montrent que le fait qu'il s'agisse autant de microphones que d'enceintes connectées a été bien compris du grand public. L'imagerie de l'espionnage est volontiers convoquée contre ce qui est parfois perçu comme un mouchard, y compris par des utilisateurs ou propriétaires d'enceintes connectées. Pour autant, le fait que cette réaction ait été très répandue parmi les enquêtés et très relayée dans la presse ne doit pas nous mener à surestimer cette attitude de défiance. Le simple succès commercial de ces dispositifs indique qu'une large part de la population, même avec des réticences initiales, est tout à fait susceptible d'adhérer finalement à ces nouveaux usages et aux dispositifs associés. Il ne s'agit cependant pas d'une nouvelle itération du *privacy paradox* dans lequel des consommateurs prétendraient valoriser leur vie privée pour aussitôt s'équiper du dernier dispositif connecté en vogue au détriment de leurs intérêts et principes affichés. Pour le comprendre, il faut désormais voir comment ces objets s'insèrent dans l'espace technique et social du logis contemporain.

Chapitre 2 - LE HUB DOMOTIQUE

« L'attrait de tout cela est facile à comprendre. Qui ne voudrait pas d'une technologie permettant d'arrondir les angles de la vie moderne, d'intervenir de façon subtile, au besoin, pour nous guider lorsque nous sommes perdus, et nous rappeler les choses que nous avons oubliées ? Qui objecterait face à une technologie qui nous épargne la collection d'ordinateurs et autres appareils numériques qui nous entourent, tout en faisant – mieux – ce qu'ils font déjà ? »[530]

Dans une époque où tout un chacun dispose de smartphones qui sont autant d'ordinateurs compacts, individuels, performants, bardés de capteurs et de fonctions de communication les rendant utilisables en tout lieu et interfaçables avec tous les autres objets dits connectés, le tout en s'affranchissant d'un fil d'alimentation grâce à des batteries à la durée de vie de plus en plus conséquente, il peut sembler étonnant que l'un des marchés de technologie grand public les plus dynamiques soit porté par des ordinateurs à nouveau fixes, à l'alimentation filaire, partagés entre les membres du foyer, et pourvus exclusivement d'une interface humain-machine, la voix, qui en limite drastiquement les potentialités techniques et créatives.

En réalité, c'est précisément cette fixité et ces limitations qui font tout l'intérêt des enceintes connectées. L'enceinte connectée ne vise pas à augmenter l'espace du logis de fonctions inédites, ni à libérer ses habitants de l'ancrage spatial du domicile – autant d'objectifs déjà atteints par le smartphone et, dans une moindre mesure, par l'ordinateur personnel portable. La fonction primordiale de l'enceinte connectée est d'agir comme un centre du logis connecté, un *hub* pour l'IoT domotique. Pour reprendre les termes d'Adam Greenfeld en exergue de cette partie, son rôle est « d'arrondir les angles de la vie moderne », de nous éviter de nous « [perdre] » dans l'écosystème de machines et de logiciels dont nous sommes de plus en plus équipés. Elle ne nous épargne cependant pas tant « la collection d'ordinateurs et autres appareils numériques qui nous entourent, tout en faisant – mieux – ce qu'ils font déjà », puisqu'elle n'est pas en soi d'une grande sophistication, mais elle propose plutôt une interface unique permettant une interaction fluide avec l'ensemble des autres appareils de la maison. Elle agit, en somme, comme le « mât des nomades » décrit par Dominique Boullier, comme un nouveau trousseau de clés outillant nos habitèles domestiques pour ouvrir les nouvelles et innombrables portes

[530] A. GREENFIELD, *Every[ware]*, *op. cit.*, p. 8

numériques des domiciles augmentés. Nous allons donc voir ici en quoi ces dispositifs sont bien plutôt des innovations sur le plan ergonomique que sur le plan strictement informatique.

I - LA FLUIDITE D'ACTION COMME HORIZON : NE MEME PLUS AVOIR BESOIN DE LEVER LE PETIT DOIGT

L'émergence d'agents conversationnels performants permettant un contrôle à la voix est la condition qui rend possible la fluidité d'action au sein du domicile promise par les enceintes connectées. Il s'agit du seul véritable apport fonctionnel amené avec les enceintes connectées par rapport à un smartphone ou à un ordinateur classique antérieurs. L'intérêt en est simple : il faut permettre à l'utilisateur de ne plus avoir à bouger même un doigt pour piloter son logis augmenté.

Exercer un contrôle physique sans la contrainte physique

C'est d'abord un désir de fluidité qui est recherché par les utilisateurs mécanisant puis domotisant leur lieu de vie, et ce dès avant que cette domotique ne soit dite connectée, ou avant qu'elle soit interfacée avec une commande vocale. L'installation d'un rideau roulant électrique, même piloté par un interrupteur, épargne à l'habitant qui l'actionne les quelques secondes et l'effort de tourner la manivelle. Le portail d'entrée commandé à distance, voire automatiquement activé à l'approche de la voiture associée ne sert lui aussi qu'à éviter la rupture de charge au retour chez soi consistant à quitter son habitacle et à ouvrir soi-même les ventaux. De ce point de vue, les enceintes connectées et l'IoT domestique ne font que s'inscrire dans l'histoire d'une quête de confort qui leur est bien antérieure, et qui repose sur la limitation continue des efforts à faire pour paramétrer physiquement son lieu de vie à la multiplicité des pratiques qui s'y déploient. La nouveauté de la commande à la voix est de faire disparaître les derniers mouvements moteurs du corps encore nécessaire. Non seulement ne veux-je pas avoir à déplacer physiquement les lames de mon volet ou les ventaux de mon portail, je ne veux plus avoir non plus à appuyer sur l'interrupteur qui commandera à un moteur de le faire pour moi, un simple mot pourrait suffire.

Pour illustrer ce côté magique de l'absence d'aspérité physique à la simple formulation d'un souhait, la réaction suivante d'E20 est d'autant plus intéressante qu'elle est elle-même défavorable aux enceintes connectées et à la quête du moindre effort. Décrivant une interaction avec une Google Home possédée par une de ses amies proches, elle s'est dit particulièrement « [bluffée] » par le fait que les microphones étaient assez sensibles et la connexion de données

suffisamment forte pour activer l'enceinte de la cuisine jusque dans le salon, et ce, à travers une cloison :

> « [>E20]: C'est assez bluffant notamment chez une amie ou sa cuisine et son salon sont côte à côte juste avec une petite paroi et une porte, en fait en parlant dans la cuisine ça peut connecter l'enceinte qui est dans le salon, ça peut déclencher, ça peut déclencher... [de la musique] » (entretien 13, 3 min 20 s)

Elle utilise le terme bluffant pour décrire cette situation et cet agencement particuliers, qui dépassaient l'attente qu'elle pouvait avoir en général vis-à-vis d'une enceinte connectée. Ce qui motive cette admiration – mâtinée d'inquiétude, comme on l'a vu – , plus que la seule qualité technique des microphones ou des antennes, c'est aussi le fait que l'enceinte n'était même plus présente *physiquement* dans la cuisine au moment de son activation. En cela, il y a eu comme une abolition des lois physiques, ou plus exactement comme une réalisation du fantasme de la maison entièrement interactive (voir « Un fantasme technophile en cours d'actualisation », p. 368).

E5, comme souvent, identifie avec finesse l'intérêt et les enjeux d'une technologie qu'il refuse pour lui-même encore plus radicalement qu'E20. D'un point de vue strictement pratique, il identifie l'enceinte comme un moyen de limiter toujours plus le nombre d'étapes entre soi et l'objet de notre désir, démarche qui lui semble être plus généralement être celle de « l'informatique » moderne dominante (« Toute cette informatique qui vient jusqu'à chez toi pour te dire "tu n'as que à cliquer là ou là". »), et qu'il étend jusqu'aux services de livraison à domicile :

> « Mais sur les enceintes connectées, je suis complètement en phase, un des enjeux des enceintes connectées, c'est de capter les activités commerciales ou de proximité. Et donc, que tes achats que tu ferais chez BioCoop (où nous avons été en arrivant, quand je l'ai croisé en bas de chez lui) , tu les aurais faits directement chez Amazon parce que de toute façon c'est plus facile, tu n'as qu'à le dire à ton enceinte conne... à Alexa. (…) Toute cette informatique qui vient jusqu'à chez toi pour te dire "tu n'as que à cliquer là ou là".
> JF: (acquiesce)
> E5: "Regarde, c'est à deux centimètres et tu auras tous les choix ! Tu n'as même pas à cliquer trop loin !". Un enjeu de cette informatique, c'est l'enjeu de la facilité. La facilité c'est un discours pour t'apporter le produit et te convaincre. Et ça ça rentre dans... un discours qui me semble vaste et important socialement. » (entretien 2 ; 1 h 20 min)

Il se focalise ici particulièrement sur les enjeux commerciaux. De fait, au moment de l'entretien en août 2018, la presse spécialisée et les experts du domaine identifiaient surtout cette question de savoir quels acteurs seraient mis en avant pour la fourniture de services aux particuliers – en demandant à son enceinte un transport individuel, nous proposerait-elle de commander un chauffeur de la marque Uber ? Lyft ? de passer un coup de fil à une société de taxi, et si oui laquelle ? Cette question pouvant s'appliquer tout aussi bien à la commande d'une pizza, ou à une demande de rendez-vous chez le coiffeur. Dans tous les cas, une interface vocale ne permettant pas sans y perdre beaucoup de temps de présenter un grand éventail de choix, l'enjeu commercial principal, plus encore que sur une interface visuelle comme un écran, semblait pour les commerces et les services de s'assurer d'être la première, voire la seule suggestion faite par l'enceinte connectée du consommateur potentiel.

Pour autant, si E5 manifeste ici encore sa connaissance des enjeux affichés ou identifiés par le secteur[531], il est surtout intéressant de voir que cet enjeu lui semble être le dernier développement en date de la question d'une informatique cherchant à faciliter au maximum les actes de consommation, le « confort »[532]. Cela passe pour lui par le minimum de « clics ». Il est intéressant de constater qu'il s'en tient au geste du clic alors que nous parlons ici d'interfaces vocales. Cela tient sans doute au fait qu'il ne soit pas lui-même familier de ces objets. Pour autant, la figure du clic reste pertinente si elle est comprise comme un acte informatique facile, et dont il faudrait que ces actes soient les moins nombreux à faire pour commander un objet ou un service. *De facto*, l'ordre vocal est encore plus facile à faire que le clic, dont il est l'équivalent vocal plutôt que digital, et il dispense (presque) de tenir compte de l'interface de saisie. D'une certaine manière, grâce à la voix, il n'est donc plus même nécessaire de « lever le petit doigt » pour voir un désir réalisé.

Si le discours d'E5 est très critique, on le retrouve dans une formulation différente et nettement méliorative chez E21 à travers la notion de « liberté » :

> « Donc j'aime cette liberté-là. Les objets connectés, j'aime bien le fait... pour moi c'est une liberté de ne pouvoir faire aucun effort. Pour moi c'est la liberté de l'être

[531] Il faut d'ailleurs relever que ces enjeux ne sont pas encore si forts en France trois ans après, surtout en comparaison des États-Unis où le panel des services disponibles *via* les enceintes connectées est beaucoup plus varié.

[532] Dans les minutes qui suivent, il fait une distinction intéressante entre la volonté d'un certain modèle de société (il n'hésite pas à parler de « capitalisme » en un moment de l'entretien) à maximiser le maintien dans une « zone de confort » du consommateur contre le discours à en sortir et à « se dépasser » en tant que « producteur », au travail.

> humain. De ne pas faire d'effort, que tout soit à portée de main. » (entretien 14, 35 min)

Puis une minute plus tard :

> « Quand tu es connecté tu es libre, d'une certaine façon, tout est facile, tu dis à Alexa, elle te donne ton panier d'achat, c'est quand même très facile de le dire, comme ça, verbalement...»
> (entretien 14, 36 min)

Elle reprend à trois reprises dans cette séquence de l'entretien le terme de « fluidité » que je lui suggère, mais c'est bien le terme de liberté qui revient le plus dans son discours. Elle l'utilise à 30 reprises dans ce seul entretien, contre 2 pour moi dans cet entretien, et contre une soixantaine d'occurrences pour le corpus entier. Si le terme est souvent employé dans un contexte plus général, comme une valeur individuelle fondamentale[533], il lui semble tout aussi bien définir la liberté de mouvement, le « confort » qui réside pour elle dans l'absence d'effort. Il ne s'agit pas d'une simple paresse ou d'une réticence générale à l'activité physique : E21 est une femme par ailleurs très active qui a fait l'essentiel de sa carrière dans le domaine sportif. C'est bien là pour elle une forme d'objectif anthropologique (« c'est la liberté de l'être humain ») que de se faire assister de machines pour se délester de toutes les activités qu'elle juge rédhibitoires afin de ne consacrer son temps qu'à des activités plaisantes ou permettant une élévation individuelle.

Elle n'en partage pas moins les inquiétudes d'E5 quant à la question du guidage des choix de consommation par son Alexa, mais son inquiétude à elle tient davantage à la crainte de tomber dans une bulle de filtre et de perdre son autonomie intellectuelle. Elle n'a en revanche rien contre le principe de la livraison à domicile, et me confie même ne plus être capable d'acheter des vêtements en magasin tant il lui est nécessaire de s'assurer qu'elle ne trouvera pas moins cher ou une alternative préférable ailleurs – en plus du « confort » qu'il y a à pouvoir faire ses essayages dans son salon.

Automatisation et routines

Le stade encore supérieur à une activation sans effort physique des effecteurs des objets connectés consiste à ne pas avoir même à donner l'ordre que l'on voudrait voir exécuté. Ce qui est encore plus plaisant que de pouvoir relever le volet sans toucher à un interrupteur en arrivant dans ma cuisine le matin, ce serait qu'il s'ouvre de lui-même en fonction de la luminosité ou de

[533] Elle développe longuement sur la « liberté de pensée » et la « liberté d'expression », en particulier. Son discours sur la vie privée est qu'il s'agit toujours de tenir l'équilibre entre « confort » et « discrétion », la liberté pouvant relever de ces deux pôles qu'elle présente et vit comme antagonistes.

la température extérieures et que je n'ai même plus à *penser* à l'ouvrir ou à le fermer. Cette promesse d'automatisation est l'étape finale d'une installation domotique au sens plein, dans laquelle le logis se régule lui-même pour assurer le confort de ses habitants grâce à des capteurs et des logiciels qui les déchargent de tous les paramétrages et vérifications du quotidien (le degré d'ouverture d'un volet, donc, ou encore le réglage du radiateur, l'arrosage des plantes, le relevé de la boîte aux lettres…).

Chez E3, l'intérêt pour la domotique automatisée est sans doute renforcé par son métier, qui est de produire des logiciels pour automates dans un grand groupe industriel européen. À l'instar d'E21, il est convaincu par l'idée qu'on puisse, voire qu'on doive automatiser les processus jugés pénibles (« rébarbatifs »). Il décrit son métier ainsi :

> [>E3]: Pour... alors le truc de base c'est tuer de l'emploi, mais en fait c'est un peu plus que ça. C'est...[31:22] faire en sorte que les trucs rébarbatifs ne le soient plus, quoi. Alors voilà. Faire en sorte que tout soit automatisé quoi.[31:32] Et...[31:34] je développe là-dedans, mais tout ce qui est sécurité, et même vie privée, c'est des trucs auxquels nous on doit réfléchir.

Même si sa remarque sur le fait de « tuer de l'emploi » est sans doute une manière de désamorcer une critique récurrente contre la mécanisation et l'automatisation, sa formulation laisse néanmoins à penser qu'il a conscience de ce que l'automatisation peut avoir des conséquences immédiates néfastes, il ne récuse pas cet argument adverse qu'il me présente d'ailleurs de lui-même. Après l'emploi, il évoque également la question de la sécurité, « et même » de la vie privée. On devine là encore aux formulations qu'il a conscience des enjeux autour de ces questions (lui et E4 évoqueront spontanément le RGPD plus tard dans la conversation, par exemple), mais que ces enjeux sont secondaires face à l'impératif non questionné qui est d'automatiser les tâches « rébarbatives ».

Cette automatisation passe par un travail préalable de production de petits scripts logiciels par l'utilisateur, qui portent des noms comme « routine » chez Amazon ou « scénario » pour les objets connectés de la marque Konyks. Ils peuvent automatiser tout ou partie des actions effectuables par les appareils connectés du domicile. Ainsi, E3 a créé une routine « cinéma » qui va déclencher une série d'opérations comme le tamisage de la lumière ou l'allumage de la télévision et de la barre de son pour regarder un film confortablement. À un niveau d'automatisation supérieure fondé cette fois sur des capteurs, E15 et E16 ont installé un système d'arrosage en goutte-à-goutte associé à des capteurs d'humidité qui s'occupe de leurs plantes sans intervention de leur part. La plupart des interfaces de programmation de ces scripts

sont des GUI (*graphical-user interface*) simples fournies par les fabricants d'objets connectés et qui ne requièrent pas de compétence en matière d'écriture de code. Certaines sont plus avancées et très finement paramétrables, par exemple avec le protocole IFTT (voir « L'absence de standard universel », p. 327).

L'automatisation est un véritable idéal pour les enquêtés ou les utilisateurs qui se sont engagés dans cette voie : de telles configurations prennent du temps et réclament, même pour les plus simples, un minimum d'autoformation, ainsi que de l'entretien sur le temps long en cas de bug ou de mise à jour logicielle. Il n'y a pas réellement de débat pour savoir si l'on va gagner plusieurs centaines de secondes mises bout à bout en configurant son installation *home cinema* pour s'activer d'une seule commande vocale plutôt que d'avoir à allumer physiquement quelques appareils et à baisser un variateur de lumière. C'est même un lieu commun, notamment sur les groupes d'entraide en ligne, que de s'amuser du fait que les configurations un tant soit peu élaborées font globalement perdre plus de temps à la conception qu'elles n'en font gagner à l'usage. La pratique relève donc au minimum du hobby, et parfois d'un idéal plus élevé qui touche à la conception même de la manière de mener sa vie quotidienne, comme chez E21. De fait, et à ce jour, la fiabilité des enceintes connectées et des configurations IoT domestiques est souvent beaucoup plus faible que ce que les enquêtés laissent entendre, et l'idéal de fluidité absolue au quotidien rarement atteint.

Une fiabilité imparfaite

Malgré les promesses promotionnelles et les discours souvent très enthousiastes de leurs utilisateurs, les enceintes connectées sont d'une fiabilité pour le moins imparfaite. Une grande partie des démonstrations faites en entretien ont échoué, alors même que les circonstances étaient généralement idéales : un environnement sonore calme, et une démonstration faite par un utilisateur maîtrisant *a priori* les contraintes de son appareil et de son logis. De manière générale, les tests et le discours des vendeurs et des utilisateurs d'enceintes connectées avancent que les enceintes de Google et d'Amazon sont les plus polyvalentes en termes de fonctionnalités et ont les agents conversationnels capables des discussions les plus naturelles, alors que celles d'Apple étaient plutôt limitées mais beaucoup plus efficaces pour capter et comprendre la voix. Ces assertions se sont plutôt bien vérifiées dans mon panel, par ailleurs trop restreint pour que je puisse corroborer statistiquement ce qui reste un simple sentiment – seuls deux enquêtés utilisent une HomePod, notamment.

Concernant Google Home, une longue interaction assez rocambolesque a lieu chez E5 et E6. Après qu'ils m'ont expliqué pouvoir facilement activer l'enceinte située dans leur salon depuis le couloir naissant à l'autre bout de la pièce, soit à une distance d'environ huit mètres, nous passons à la question de leurs usages. Ils évoquent le fait qu'ils écoutent les dernières actualités le matin en lien avec l'application de la radio France Info, ce dont E6 me fait spontanément la démonstration, alors que nous sommes attablés dans le salon, à deux ou trois mètres de l'enceinte et en ligne directe :

« E7: Ouais tu dis juste "dis Google, quelles sont les dernières infos", et...
E6: (il se tourne vers GH et parle d'une voix forte) Dis Google.
Google Home: (elle semble ne pas comprendre)
E7: Ben tu l'as coupée.
E6: Dis Google, quelles sont les dernières actualités ?
Google Home: Vous pouvez écouter les actualités à tout moment.
E6: (dépité) Ouais. Bon.
Google Home: (continue ses explications sans nous donner les actualités)
E6: On l'a fait bugger.
E7: Moi j'avais dit la (incompréhensible)
E6: Ouais, désolé, j'aurais dû me taire. (toute cette interaction est assez foutraque, GH continue de parler en fond)
(…)
E6: Hier matin par exemple je lui dis "Dis Google quelles sont les dernières actualités ?"
E7: (interrompant) ... et t'as celles de 7h, quoi.
E6: (il reprend) Là elle me dit "voici les actualités France Info de 7h45".
JF: D'accord (GH continue de parler en fond) .
E6: Dis Google ? Stop. (cela ne fonctionne pas) Dis Google ? Stop. (cela fonctionne) »
(entretien 3, 15 min)

Il est à noter que E7, qui s'exprime d'une voix normale, n'active pas l'enceinte en me disant la première à voix haute par quelle commande activer le résumé des actualités du jour. Ces « fausses » activations surviendront néanmoins à d'autres moments de l'entretien. Lorsqu'E5 prend le relais, il le fait d'une voix forte et en se retournant vers l'enceinte, placée contre le mur derrière lui de l'autre côté de la pièce. L'enceinte ne réagit pas à son mot d'activation. Il insiste, l'enceinte réagit, mais elle ne nous donne pas les informations attendues, seulement un message générique sur la manière de configurer l'assistant à cette fin. Tandis que nous poursuivons l'échange, l'enceinte continue son bavardage au point qu'E5 finit par lui demander de se taire. Même alors, il doit réitérer la commande pour que l'enceinte finisse par se taire. Le fait le plus étonnant ici est que l'enceinte n'ait pas réagi comme anticipé à une commande qu'il lui fait

pourtant tous les matins. Il est possible qu'une mise à jour de l'application ait changé la phrase de commande de la fonctionnalité ou qu'il y ait eu une indisponibilité momentanée du service. L'interaction n'en reste pas moins un échec. Moins surprenant est le fait que les micros aient moins bien fonctionné qu'annoncé par E5. Une forme de biais de validation incite sans doute certains enquêtés à survaloriser les capacités de leur enceinte, comme pour justifier de l'utilité d'en posséder une. Ce type d'échecs d'écoute est également courant dans l'entretien avec E3 et E4 lorsqu'ils me font démonstration de leur enceinte Amazon Echo Dot de petit format (qui entend, elle, « depuis la salle de bains » en forçant un peu la voix[534]), échecs récurrents dont je peux aussi rendre compte dans l'utilisation de l'enceinte Amazon Echo de plus grand format installée dans mon propre domicile.

Concernant la HomePod d'Apple, en revanche, j'ai pu constater en magasin l'efficacité de sa captation de la voix. C'est la principale qualité de l'enceinte mise en avant par E15 et E16, en plus de sa qualité audio, notamment en comparaison avec un iPhone équipé de Siri, beaucoup moins performant :

> « E15: Ah oui oui, si notre téléphone est là (désignant la table basse du salon autour de laquelle nous sommes installés) , et qu'on est dans la cuisine (cuisine américaine, ouverte sur le salon), par exemple, ça marche pas. Enfin... ouais, avec un téléphone. Avec l'enceinte ça marche.
> (…)
> « E15: Y a la musique, aussi. Enfin on avait déjà des enceintes, hein.
> E14: Mais elle fait du bon son, et elle écoute même pendant la musique (au sens où les autres enceintes peinent parfois à discerner un ordre dans un environnement bruyant) .
> E15: (acquiesce) Ah oui, avec le téléphone ça marche pas.
> E14: Pendant qu'il y a de la musique, tu peux lui parler aussi. Elle arrive à dissocier le bruit de la musique, enfin ta voix.
> E15: (acquiesce)
> E14: Et à t'écouter PENDANT la musique, ce qui est assez dingue. C'est... c'est assez puissant.
> E15: Elle écoute bien.»
> (entretien 9, 3 min 35 s)

[534] « E3: Non. Beh on n'a pas un grand appart, ça fait 60 m², et de la salle de bains on peut lui parler. JF: Ah oui ? E3: Ça c'est un truc qui est assez bluffant. Les micros directionnels marchent hyper bien. Même quand il y a le ventilo (un ventilateur tourne dans le coin de la pièce), même quand il y a la télé, ça entend et ça capte bien pile notre voix... En fait, le truc bête c'est quand on est à la salle de bains, on n'a pas d'horloge, et c'est juste... bah "quelle heure il est ?", quoi. Et c'est suffisant pour de là-bas lui dire "Alexa quelle heure il est ?" et hop, ça nous répond, c'est pratique.» (entretien 1, 19 min 30 s)

Le fait que l'enceinte soit activable et comprenne efficacement même avec un fond musical leur semble particulièrement remarquable, notamment en comparaison de leurs iPhones. De fait, et quoique d'autres enquêtés aient pu vanter largement aussi les capacités d'écoute de leurs enceintes[534], ils sont les seuls à signifier que leur enceinte peut les écouter en même temps qu'elle émet de la musique, et il n'y a que chez eux qu'aucune démonstration ne dysfonctionne du point de vue de l'écoute des micros. Ils sont en revanche beaucoup moins enthousiastes quant aux fonctionnalités de leur HomePod, dont ils disent sans ambages qu'elles sont beaucoup plus limitées que celles des autres marques. En outre, et quoique leur installation soit sans doute la plus riche de périphériques domotiques et qu'elle fonctionne visiblement assez bien, certaines démonstrations ne se déroulent pas comme prévu chez eux non plus :

> « E15: Par exemple... (sans lui répondre, en continuant à lire) Heu... si je lui dis de lire ça... "Voyage X 2019"... Dis Siri, quelle est ma note "voyage X 2019" ?
> Siri: Vous devez connecter l'appareil iOS associé au même réseau Wi-Fi pour que je puisse vous aider avec les requêtes personnelles.
> E15: Ah oui, je suis pas connecté, j'ai pas mis le Wi-Fi... voilà. Je refais (il réitère la demande) .
> [2291,4] Siri: Voyons voir...
> E14: Très rapide (ironique, cela prend du temps) .
> E15: Ouais;
> Siri: Vous devez connecter l'appareil iOS associé à ce HomePod au même réseau Wi-Fi (continue couverte par nos voix)
> E15: Voilà, l'intelligence d'Apple ! (ton ironique)
> JF: Voilà !
> E14: (petit rire)
> E15: C'est pour ça qu'on reste avec des requêtes assez simples, hein. (pause)
> JF: Mais les textos tu as déjà essayé, ça marche...?
> E15: (non de la tête) Mais on peut essayer. "Dis Siri, envoie un message à E14".
> Siri: Vous devez connecter l'appareil iOS associé...
> E15: Rooooh c'est dingue ! T'es sûr qu'on est sur le même réseau Wi-Fi, E14 ? Avec tous tes changements que t'as fait ce midi ?
> E14: (à moi) Oui on a changé la box Internet ce matin.
> JF: Ah ! Bah ça doit être ça.
> E14: J'ai un peu... j'ai essayé de remettre tout à jour avant que tu arrives parce que... (petit rire)
> E15: Bah là je suis sur le... ah, il s'est peut-être connecté sur celui du haut ! Je sais pas. Vu qu'il y a pas de réglages.
> JF: Bon, mais c'est pas très... pas très grave. C'était pour voir comment ça marchait.
> E14: En tout cas nos données privées sont protégées, là.
> E15: Bah oui, ça marche pas ! (nous rions tous les trois)» (entretien 9, 33 min 25 s)

Il faut d'emblée préciser qu'ils venaient de recevoir et de configurer une nouvelle box Internet pour leur domicile le jour même, en complément d'un répéteur Wi-Fi (« celui du haut ») dans une autre pièce de leur appartement. Il est probable que leur installation ait mieux fonctionné en conditions normales. Pour autant, et malgré la simplicité de configuration initiale de leur enceinte à Noël [535], le long exemple ci-dessus montre bien quelles difficultés peuvent être rencontrées même sur un système comme celui d'Apple, qui se veut le plus simple possible pour l'utilisateur et qui bénéficie d'une bonne intégration avec les autres appareils, qu'ils soient de la même marque (ici, entre le HomePod et l'iPhone) ou de marques tierces. E15 commente même « Voilà, l'intelligence d'Apple ! » sur un ton ironique, avant de finir sur une plaisanterie : leur vie privée est d'autant mieux protégée que le système ne « marche pas ».

Face à ces difficultés récurrentes, les utilisateurs ne font pas toujours confiance à leur enceinte, même pour des tâches simples, mais importantes. E6, qui se décrit comme très précautionneux en matière de réveil, et même « parano » selon sa compagne, préfère un radio-réveil classique ou son téléphone à une enceinte connectée pour être sûr de ne pas rater son heure de lever. Son discours laisse entendre que c'est avant tout le radio-réveil qui lui semble le plus fiable, soit un appareil très peu élaboré et doté de fonctionnalités limitées, mais éprouvées : « le truc de base, où t'es sûr que ça va sonner » (entretien 3 ; 8 min 35 s). Il n'est cependant pas rétif à l'utilisation du mini-ordinateur qu'est son *smartphone* pour cet usage : la sophistication de l'objet n'est donc pas en soi un problème. Il semble véritablement ne pas faire confiance à l'enceinte pour cette fonctionnalité qu'il estime critique. On peut supposer que ce manque de confiance provient de défaillances précédentes, même mineures, de sa Google Home, ainsi que du sentiment d'un manque de contrôle sur cet objet qui n'offre que peu de *feedback* à son utilisateur, notamment visuel – sauf à utiliser une version dotée d'un écran ou de recourir à l'application dédiée sur *smartphone*, ce qui fait perdre de son intérêt à l'opération : autant utiliser directement le téléphone. Ce manque de confiance concorde bien avec la conception de leur Google Home qu'ont les deux membres de ce couple d'enquêtés, et qu'ils sont parmi les

[535] « JF: Heu... Et du coup, est-ce qu'il y a une application dédiée, sur le téléphone ?
E15: Non.
E14: Non.
JF: C'est que Siri ?
E15: C'est très bizarre, ouais, c'est assez bizarre. La seule configuration qu'on peut faire... bah dès lors qu'on l'a branchée, bah c'était chez tes parents du coup, c'était Noël, il a... il a demandé d'approcher un téléphone.
JF: (acquiesce)
E15: Et donc du coup il s'est configuré à partir du téléphone et le compte associé au téléphone, heu... et puis voilà, c'est tout.
E14: En l'approchant. »
(entretien 9, 33 min 40 s)

plus enclins du panel à décrire comme un simple gadget. Au moins dans cette phase encore précoce du déploiement des enceintes connectées, un sentiment d'absence de maturité de la technologie se dégageait donc assez nettement.

Pour autant, à force de bricolage et de montée en expertise, il reste possible d'avoir une infrastructure matérielle et logicielle fonctionnelle. Soit en s'appuyant sur ses propres compétences techniques initiales en informatique, comme c'est notamment le cas de E3, E8 ou E14, qui finissent tout de même toujours par parvenir à leurs fins. Soit en y consacrant du temps, comme c'est le cas de E16, qui a également un certain bagage technique à travers son activité complémentaire de mixage musical notamment, mais qui a surtout consacré du temps à son installation, capitale pour lui assurer plus d'autonomie dans sa situation de handicap. Après m'avoir longuement décrit son installation, il reprend volontiers le terme de « bordel », que je lui ai suggéré, mais pour ajouter qu'on finit par s'y retrouver :

> « (…) C'est bordélique, et à la fois... rudement efficace quand on... quand on arrive à se frayer un chemin au milieu de ce bordel, quoi. Voilà. » (entretien 10 ; 26 min 30 s)

Malgré la complexité de son installation, qui a réclamé entre autres choses qu'il mette en place un script IFTTT pour contrôler le volume sonore de ses enceintes Hi-Fi *via* Google Home, qu'il utilise un émetteur infrarouge indépendant pour contrôler ses rideaux roulants ou sa télévision, et même envisagé de prendre une enceinte Amazon Echo en complément de sa Google Home pour avoir accès nativement au contrôle de son Chromecast, il finit donc par insister sur le caractère « rudement efficace » de ces prothèses électroniques.

Les déficiences des enceintes peuvent même être vues, dans une certaine mesure, comme un défaut presque aimable. Les activations intempestives d'une enceinte qui a été activée par erreur au milieu d'une conversation qui ne lui était pas destinée amuse régulièrement les enquêtés, parfois au moment même de l'entretien. Et si elle agace souvent, la mauvaise interprétation d'une commande vocale mène parfois à des quiproquos également amusants, voire à de véritables découvertes imprévues. C'est là encore l'entretien avec E16 qui en fournit un exemple au cours d'une séquence où il m'explique que le fait qu'une de ses requêtes pour telle musique ait été mal interprétée par l'assistant Google lui a permis de découvrir de bons morceaux qu'il ne connaissait pas, ou simplement de le faire rire par le décalage entre sa requête et le résultat obtenu :

> « E16: Elle m'a fait découvrir beaucoup de musiques que j'aurais pas forcément écoutées, et comme tu tombes dessus, tu peux lui dire que tu aimes cette musique,

l'ajouter à ma bibliothèque, bah voilà, j'ai trouvé un artiste ou une connerie que j'ai bien aimé, et je peux aller voir après sur mon téléphone, sur mon application Spotify, "tiens, c'était quoi...?".
JF: Et c'est pas une suggestion de Spotify, c'est vraiment une erreur, d'écoute ?
E16: Non non, c'est vraiment une erreur. Elle a mal compris l'artiste, ou elle a compris qu'à moitié, et elle t'a mis autre chose, quoi. Donc des fois l'erreur sont... sont rigolotes (sic). Bon, des fois tu tombes sur un mec qui chante du créole qui vient de la Martinique et tu zappes très vite, mais...
JF: Ca peut être bien aussi !
E16: Oui ! Tu te tapes des bonnes barres de rire, des fois.
JF: (pouffe) Oui.
E16: (souriant) Et tu utilises très vite ton "Ok Google, vire-moi c'te merde !". Mais ouais, non.
Google Home: Excusez-moi, je n'ai pas compris.» (entretien 10 ; 27 min)

Il explique ici que c'est bien d'erreurs d'interprétation vocale qu'il parle, et non de suggestions de Spotify – bien que le résultat de cette erreur soit finalement suggestif, même par accident. Féru de musique électronique, il s'amuse également du décalage avec un morceau de musique instrumentale chantée en créole qui sera finalement joué par son enceinte à la suite d'une incompréhension, et qui provoque « des barres de rire » à défaut de l'intéresser musicalement. Enfin, on peut aussi relever à la fin de cette petite séquence une forme de mise en abyme de l'erreur d'interprétation vocale, puisque son enceinte intervient inopinément dans la conversation en commettant ici une double erreur : d'abord, elle croit qu'E16 s'adresse à elle alors qu'il ne fait que me rapporter une commande sur un ton ironique pour appuyer son propos (« Ok Google, vire-moi c'te merde ! ») ; ensuite, et alors qu'une commande a effectivement été donnée, l'enceinte rapporte juste qu'elle ne l'a pas comprise. Aucune musique n'était jouée pendant l'entretien, et sa requête grossière était peu spécifique, mais l'enceinte aurait pu comprendre qu'il fallait par exemple éteindre les lumières, ou du moins lui demander explicitement de préciser sa demande.

En tout état de cause, c'est sans doute la tirade d'E16 qui résume le mieux le rapport aux enceintes connectées à la domotique connectée dans le rapport au gain de temps et à l'efficacité générale : « (…) C'est bordélique, et à la fois... rudement efficace quand on... quand on arrive à se frayer un chemin au milieu de ce bordel, quoi. Voilà. » (entretien 10 ; 26 min 30 s)

Contrôle à la voix ou contrôle à l'écran ?

Un enjeu de design fort autour des enceintes connectées est de motiver l'utilisation d'une interface vocale, en particulier dans le cas du contrôle de la domotique, et considérant

que l'usage proprement conversationnel des enceintes connectés est encore peu développé. Pourquoi se doter d'un dispositif vocal indépendant quand il est déjà possible, pour tous les enquêtés et pour la plupart des possesseurs d'enceintes connectées, d'utiliser un *smartphone* ou une tablette déjà à disposition ? En effet, malgré tout le discours commercial sur le naturel d'une interaction vocale comparable à une conversation humaine, les défauts des interfaces vocales ont déjà été identifiés. Boullier évoque par exemple des voitures dotées de signaux vocaux pré-enregistrés, les Renault 25, commercialisées de la fin des années 1980 au début des années 1990 : « (…) Certains [objets] d'ailleurs vont jusqu'à parler vraiment, comme les R25 particulièrement énervantes d'une époque, et l'on sait alors qu'il ne faut pas abuser de cette ressource qui permet à l'objet de s'imposer, alors qu'un voyant ne fait qu'offrir son information à votre vision. (…) ».

Ainsi, E14 et E15 insistent dès le début de l'entretien sur le fait que leur HomePod n'ajoute aucune fonctionnalité nouvelle à leur installation. Auparavant, ils commandaient déjà les dizaines d'objets connectés installés chez eux avec leur smartphone, via des applications :

> « JF: Mais vous le pilotiez comment, tout ça, avant ?
> E15: Avec une... (E14 montre son téléphone) Voilà, avec une application.
> JF: Okay.
> E14: Sur l'iPhone ou... enfin le téléphone, quoi. Et maintenant... même un peu avec Siri parce que Siri était présent déjà sur l'iPhone et on avait réussi à le connecter ensemble pour que Siri puisse commander... Ben les autres modules aussi.» (entretien 9, 2 min)

Outre les interfaces visuelles des applications, ils utilisaient aussi dans une moindre mesure l'assistant vocal Siri sur leurs iPhones, avant que d'utiliser celui de leur HomePod. Pour autant, comme on l'a vu plus haut, ils louent la qualité des microphones de leur HomePod, nettement plus sensibles que ceux de leurs téléphones. Quoiqu'ils signalent également la qualité musicale de l'enceinte, ils rajoutent là encore aussitôt qu'ils possédaient déjà un bon système Hi-Fi auparavant. Autrement dit, c'est d'abord et avant tout la capacité d'écoute et le caractère fixe de l'enceinte qui lui confèrent son intérêt :

> « E15: L'enceinte elle n'apporte rien par rapport à ce qu'on avait avant, hein.
> E14: (pause hésitante) Bahhh, si. Il y a le... elle nous écoute ! En permanence. Avant ça ne nous écoutait pas. C'était à nous de déclencher.
> JF: (acquiesce)
> E15: (pause) Bah non.
> E14: Non mais quand tu faisais sur le téléphone ?
> E15: Bah non.
> E14: Ah ouais, remarque, le téléphone il écoutait...

E15: Il se déclenche même quand on le sollicite pas, hein.
JF: (petit rire) C'est vrai, ça c'est un truc qui arrive souvent.
E15: Donc c'est exactement pareil (d'un ton pincé) C'est juste que... C'est juste que si t'as pas ton téléphone à côté de toi, heu...
E14: Ouais, c'est vrai.
E15: ...l'enceinte elle écoute mieux, c'est tout. Voilà.» (entretien 9, 2 min 35 s)

En termes d'écoute, le fait de ne pas avoir à activer le téléphone avant de le solliciter vocalement est un vrai avantage pour eux, mais qui là encore est douteux : quoique la possibilité n'ait pas toujours existé selon les systèmes d'exploitation et leurs versions, il était en fait tout à fait possible pour eux au moment de l'entretien de configurer un iPhone sur un mode d'écoute permanente, à l'instar d'une enceinte connectée. E15 corrige E14 à ce sujet, et conclut que « l'enceinte écoute mieux, c'est tout ». Le cas de ce couple reste extrême en cela qu'ils sont déjà complètement équipés en termes de matériel audiovisuel. Seul le couple de E3 et E4 peut en dire autant, et sans doute aussi E21. Mais ce caractère extrême est particulièrement intéressant en cela qu'il fait d'eux un cas-limite des plus instructifs : ils peuvent finement identifier cet avantage de la qualité d'écoute comme le seul qui soit réellement différenciant par rapport à l'ensemble de ce que le marché de l'équipement de la maison propose aujourd'hui. Pour autant, cela ne doit pas nous inciter à négliger l'ensemble des possibilités offertes par une enceinte connectée (et au premier rang desquels la diffusion du son), qui ne sont pas redondantes avec le reste de l'équipement chez tous les enquêtés, et à plus forte raison tous les utilisateurs.

La qualité d'écoute des enceintes entraîne une conséquence pratique majeure : elle permet d'avoir à se passer d'un téléphone qui, quoiqu'il puisse répondre aux mêmes commandes qu'une enceinte, est victime de ses qualités à l'intérieur du domicile. Certes, il est mobile, mais il est donc déplaçable, égarable ou pas forcément déposé à un endroit permettant une activation facile à la voix. L'enceinte n'a, elle, pas vocation à bouger, on sait toujours où elle est. Certes, le smartphone fonctionne sur batterie, mais il est donc susceptible d'être déchargé au moment du besoin d'activation. L'enceinte, elle, n'a à craindre qu'une coupure de courant, coupures qui sont rares en France métropolitaine. Certes, le smartphone peut accéder à Internet dans tout l'espace couvert par des cellules de téléphonie mobile, mais cela n'a pas d'intérêt par rapport à une enceinte connectée à une box Internet fixe elle aussi, et dont la fiabilité à l'intérieur d'un bâtiment est souvent supérieure à une connexion cellulaire. Certes, le smartphone dispose d'une interface supplémentaire avec son écran tactile. Mais l'enceinte, elle,

n’a pas besoin d’être saisie et d’occuper une main pour ce faire, y compris d’ailleurs quand elle dispose d’un écran comme c’est de plus en plus souvent le cas sur les modèles récents.

En réalité, si la commande des objets connectés est facile avec un smartphone, elle n’en crée pas moins le besoin de recourir à un point d’entrée, une interface très localisée que sont les quelques centimètres carrés de l’écran. Avec une enceinte connectée, c’est tout le phonotope couvert par les microphones qui devient potentiellement une interface, interface qui ne mobilise ni la mémoire de l’utilisateur (« qu’est-ce que j’ai fait de cette télécommande / de mon téléphone ? ») ni ses mains. Même avec une tablette, qui dispose d’un grand écran plus confortable que celui d’un smartphone, et dont on peut penser qu’elle la déplace moins que son téléphone, E21 préfère quant à elle son enceinte à sa tablette pour la diffusion de musique :

> « E21: Mais quand tu en as plusieurs... voilà. Et j'ai même, heu, ajouté... parce qu'elle commande même les ampoules qui sont éloignées, donc dans ma salle de bains, dans la chambre, qui est à l'autre bout, c'est géant, parce qu'elle allume tout, dans toute la maison. Dans tout l'appartement. Et sinon, oui, quand j'ai envie d'écouter un... une petite musique calme, je commande sur Alexa, plus facilement, plutôt que d'aller sur ma tablette... j'ai quand même ma tablette qui est branchée continuellement en Bluetooth à mon enceinte, heu, indépendante, mais c'est vrai que depuis que j'ai Alexa je passe par Alexa, c'est plus simple. » (entretien 14, 1 h 09 min)

Si une interface visuelle est beaucoup plus riche et de toute façon nécessaire au moins le temps de paramétrer les configurations plus avancées, l’interface vocale est en revanche beaucoup plus efficace pour les commandes les plus simples. Un des usages qui revient le plus dans le discours des enquêtés, en plus de la musique ou la radio, et qui illustre bien cet état de fait, est celui de la minuterie de cuisine. Malgré sa banalité apparente, elle me semble cristalliser tout l’intérêt ergonomique des enceintes connectées. Il s’agit en effet d’une fonction basique, très peu susceptible d’erreurs, et dont le bon fonctionnement est aisément contrôlable. Il suffit d’activer la fonction « chronomètre » et de spécifier une durée. Surtout, elle est l’exemple même de l’intérêt d’une activation à la voix par rapport à une activation sur écran : inutile de s’interrompre pour se laver ou se sécher les mains afin de manipuler un smartphone ou autre, qu’il faudra à nouveau manipuler pour désactiver l’alarme, et qu’il faudra déposer en attendant à proximité immédiate plutôt que de dégager sa table ou son plan de travail. En somme, et même si une interface visuelle permettrait ici de multiplier plus facilement les chronomètres, par exemple pour différentes cuissons, ou de suivre visuellement le ou les décomptes du temps, c’est au finalement l’interface vocale, moins riche mais plus ergonomique dans ce cas de figure, qui l’emporte dans l’usage.

II - CHOISIR SON MAITRE D'ORCHESTRE

La question du prix

Quoique les enquêtés interrogés aient pour beaucoup été bien renseignés sur les différences entre les marques et les types d'enceintes connectées disponibles, un critère absolument déterminant est presque à chaque fois revenu pour déclencher ou non un achat : le prix de vente. Il éclipse presque toujours les autres considérations, même chez les plus technophiles et/ou les plus riches des enquêtés. Cela n'a bien sûr rien de surprenant pour un objet qui reste un bien de consommation. Si l'on affine la lecture des discours tenus, on peut néanmoins retenir deux idées plus spécifiques aux enceintes connectées. D'une part, l'acte d'achat semble relever avant tout de l'opportunité, particulièrement dans un contexte d'offres promotionnelles très régulières de la part des fabricants. D'autre part, la distinction entre les différentes marques ne se fait que peu en fonction du prix, sauf en ce qui concernait la HomePod d'Apple, nettement plus chère que la concurrence, et qui n'est plus aujourd'hui en vente.

La quasi-totalité des enquêtés ayant acheté une enceinte connectée ne l'a pas acquise à son prix public, ou pas sans une incitation supplémentaire sous la forme d'une offre groupée. J'ai pu le constater de première main lors de mes observations en magasin. Lors de ma première rencontre le 9 mars 2018 avec E17, vendeur dans un grand magasin d'électronique[536], l'une des principales questions des deux clientes qui l'interrogeaient sur Google Home était de savoir si l'offre combinée avec le service musical en ligne Deezer était toujours valable, ce qui ramenait le prix de l'enceinte à une quinzaine d'euros seulement après déduction de l'équivalent financier des mois gratuits sur Deezer – elles comptaient offrir l'enceinte et conserver les bons pour elles-mêmes. Il m'a confirmé plus tard en entretien qu'il avait vu les ventes s'envoler à partir de l'arrivée des versions mini des enceintes vendues généralement une trentaine ou une quarantaine d'euros (pour un prix public autour des 60 €), et dans son cas de la Google Home Mini :

> « La force de Google... ça coûtait une centaine d'euros. Là, la force de Google, c'est que la même chose existe, mais en plus petit, et à une trentaine d'euros. C'est, c'est, c'est... c'est magnifique ! C'est-à-dire que c'est quelque chose de pas cher... alors si, y a certains clients qui me disent "mais y a quand même un loup, il y a quelque chose", et là je leur dis juste "bah oui, ça collecte plein de renseignements, alors c'est pas vous qui êtes surveillé, mais c'est un ensemble qui fait que c'est utile pour l'entreprise, qui les revend à des services divers dont on a même... qu'on connait

[536] Les informations au sujet de son lieu de travail restent vagues à sa demande.

même pas".»
(entretien 11 ; 15 min 20 s)

Il est intéressant de constater que les acheteurs potentiels étaient alors étonnés du faible prix de ces enceintes, au point qu'ils y voyaient « un loup ». De fait, les Google Home Mini ou les Echo Dots d'Alexa étaient et sont encore généralement vendus à proximité des autres enceintes, notamment de type Bluetooth seul, dont les prix plancher sont au mieux de cet ordre de grandeur et peuvent monter beaucoup plus haut, alors même qu'elles proposent une variété de fonctionnalités infiniment moins importante. Il est particulièrement intéressant de constater qu'E16, quoiqu'il ne soit sans doute pas représentatif de sa profession, précise sans détour à ses clients que la collecte de données à des fins publicitaires, qui fonde une grande partie du modèle d'affaires de Google, est intégré au prix de ces enceintes. J'ai d'ailleurs pu le constater par moi-même lors de l'interaction évoquée plus haut, où il a effectivement tenu ce discours en situation de vente.

Un discours tout à fait similaire m'a été tenu, cette fois par une acheteuse, à la FNAC du centre commercial de la Part-Dieu à Lyon le 21 décembre 2020. Abordée immédiatement après sa conversation avec un vendeur où divers points pourtant intéressants, d'ordre technique ou pratique, ont été évoqués, sa première réaction est de me parler de l'offre financièrement intéressante du jour – habituelle des périodes de fêtes :

[>E11]: Ben en fait, heu, ouais, parce que vous m'avez entendu parler (avec le vendeur) c'est ça ?[03:14]
[>JF]: Oui oui, du coup j'ai suivi un peu votre conversation.[03:16]
[>E11]: Non mais en fait moi je connaissais pas et j'ai pas forcément l'utilité, mais je regardais vu qu'il y avait une offre en fait.[03:20] A partir de 150 € d'achats, au lieu de coûter, heu, 60 €, elle passe à, à 20 €.
[03:25] [>JF]: Ouais !
[>E11]: Donc c'est intéressant.
(entretien 7, 3 min 15 s)

Il n'y a donc pas chez elle d'intention particulière en matière de marque ou de modèle : il était déjà acquis qu'elle désirait offrir une enceinte connectée quelle qu'elle soit à ses parents, elle est déjà très familière des services de Google, et le discours commercial du vendeur de la FNAC associé à la promotion en cours ont achevé de provoquer l'acte d'achat.

Lors de l'entretien de groupe avec E3 et E4, ils me rapportent également sans détour que le prix a été le principal de leurs critères lors de l'achat de leur Echo Dot. Là encore, E3 a pourtant une approche technique, voire technicienne, des enceintes et des objets connectés. Ses

compétences professionnelles lui permettent d'avoir une assez claire vision des mécanismes et protocoles liés à la domotique. Au moment de l'entretien, il avait même déjà développé sur son temps libre une *skill* (application) pour Alexa, à savoir un petit *quizz* sur les villes capitales. Je l'ai par ailleurs rencontré sur hardware.fr, un forum technique de bidouilleurs avertis suivant l'actualité du domaine. Même pour lui, l'intérêt technique est au second plan derrière le prix : il fallait, certes, que l'enceinte soit compatible avec les quelques objets connectés qu'ils possédaient déjà, essentiellement des ampoules Phillips Hue. Au bout du compte, c'est le prix qui a achevé de le convaincre, puisqu'à 25 € au moment de l'achat, il n'investissait au fond que le prix d'un repas au restaurant :

> [>E3]: En fait 60 euros, je vais pas dire que c'est une grosse somme, mais... ben je réfléchis plus. Voilà, 25 euros, c'est...[18:24] c'est le prix d'un repas au resto, je dis "pour tenter, au pire j'ai perdu 25 euros".[18:34] 60 ça m'embêterait plus. (entretien 1 ; 18 min 20 s)

Le choix d'Echo plutôt que de Google Home ne tenait donc qu'au prix, la gamme de leurs ampoules Philips, déjà bien installée à l'époque, était de toute façon bien prise en charge par l'ensemble des marques d'enceintes connectées. Et ils utilisent sans réserve les services de Google, notamment Google Calendar et Google Musique (payant), qu'il aurait été intéressant de pouvoir utiliser *via* une enceinte, ce qui n'a pourtant pas été un facteur de choix là non plus. De ce fait, la seule enceinte qu'ils ont toujours écartée de leurs choix possibles était la plus onéreuse HomePod d'Apple, qui venait de sortir au moment où ils ont envisagé l'achat d'une enceinte connectée.

De fait, la HomePod d'Apple s'est longtemps singularisée dans le marché des enceintes connectées, jusqu'à l'arrêt de sa production. Pour E3, son prix était rédhibitoire : « Heu... en fait c'était juste que, en fait, moi quand je l'ai pris, Apple ils commençaient juste d'arriver, mais toujours avec leur enceinte à pas loin de 200 balles. » (entretien 1 ; 14 min 57 s). En réalité, son prix public était même de 350 €. Il n'y a pas de réticence à la marque Apple chez E3 et E4, qui ont longtemps été équipés en iPhones et en MacBook, et qui reconnaissent la qualité de ces produits, bien qu'ils les aient toujours trouvés assez chers. Au-delà du prix tout de même, il est à signaler que Siri leur semblait moins efficace comme agent conversationnel. La stricte reconnaissance vocale des HomePods leur semblait probablement la meilleure, y compris avec un fort bruit de fond, mais ils sont satisfaits de celle de leur Echo. Au bout du compte, il s'agit ici simplement d'une question de gamme de prix : E3 ne se sent explicitement pas dans la « cible » (E3 ; entretien 1 ; 15 min 17 s) *marketing* d'Apple en termes d'enceintes connectées.

Il est à noter que les questions de vie privée n’ont joué en aucune façon dans le choix de la marque. Parmi les GAFAM, seul Facebook leur semble être pire que les autres. Pour le reste, c’est équivalent :

> [>JF]: Okay, du coup tu m'as dit pour la marque (pas de préférence pour l'une ou l'autre, toutes se valent même Apple, c'est le prix le critère déterminant) . Un truc qui m'intéresse des fois, c'est de savoir par rapport à Apple, sur les questions de vie privée, les gens sont parfois plus sereins vis-à-vis d'Apple.[14:52]
>
> [>E3]: Non, les trois c'est les mêmes...
>
> [14:55] [>E4]: ...ils sont tous pareils ![14:57]
>
> [>E3]: ... on peut mettre Facebook, Facebook c'est un peu à part mais... tout ce qui est Google, Amazon et Apple, ils traitent ça de la même manière. Heu... en fait c'était juste que, en fait, moi quand je l'ai pris, Apple ils commençaient juste d'arriver, mais toujours avec leur enceinte à pas loin de 200 balles.
>
> [15:15] [>JF]: Même plus, 350 je crois

Au bout du compte, seuls E14 et E15 ont beaucoup dépensé pour leur enceinte chez Apple (ce que E15 avait souligné par « c’est un beau cadeau »). Leur critère de choix était de prendre un objet facile à intégrer à leur matériel existant largement dominé par Apple, par exemple pour simplifier les partages de calendrier ou d’autres informations de ce type déjà renseignés via leur compte iCloud. Dans leur cas, on peut même faire l’hypothèse que le prix élevé a peut-être également joué aussi *en faveur* de l’achat d’une HomePod : le fait que E15 rappelle à deux reprises qu’il s’agissait d’un « beau cadeau » signale sans doute que le prix de l’enceinte la qualifiait d’autant plus, selon la logique de la consommation de luxe de biens dits positionnels, dont l’intérêt est davantage de marquer la position sociale de son possesseur (ou de l’offrant) que de faire montre de capacités techniques supérieures.

En d’autres termes, la segmentation en gammes du marché des enceintes connectées au sens strict, sans écran d’appoint d’une taille significative, est encore très limitée, et elle s’est encore réduite avec l’arrêt de la production des modèles Apple les plus onéreux. Cela me semble révélateur du fait que ce marché est encore en train de se constituer, et que la principale préoccupation des fabricants est toujours d’en conquérir le plus de parts plutôt que de maximiser leurs marges.

Entre le passe-temps et le défi technique

Quand E7 évoque le désir initial de son compagnon E6 de mettre en place une installation plutôt élaborée, interconnectant son ordinateur personnel, sa console de jeu et leur Google Home, celui-ci botte immédiatement en touche :

> « E6: (il s'anime) Oui ! Je voulais faire un truc avec la PS4 et avec mon PC, aussi, mais ça c'était purement gadget.
> JF: Oui.
> E6: C'était pour m'amuser, pour qu'il s'allume tout seul, et tout. Mais apparemment c'est pas possible.
> JF: Ah !
> E6: Je suis très déçu. » (entretien 3 ; 7 min 20 s)

Étonnante est sa volonté de diminuer l'intérêt et la difficulté de ce projet avorté, intérêt qui transparaît pourtant dans son regain de vivacité après cette évocation. E6 donne ensuite les raisons techniques qui l'ont découragé et empêché de mettre en œuvre son idée, mais il ne la diminue pas moins en la qualifiant de « gadget », terme qu'il intensifie même de l'adverbe « purement gadget », avant de préciser encore qu'il ne s'agissait que de « s'amuser », pour insister sur la vanité du projet. Il y a ici une nette volonté de montrer à l'enquêteur qu'il est très détaché de l'objet Google Home comme des possibilités d'aménagement de ses équipements électroniques, qui contraste avec l'intérêt qu'il démontre pour la technologie, explicitement et implicitement, tout au long de l'entretien. Sa fierté était par exemple manifeste lorsqu'il m'a décrit comment il avait projeté l'écran de son *smartphone* sur sa télévision *via* Chromecast, même si l'enceinte n'était pas impliquée dans ce cas (voir « Contrôle à la voix ou contrôle à l'écran ? », p. 316). Si son « je suis très déçu » est sans doute volontairement exagéré, il dénote néanmoins d'une déception non feinte. De fait, chez d'autres enquêtés très technophiles, comme E3 ou E14, on a pu constater à plusieurs reprises déjà que leurs diverses réussites, de l'aménagement de leur domotique à la programmation de *skills* pour Alexa, étaient de véritables motifs de fierté. Cette fierté se retrouve également en ligne sur les groupes d'entraide, où le style de poste d'utilisateurs se vantant d'avoir réussi un aménagement domotique esthétique ou complexe est courant, de même que les remarques appréciatives pour ces mêmes aménagements.

La volonté de diminuer l'importance ou l'intérêt d'aménagements domotiques élaborés tient sans doute également souvent à une dynamique de groupe, et particulièrement de couple. Ainsi, dans la minute qui suit l'expression de déception et les explications techniques d'E6, sa compagne E7 le reprend, goguenarde, « Et puis c'est vrai que notre appartement est tellement

grand que c'est dur d'aller appuyer sur un bouton ! (rire)» (entretien 3 ; 8 min). C'est un réflexe qu'on retrouve également quelque peu chez E4 par rapport à E3, mais presque pas chez E15 par rapport à E14, ces deux derniers partageant plus équitablement leur intérêt pour la domotique.

Maximiser la compatibilité avec les applications et objets possédés ou désirés

La question de la compatibilité est fondamentale en termes d'usages possibles et, *ipso facto* dans le choix de tel ou tel appareil, dès lors qu'on cherche à aller plus loin que les usages standards du type de l'allumage de luminaires. Il n'existe en effet pas de protocole standard pour l'ensemble des usages domotiques ou multimédia impliquant des objets connectés. Par exemple, au cours de l'entretien 10, E16 cherche à me faire la démonstration que YouTube n'affiche pas de publicités quand il est affiché sur son téléviseur LG plutôt que sur son *smartphone* ou son ordinateur. Cette démonstration est surtout l'occasion de constater combien compliquées sont les installations à faire pour un usage *a priori* simple, tant d'un point de vue logiciel que matériel :

> « E16: Mais je regarderai, quand même. (il regarde son téléphone pour afficher YouTube sur le téléviseur) Et les trucs où il y a de la pub... ça m'étonne, d'ailleurs. Il y a forcément de la pub, sur un machin comme ça ? Aucune connexion... Ah, là il y a de la pub. Fais voir, si j'envoie sur "Télé LG"...
> JF: Il lance l'appli... l'appli qui est dans la télé, en fait ?
> E16: Alors là, tu as le Chromecast. Moi j'envoie YouTube de mon téléphone sur le Chromecast.
> JF: Ouais.
> E16: Et Chromecast, il va faire YouTube, Spotify, et... et après, c'est tout. Je vais rien pouvoir faire d'autre, c'est pour ça que j'utilise Apple TV à côté. On a oublié de parler de l'Apple TV, si tu voulais en parler en plus, qui me sert à mettre du streaming. Parce que je peux pas utiliser le Chromecast pour mettre en streaming n'importe quelle vidéo, sur mon iPad ou quoi que ce soit. Je peux pas la transférer sur du... un lecteur OpenLoad, ou un lecteur Stream&Go (sites de streaming illégaux) je peux pas les mettre sur le Chromecast.
> JF: Tu peux pas... envoyer n'importe quel flux vidéo, par le Chromecast ?
> E16: A priori non.
> JF: Je pensais que c'était plus ouvert que ça.
> E16: Moi aussi ! Du coup j'ai été obligé de récupérer le, l'Apple TV de mon père, qui l'utilise pas. C'est pour ça que moi j'ai pleiiin de trucs à droite à gauche pour compléter, parce qu'il manque ci à droite, ça à gauche... Mais ouais, ouais, tu vas sur un site de streaming, tu mets en plein écran, le seul truc qui s'affiche, c'est le logo pour avoir le AirPlay. Et t'as pas le logo Chromecast qui s'affiche. » (entretien 10 ; 1 h 16 min 10 s)

Plus tôt dans l'entretien, E16 avait déjà eu longuement l'occasion d'évoquer des questions techniques et pratiques de cet ordre. Même alors, il avait oublié de me préciser qu'il disposait également d'une Apple TV, tant sont nombreux les appareils qu'il est contraint d'utiliser (« Du coup j'ai été obligé de récupérer le, [le boîtier de] l'Apple TV de mon père, qui l'utilise pas. C'est pour ça que moi j'ai pleiiin de trucs à droite à gauche pour compléter, parce qu'il manque ci à droite, ça à gauche... »). En l'espèce, bien que la clé Chromecast de Google soit le standard *de facto* pour la diffusion sans fil d'images via le Wi-Fi, on s'aperçoit ici qu'il ne permet pas de simplement transférer le flux vidéo de manière universelle. Il semble que l'application YouTube du *smartphone* agisse ici plutôt comme une télécommande pour l'application YouTube installée sur le téléviseur. C'est d'ailleurs de la question de la différence entre les deux applications quant à la diffusion de publicité qu'est venue la démonstration d'E16. Il précise en outre que son Chromecast filtre certains contenus, en l'occurrence des sites de *streaming* vidéo illégaux. Cela a conduit E16 à utiliser en complément une Apple TV, reposant encore sur d'autres protocoles de transmission, et qui lui permet l'usage recherché. Du point de vue des assistants connectés, cela le conduit donc à devoir mobiliser son Google Home, mais aussi le Siri de son téléphone ou de son ordinateur, pour peu qu'il veuille exécuter ces commandes à la voix.

Il est cependant à signaler que, malgré ces difficultés d'interopérabilité, les enceintes connectées sont aujourd'hui un des meilleurs pis-aller pour certains usages simples, comme l'allumage d'ampoules connectées de marques diverses. E21 explique ainsi avoir été ravie de découvrir qu'elle n'avait plus à passer d'une application à une autre pour piloter les ampoules de son appartement, produites par trois marques différentes, et requérant une application chacune pour leur pilotage *via* une interface visuelle :

> « E21: Moi j'ai bien mon ampoule. Et avant j'utilisais bien, sur ma tablette, chaque ampoule c'était même pas la même application, il y avait plusieurs applications, tu as Tuya, tu as...
> JF: Ah oui, c'était pas la même...?
> E21: Ça dépend du… du truc que t'achètes. J'ai trois applications pour toutes les ampoules. Et... avant je faisais ça sur ma tablette. Et un jour j'ai découvert, pour m'amuser, j'ai dit "Alexa, change la lumière jaune en blanc", et elle l'a fait. "Change la lampe africaine, par exemple, rouge en jaune", je la fais clignoter, tout, pas mal. » (entretien 14, 2 h 21 min 20 s)

Pour peu que plusieurs objets connectés ayant un même usage soient connectés à une enceinte connectée, il est alors possible de les activer collectivement, par exemple en créant un groupe « Salon » ou « Chambre ». Une commande de type « Allume le salon » activera alors toutes les ampoules de la pièce, même si elles sont de marques différentes. Les réglages plus fins

nécessiteront toujours de passer par les applications idoines, comme pour activer des modes propres aux fabricants (synchronisation de la lumière avec la musique jouée dans la pièce, changements dynamiques de la couleur de la lumière, etc.), mais l'enceinte peut malgré tout jouer son rôle de hub pour les usages généraux.

L'absence de standard universel

La question d'un protocole domotique universel permettant de couvrir l'ensemble des usages de l'IoT du domicile est en fait un véritable serpent de mer, qui revient très régulièrement dans les groupes de discussion d'entraide, ou dans la presse spécialisée. En août 2021 encore, et alors même que le marché de la domotique est bien identifié par les entreprises comme un secteur en forte croissance (voir « Le marché de la *smart home* », p. 167), l'avènement d'un standard universel est encore si improbable que le journal en ligne d'information sur le numérique grand public *Numerama* titrait sur le « bazar » continuel dans le secteur (« C'est toujours le bazar dans la domotique et ça ne va pas s'améliorer de sitôt »[537]). Résumant la situation du secteur, le journaliste spécialisé Corentin Bechade affirme que « La domotique reste un hobby de technophile averti et la situation n'est pas prête (sic) de s'améliorer ». À rebours des prétentions à la simplicité des entreprises du secteur, force est en effet de constater que l'interconnexion de services et d'objets requiert toujours des recherches préalables poussées, et une installation parfois complexe, comme nous l'avons vu dans l'exemple d'E16. Un protocole véritablement standard est en effet un prérequis à l'interopérabilité de l'IoT, à l'instar de (piles de) protocoles comme TCP/IP qui permettent à n'importe quel terminal de communiquer avec l'ensemble des autres terminaux connectés à Internet, sans se soucier, par exemple, de la marque de son fabricant, ou du fait qu'il se connecte par un réseau de téléphonie mobile ou *via* un modem domestique, un réseau Wi-Fi mesh ou autre.

La question de l'élaboration de protocoles standards est en soi une question récurrente dans l'ingénierie, et à plus forte raison dans l'ingénierie informatique. Comme l'écrit Pierre Musso, « Le but de la normalisation est de permettre l'interopérabilité des réseaux et des terminaux. Elle conditionne l'existence des télécoms à l'échelle internationale, comme l'a montré la création précoce de l'UIT. »[538] Cette affirmation ne vaut pas seulement pour les réseaux de télécommunications de très large échelle (régionale ou nationale), mais elle

[537] C. BECHADE, « C'est toujours le bazar dans la domotique et ça ne va pas s'améliorer de sitôt », *Numerama*, 16 août 2021 (en ligne : https://www.numerama.com/tech/732843-cest-toujours-le-bazar-dans-la-domotique-et-ca-ne-va-pas-sameliorer-de-sitot.html ; consulté le 17 août 2021)
[538] P. MUSSO, « IV. La numérisation du système des télécoms », dans *Les télécommunications*, Paris (France), La Découverte, 2008, p. 60-73

s'applique également à l'échelle très fine de nos objets connectés : l'utilisation d'un même protocole (ou de protocoles compatibles, s'appuyant sur la même norme ou le même standard) est absolument nécessaire pour que l'information transmise d'un objet à l'autre soit comprise et interprétée. Or, dans le domaine de l'IoT, il n'existe pas encore d'équivalent de l'UIT (Union internationale des télécommunications) pour réunir les acteurs du secteur afin de convenir d'une véritable norme. Pour reprendre Pierre Musso, si « Des normes stables évitent d'investir dans de multiples passerelles entre réseaux et favorisent les effets d'échelle [et que la] normalisation est d'autant plus importante qu'il s'agit d'interconnecter, à l'échelle mondiale, divers types de réseaux au moment même où la dérégulation multiplie leur segmentation », alors la situation actuelle dans l'IoT et la domotique en particulier est clairement encore celle d'une grande segmentation.

Dans le domaine de la domotique et des enceintes connectées, plusieurs tentatives ont déjà échoué ou n'ont pas encore réussi à s'imposer. Un article de synthèse du journal en ligne Next INpact consacré aux protocoles radio dans l'IoT en juin 2022 était encore ironiquement sous-titré « Pourquoi faire simple quand on peut faire compliqué »[539]. Il existe en effet une petite dizaine de protocoles aujourd'hui, à l'interopérabilité faible voire inexistante, ce qui obère le récit général de fluidité et de simplicité associé à l'IoT domestique. On peut néanmoins signaler qu'avec Matter, « Un standard censé mettre tous nos appareils d'accord sur un protocole de communication unifié vient d'être repoussé à l'année prochaine ». Le protocole Matter est, à partir de l'annonce de son soutien par Google en mai 2021, le nouveau nom du protocole CHIP. Initialement développé par la Zigbee Alliance, cette dernière a également été renommée à cette occasion Connectivity Standards Alliance[540]. CHIP était déjà lui-même fondé sur la norme 802.15.4 de l'Institute of Electrical and Electronics Engineers (IEEE). Ce *re-branding* est révélateur des ambitions du protocole : devenir la matrice de protocoles standards pour l'ensemble du secteur. Matter est soutenu officiellement par Google, qui souhaite ainsi « simplifier la *smart home* par l'utilisation d'un standard unique pour l'ensemble du secteur »[541]. Avec la contribution de cet acteur majeur, le protocole pourrait parvenir à s'imposer. Il sera en

[539] S. GAVOIS, « On vous explique les protocoles pour les objets connectés : Zigbee, Z-Wave, EnOcean, DIO… », *Next INpact*, 29 juin 2022 (en ligne : https://www.nextinpact.com/article/69505/on-vous-explique-protocoles-pour-objets-connectes-zigbee-z-wave-enocean-dio? ; consulté le 1er juillet 2022)
[540] S. GAVOIS, « Domotique : CHIP devient Matter, la Zigbee Alliance renommée Connectivity Standards Alliance », *Next INpact*, 12 mai 2021 (en ligne : https://www.inpact-hardware.com/article/2469/domotique-chip-devient-matter-zigbee-alliance-renommee-connectivity-standards-alliance ; consulté le 27 septembre 2021)
[541] « (…) simplifies smart homes by using one standard across the industry » M. TURNER, « 4 Google smart home updates that Matter », sur *Google*, 19 mai 2021 (en ligne : https://blog.google/products/google-nest/four-google-smart-home-updates-matter/ ; consulté le 11 septembre 2021)

effet intégré nativement au système d'exploitation mobile de Google, Android, qui était présent sur 85 % des smartphones expédiés dans le monde en 2017, avec une projection à 86,2 % pour 2022[542]. La version finale du protocole a été publiée début octobre 2022[543].

Il est à noter que si Amazon est lui aussi partenaire de la Connectivity Standards Alliance, Apple continue de faire cavalier seul avec son protocole HomeKit. Si les chances de Matter de parvenir à s'imposer comme un nouveau standard industriel semblent importantes, le marché de l'IoT restera malgré tout divisé dans un proche avenir au moins, avec des produits qui pourraient rester dédiés uniquement à l'intégration dans le système d'Apple, politique technique et commerciale qui s'inscrit du reste dans les pratiques historiques de la marque, par exemple en matière de connectique filaire pour l'alimentation ou les connexions de données de ses appareils.

III - L'ENCEINTE COMME BIEN COMMUN DOMESTIQUE

Si l'enceinte connectée a pour fonction d'être le point de jonction prédominant entre les objets connectées d'un logis et ses habitants, la question se pose de son statut hybride d'objet collectif dans l'espace domestique, mais utilisé par des individus différents aux profils et aux habitèles multiples.

Une utilisabilité universelle dans le phonotope domestique

La promesse de fluidité d'action permise par les enceintes connectées, malgré ses imperfections effectives, est beaucoup plus inclusive que celles des outils numériques antérieurs : si un nombre de personnes non-négligeable restent touchées par l'illectronisme et peine parfois à se servir d'un *smartphone* ou d'un ordinateur, il suffit en théorie de savoir parler pour pouvoir interagir avec une enceinte. Du petit enfant à la vieille personne, aucun outil numérique aussi sophistiqué n'a jamais été aussi facile à actionner et à commander – sans pour autant dire que ces commandes, au sens informatique du terme, seront bien interprétées. L'enceinte connectée me semble être la première interface numérique aussi universelle : seule

[542] IDC, « Répartition des expéditions de smartphones dans le monde par système d'exploitation entre 2013 et 2022 », sur *Statista*, décembre 2018 (en ligne : https://fr-statista-com.ezproxy.u-pec.fr/statistiques/570954/part-de-marche-mondiale-des-systeme-d-exploitation-de-smartphone-en-expeditions-d-unites--2020/ ; consulté le 22 août 2022)

[543] Anon., « Domotique : le protocole Matter a sa version finale », *Next INpact*, 4 octobre 2022 (en ligne : https://www.nextinpact.com/lebrief/70089/domotique-protocole-matter-a-sa-version-finale ; consulté le 4 octobre 2022)

l'aphasie empêche pour l'instant d'actionner une enceinte[544], et même la surdité n'empêche pas tout à fait de l'utiliser.

En tant que maître d'orchestre de la nouvelle informatique domestique, l'enceinte peut être amenée à être utilisée par n'importe quelle personne présente à portée de voix efficace de ses microphones. Pour autant, une enceinte connectée ne peut pas vocalement interagir avec plusieurs personnes à la fois : l'utilisation des fréquences sonores du phonotope domestique utilisables par la voix humaine est exclusive, une enceinte ne peut pas (encore) interpréter deux commandes simultanées, et quand bien même cela serait possible techniquement, on peine à imaginer que deux personnes ou plus trouveront opportun d'activer en même temps la même enceinte. Cela étant dit, et même si des cas existent sans nul doute hors de l'échantillon, aucune des personnes interrogées n'a rapporté de situation de captation de l'enceinte connectée à l'usage exclusif d'un seul membre de la famille. Dans la totalité des cas, l'enceinte apparaît comme un bien commun domestique, à l'inverse par exemple d'un smartphone qui reste généralement un objet individuel, et peut entraîner des conflits d'usage de la ressource exclusive qu'est le phonotope : je pense par exemple à la concurrence que peuvent se faire des individus souhaitant diffuser leur musique sur une enceinte Bluetooth, et qui pourront être tentés de se disputer le canal pour leurs usages respectifs. *A contrario*, l'enceinte connectée, en tant que maître d'orchestre de la domotique de la maisonnée, mais aussi comme nouvelle intervenante dans le phonotope du domicile, est, presque par définition, un objet partagé.

Qui possède quelle enceinte ?

Cette dimension collective de l'objet est nettement apparue à partir d'une question d'apparence anodine dans le guide d'entretien : qui possède l'enceinte ? Dans les faits, l'objet est souvent acheté ou acquis ensemble, par exemple comme cadeau-bonus lors d'une promotion. Il s'agit aussi très couramment d'un cadeau, qui dans ce cas sera peut-être destiné à une seule personne du foyer, mais qui finira généralement installé dans une pièce commune et sera utilisé par tous. Si E3, E8 et E21 ont acquis leur enceinte eux-mêmes, tous l'ont finalement placée dans le salon et ouvert à l'utilisation des autres membres du foyer. Elle a été offerte à E6, E14 et E16. Les deux premiers l'ont, là encore, placé dans le salon à l'usage de tous. E16 présente un cas particulier en cela qu'il s'agissait plus pour lui d'une forme de prothèse lui permettant de compenser sa mobilité réduite : il est le seul à l'avoir installée dans sa chambre. L'acquéreuse

[544] Cela est déjà de moins en moins vrai avec les fonctions vidéo ou de détection de mouvement dont on a vu qu'elles commencent à se développer, et qui permettront à terme des interactions gestuelles avec l'appareil.

d’une Google Home rencontrée à la FNAC, enfin, la destinait à ses parents, mais dans ce cas là aussi il s’agissait d’un cadeau collectif et non individuel.

Une fois placée dans un espace collectif, la propriété de l’enceinte comme objet n’est plus très pertinente. Elle finit utilisée (ou du moins utilisable) par tous, au même titre que tout autre appareil électronique ou ménager. En tant qu’interface vocale, elle est d’abord et avant tout définie par le phonotope dans lequel elle se trouve, qui devient le véritable enjeu spatial dans l’utilisation de l’enceinte. Même si son utilisation est exclusive à une personne pendant la durée de son activation, ces activations sont généralement plutôt brèves, et permettent à tous de l’utiliser à un moment ou à un autre.

On peut faire l’hypothèse que la situation serait très différente pour une enceinte installée dans un espace privé tel qu’une chambre. Même si la portée des micros de l’enceinte permettait de l’activer de l’extérieur de la pièce, c’est bien le phonotope de la chambre qui serait mobilisé, avec le potentiel de lutte des places qu’on imagine aisément entre le ou les occupants de la chambre et les autres. Des cas concrets n’ont cependant pas été évoqué par les enquêtés utilisateurs d’enceintes, qui n’en possédaient tous qu’une seule par foyer à l’époque de la campagne d’entretiens. E3 a en revanche clairement évoqué son intention d’en offrir une à terme à leur fille pour qu’elle la mette « dans sa chambre », au même titre que les chaînes Hi-Fi de sa propre enfance :

> « E3: Je pense qu'à terme elle aura une enceinte pour elle... Pour moi c'est les chaînes Hi-Fi du futur pour les gamins. Quand j'étais gamin on voulait, on rêvait tous d'avoir sa chaîne Hi-Fi, le gros truc dans sa chambre, pour pouvoir écouter ses CD ou ses cassettes, et... c'était une question d'indépendance vis-à-vis des parents. Et je pense que pour les enfants futurs c'est quand même hyper pratique, parce que quand ils voudront écouteur leur musique, moyennant contrôle parental qui va bien, ils auront la possibilité d'écouter ce qu'ils veulent dans leur chambre sans casser nos oreilles. »
> (entretien 1, 20 min 25 s)

L’enceinte connectée ne lui semble pas beaucoup plus spécifique ici qu’une chaîne Hi-Fi classique, à ceci près qu’elle dispensera son utilisateur de gérer CD et cassettes, et qu’elle nécessitera des mesures de « contrôle parental », au même titre sans doute pour lui que n’importe quel ordinateur connecté à Internet destiné à un enfant ou un adolescent. Même si le phénomène n’est pas nouveau ni spécifique aux enceintes connectées, il est intéressant de voir qu’un tel objet aurait pour lui deux objectifs : préserver le phonotope collectif (« ils auront la possibilité d'écouter ce qu'ils veulent dans leur chambre sans casser nos oreilles ») mais aussi

permettre aux jeunes de s'approprier l'espace privé de leur chambre par la maîtrise de son phonotope (« c'était une question d'indépendance vis-à-vis des parents »). On devine qu'il admettra sans problème que cette enceinte connectée-ci soit à l'usage exclusif de sa fille, et il en fait même un des moyens par lequel il compte lui permettre d'acquérir de l'autonomie au sein de la maisonnée.

Cependant, et même si l'enceinte connectée comme objet physique s'est avérée être un bien collectif ou collectivement utilisé dans l'ensemble du panel, une question subsidiaire mais non moins importante était également de savoir à quels comptes et profils en ligne l'enceinte était liée.

Profil(s) individuel(s), usage collectif

Reposant massivement sur des services en ligne, les principales gammes d'enceintes connectées aujourd'hui encore requièrent la création de profil d'au moins un utilisateur pour accéder aux fonctions de l'enceinte. Ces profils uniques par entreprise sont interopérables avec les autres prestations du fabricant. Un utilisateur d'une Echo pourra ainsi passer commande en ligne sur Amazon via son enceinte, son compte est le même. Cette ouverture préférentielle sur le reste de l'offre du fabricant est un des moyens de s'assurer un flux régulier de revenus pour les fabricants, plus particulièrement pour Amazon et Google : il ne s'agit pas de vendre une seule fois, et généralement à un prix faible, une enceinte connectée qui aura un accès illimité dans le temps aux prestations de l'entreprise, mais d'espérer générer de nouveaux actes d'achat via l'enceinte, ou l'abonnement à des services payants comme Google Musique ou Amazon Prime.

Sans surprise, c'est généralement le propriétaire de l'objet qui crée ou lie un profil existant à son enceinte. C'est le cas dans l'ensemble de l'échantillon, avec une incertitude pour les parents d'E11 dont on peut envisager qu'elle installera chez eux l'enceinte avec son propre compte Google. Dans l'ensemble de l'échantillon, cette configuration est plutôt effectuée par des hommes, à l'exception de E21. Cette configuration est une petite responsabilité pour le propriétaire, qui aura à charge d'installer les applications complémentaires nécessaires ou demandées par les autres habitants. On a vu que, dans le cas de E14 et E15, cela pouvait être générateur de frictions plus ou moins grandes, en cela que celui qui manifestait plus clairement son souhait de configurer leur webcam de surveillance pour se désactiver à leur entrée dans l'appartement, E15, n'était pas celui qui avait accès à ces paramètres, à savoir E14, dont le compte est seulement lié à l'enceinte mais pas à la webcam de surveillance. L'enceinte ou un

objet connecté peuvent donc venir s'intégrer dans des dynamiques de pouvoir et de conflit de gestion de l'espace domestique, au même titre que les tâches d'entretien de la maison plus généralement.

On voit déjà à travers cet exemple que, au-delà de la responsabilité dans l'entretien de l'enceinte et de la domotique par le titulaire du compte associé, un enjeu de surveillance interne au domicile se pose également du fait de cette prééminence d'une personne dans la gestion d'un bien collectif. Nous évoquons plus directement le cas avec E8 à partir de la question de son accès privilégié à l'historique d'utilisation de son enceinte Echo. Après m'avoir signalé qu'il sait que son épouse utilise l'enceinte malgré ses réticences affichées vis-à-vis de l'objet, je lui demande s'il le sait grâce à l'historique. Il répond que non, et m'explique qu'il constate plus trivialement que la « radio » est souvent allumée à son retour du sport. Il développe ensuite assez largement sur sa profonde désapprobation relativement au « flicage » qu'il pourrait opérer sur sa famille via la consultation de l'historique, avec un air de gravité qui tranche nettement avec la bonhommie qu'il manifeste dans le reste de l'entretien :

> « E8: Quasiment jamais, à part quand elle [l'enceinte] n'a pas compris un truc et que ça m'agace. Mais sinon je ne le regarde pas, ça me... Ben parce que ça m'intéresse pas, en fait, tout simplement. De voir ce qu'ils ont pu demander, ou... ce qu'ils ont pu faire.
> JF: (acquiesce)
> E8: Pour le coup, c'est vraiment un truc... c'est pas un truc qui me, qui me... A ce moment-là, c'est le même, le même, heu... la même optique qu'une personne qui va regarder dans le téléphone portable de son conjoint ou de sa conjointe pour regarder s'il n'a pas des SMS, heu...
> JF: (acquiesce)
> E8: C'est la même chose, en fait ! (pas tout fait selon moi)
> JF: Oui. Ben alors autant là...
> E8: (interrompant) Ouais, je pense que sur le principe, si c'est via Alexa par exemple, ou via... en prenant le téléphone et en regardant ce qu'il y a eu sur le téléphone de... de la personne avec qui tu vis... C'est juste là encore un autre média pour avoir une espèce de flicage.
> JF: Ouais.
> E8: Mais si, personnellement, t'es pas enclin à ça... C'est pas un truc, qui... voilà (son ton est plus grave depuis quelques minutes maintenant, moins enjoué) . C'est juste une histoire de (incompréhensible) » (entretien 4, 58 min 40 s)

Cette longue tirade révèle tant le fait qu'il ait conscience de l'asymétrie de capacité vis-à-vis des membres de son foyer qui lui est offerte sur l'objet en tant que titulaire du profil-utilisateur,

et de la responsabilité éthique afférente à ne pas en faire usage. Il va jusqu'à faire la comparaison avec le fait de consulter subrepticement le téléphone d'un conjoint pour en vérifier les SMS. Cette comparaison est sans doute excessive *per se*, ne serait-ce que parce que l'enceinte n'est pas perçue, utilisée, ni d'ailleurs utilisable, pour des usages aussi personnels qu'un téléphone. Pour autant, E8 ne voit pas de différence de nature ou d'attitude entre ces deux pratiques, qu'il réprouve tout autant l'une que l'autre.

Cependant, en créant un lien avec un profil utilisateur préexistant qui n'est pas uniquement dévolu à la gestion de la domotique d'un foyer, l'enceinte n'ouvre pas seulement l'espace privé du domicile aux services d'acteurs économiques tiers, ni ne donne potentiellement accès à l'utilisateur enregistré aux pratiques des autres membres du foyer. Elle ouvre également le profil de l'utilisateur-configurateur lui-même à l'influence des pratiques autres que les siennes qui vont venir influer sur la construction de son propre profil. On l'a vu, le principe fondateur du capitalisme de surveillance est de capter le « surplus comportemental » des individus, afin de les profiler du mieux possible et d'optimiser les opérations de marketing qui les ciblent. Ce profilage peut se faire de multiples façons, mais l'association d'un appareil à un identifiant unique, en particulier s'il est lié à un profil connu et renseigné par la personne elle-même, en est le cas le plus évident. Là encore, il n'y a là non plus pas de vrai problème déclaré par les enquêtés vis-à-vis de leur enceinte. Le seul type de soucis parfois évoqué est celui de voir son profil parasité, pour ainsi dire, par l'identité d'une autre personne. C'est par exemple le cas de E6, dont la compagne regarde des vidéos sur YouTube à partir de son compte, et qui se voit exposé à des publicités et des suggestions plutôt destinées à E7, comme la chaîne de la vidéaste maquillage et beauté Enjoy Phoenix. Pour autant, quand on évoque l'enceinte elle-même, les deux sont catégoriques sur le fait qu'ils n'ont repéré aucune confusion équivalente. Il est difficile de dire objectivement si cet effet-retour sur l'utilisateur enregistré existe ou non, et la perception qu'ont les enquêtés de la situation ne permet pas de trancher en un sens ou un autre.

Enfin, il est aussi possible d'utiliser certaines fonctionnalités liées au compte de la personne ayant configuré l'enceinte en son nom, comme l'envoi de SMS :

> « E15: Il (HomePod) reconnaît toutes les voix (une pointe de fierté dans la sienne) . Mais il est connecté à un compte.
> JF: Un compte, okay.
> E14: D'ailleurs c'est gênant pour ceux qui veulent faire une mauvaise blague en disant "envoie un message à un tel", ça va l'envoyer avec le téléphone de E15.» (entretien 9, 15 min 45 s)

Le cas est hypothétique, et fait écho aux détournements effectués par des publicitaires ou la série d'animation *South Park*. Cette fois, il s'agirait non pas d'utiliser l'enceinte comme un moyen d'accéder au domicile via une diffusion extérieure de masse, mais bien pour un individu d'exploiter son accès au domicile pour utiliser les ressources de la personne ayant configuré l'enceinte : ses SMS, donc, mais pourquoi pas aussi son calendrier, ses *playlists* musicales ou autre.

Pour autant, ces deux ensembles de problèmes, qu'ils soient potentiels ou actuels, peuvent être résolus par la désactivation momentanée du profilage[545] ou, de façon plus élaborée, par la mise en place d'un profilage vocal à l'échelle des individus pour ce qui concerne les assistants vocaux partagés. En plus des enjeux sus-évoqués, il s'agit aussi plus simplement de pouvoir proposer une expérience d'autant plus personnalisée aux divers utilisateurs d'une enceinte, comme d'accéder à son agenda personnel ou de lancer ses listes musicales. L'enjeu est tout à fait comparable avec les comptes de vidéo à la demande tel que Netflix ou Prime Vidéo, qui proposent de souscrire collectivement à leur offre, mais de singulariser les membres d'un foyer pour optimiser les recommandations qui leur sont faites, et pour leur permettre d'avoir chacun leur historique de visionnage. Pour ce faire, il suffit de spécifier à quelle personne sera attribuée l'historique de la session actuelle au moment de l'ouverture de l'application. Cette sélection est triviale avec une souris ou une télécommande, mais elle est plus difficile à mettre en œuvre pour une interface vocale qui se veut le plus fluide d'utilisation possible. L'enjeu pour les fabricants est d'associer ces sous-profils à la signature vocale unique de chaque personne. Google l'a proposé en premier avec sa fonction « Voice Match » fin 2017 aux États-Unis[546], avant que cette fonctionnalité ne soit progressivement étendue au reste du monde. Amazon a rapidement suivi avec ses « Alexa Voice Profiles »[547]. Dans les deux cas, il

[545] E14 et E15 racontent par exemple qu'il est possible de désactiver le profilage d'Apple Musique, par exemple pour éviter au cours d'une soirée que les requêtes musicales des invités se traduisent par des suggestions peu pertinentes pour eux-mêmes :
« E14: Oui, mais tu peux désactiver l'option en disant... ils ont prévu maintenant l'option... parce que ça pourrit des fois... c'est le problème notamment en soirée, c'est toujours le problème des soirées. C'est super sympa, tout le monde dit ce qu'il veut écouter et après, heu... t'as tout qui...
E15: (interrompant, amusé) Ça te pourrit tes favoris !
JF: Ouais ?
E14: Dans ton Apple Music, quand tu es sur ton téléphone...
JF: Oui, c'est la question que je voulais poser.
E14: Il y a moyen de dissocier les deux.» (entretien 9, 16 min 50 s)

[546] R. AMADEO, « Google Home can now tell users apart just by their voice », *Ars Technica*, 20 avril 2017 (en ligne : https://arstechnica.com/gadgets/2017/04/google-home-gets-support-for-multiple-users/ ; consulté le 22 août 2022)

[547] T. MARTIN, « How to set up voice recognition on the Amazon Echo », *CNET*, 12 octobre 2017 (en ligne : https://www.cnet.com/home/smart-home/how-to-setup-voice-profiles-on-the-amazon-echo-alexa/ ; consulté le 22 août 2022)

faut entraîner son assistant durant quelques minutes en prononçant sur commande la série de phrases demandées pour créer un profil vocal qui sera associé à un unique compte individuel, puis ajouter ces différents comptes dans l'interface de l'enceinte du foyer. Si cette solution est élégante, elle n'est pas tout à fait triviale à mettre en place, et n'est de fait évoqué par aucun des enquêtés utilisateurs d'enceintes. En outre, si elle cloisonne les profils des différents utilisateurs, elle rend aussi possible l'accès aux données de chacun d'entre eux à travers un unique objet partagé, qui est toujours susceptible de détournements – on peut envisager le cas d'une personne enregistrant une requête vocale d'un membre de son foyer pour avoir à son agenda ou à d'autres informations en son absence, sans même parler de la possibilité d'accéder au profil de quelqu'un d'autre du fait d'une erreur de reconnaissance vocale ou un d'un bug. Comme souvent, l'individualisation accrue des pratiques permises par et sur des services numériques améliore donc la qualité du service et sa sécurité, autant qu'elle expose à un risque d'autant plus fort que les enjeux augmentent en même temps que les voies, même étroites, de mésusage du service.

*

En tant que hubs domotiques au cœur des logis augmentés, les enceintes connectées sont donc de nouveaux points focaux pour l'organisation et l'équipement du logis. Elles conditionnent le choix des objets connectés périphériques qui leur seront liés, et amènent les habitants à de nouvelles réflexions relativement à leur phonotope domestique. En somme, nous allons voir que les enceintes connectées deviennent de nouveaux enjeux de l'aménagement de l'espace domestique à l'échelle micro. Comment s'inscrivent-elles dans la gestion quotidienne de l'espace et des spatialités du foyer ?

Chapitre 3 - ENTRE L'ASSISTANT ET LE CONCIERGE

Les enceintes connectées ont été conçues pour jouer un rôle de hub dans le réseau des objets connectés. Mais ce rôle de pilotage n'est pas uniquement d'ordre technique : leurs capacités conversationnelles leur confèrent, beaucoup plus que tout autre objet technique jusqu'alors, une fonction sociale en cela qu'elles miment les interactions humaines. À ce titre, elles sont évidemment des actants, c'est-à-dire des « réalités sociales, humaine[s] ou non-humaine[s], dotée[s] d'une capacité d'action »[548]. Dépourvues de la subjectivité ou de la capacité stratégique qui feraient d'elles des acteurs au sens plein, leurs capacités conversationnelles poussent néanmoins leurs utilisateurs à les traiter comme de quasi-agents, des « actants humains non acteurs »[549], avec un rôle d'exécution. Sans rentrer dans le débat complexe sur l'autonomie stratégique d'un logiciel [550], il n'est pas exclu que des développements ultérieurs amènent ces dispositifs à être traités comme de quasi-acteurs dans le futur.

Le terme d'« assistant connecté », qui désigne les logiciels (Alexa, Siri, Google Assistant) plus que les enceintes elles-mêmes (Echo, HomePod, Google Home) est éclairant : là où l'on parle plutôt d'*assistance* à la conduite automobile ou d'*assistance* électrique pour un vélo, par exemple, ces logiciels capables de converser sont désignés par un substantif qui les personnifie davantage, *assistant*. Pour les activer, on s'adresse à Alexa ou à Siri par leur prénom, et même si Google porte celui d'une entreprise, l'un de ses mots de réveil par défaut, « Dis Google », inclue l'impératif du verbe « dire » qui contribue là encore à l'impression de s'adresser à un interlocuteur humain. Une entreprise du nord de la France a, dans un registre proche des enceintes connectées, proposé à la vente un bouton connecté aux fonctions plus limitées (il s'agit essentiellement de signaler arrivée et départ du logement pour activer en une fois un scénario global du type « allumer/éteindre les lumières », « lever/baisser les stores »)

[548] Le développement de la définition ajoute d'ailleurs « Les objets matériels s'avèrent également, dans nos sociétés où leur nombre et leur sophistication s'accroissent, des actants. On pense aux machines communicantes, parfois quasi personnifiées, mais la moindre enquête permet de voir que l'objet le plus trivial et le plus insignifiant constitue potentiellement un opérateur d'une redoutable efficacité. » *in* M. LUSSAULT, « Actant », dans J. Lévy et M. Lussault (éd.), *Dictionnaire de la géographie et de l'espace des sociétés*, Paris (France), Belin, 2003, p. 38-39

[549] M. LUSSAULT, « Agent », dans J. Lévy et M. Lussault (éd.), *Dictionnaire de la géographie et de l'espace des sociétés*, Paris (France), Belin, 2003, p. 47-48

[550] Les logiciels classiques, entièrement écrits, ne sont que la projection et l'automatisation de processus créés par leurs auteurs. Ils relèvent de la logique du mécanisme, un assemblage plus ou moins complexe, mais fini. Avec les logiciels capables d'apprentissage, le logiciel gagne en autonomie vis-à-vis de ses concepteurs. La question n'est plus de savoir « comment amener mon logiciel à faire ceci ? », mais « pourquoi le logiciel a-t-il choisi de faire cela ? ».

qu'elle a néanmoins nommé Concierge, et auquel elle propose de donner un prénom au moment de « rencontrer votre concierge » au cours de la configuration initiale dans l'application pour smartphone qui lui est associée[551]. Si le premier produit de la marque, Concierge Bell, proposait des interactions très limitées, les produits ultérieurs Concierge Call et Concierge Visio ont par ailleurs été dotées, sans surprise, de l'assistant vocal Alexa.

Le champ notionnel de l'assistant et du concierge ajoute un éclairage supplémentaire à la simple lecture de l'enceinte connectée comme hub domotique. Cette fonction est une des principales conditions de l'intérêt et du succès de ces objets, mais elle n'informe pas complètement sur l'étendue de leurs effets sociaux et spatiaux, pas plus que sur ceux de l'IoT domestique qu'ils pilotent. Les box des fournisseurs d'accès à Internet occupe une fonction tout à fait comparable dans le réseau des objets connectés d'un logement, et les enceintes connectées s'appuient d'ailleurs sur leurs capacités réseaux distante (pour l'accès à Internet) et locale (pour le Wi-Fi, quoique dans une moindre mesure). Pour autant, les enceintes connectées et la domotique qui leur est associée ont des effets sociaux et spatiaux d'échelle fine beaucoup plus nombreux, que ce soit dans l'aménagement du logis (chapitre 1) ou sa gestion à distance (chapitre 2).

I - UN GESTIONNAIRE DE/DANS L'ESPACE DOMESTIQUE

Aménager « un monde à [son] image »

Nous avons vu grâce à Sloterdijk qu'« Avec une peau médiatique électronique, le corps de l'humanité veut se créer une nouvelle constitution immunitaire »[552], peau électronique qu'il pense sans doute à une échelle globale et dont Internet est la manifestation la plus évidente, mais en voyant bien à travers la mise en avant d'une logique plus « pragmatique » et fondée par les spatialités qu'il fallait en saisir toutes les manifestations et l'interspatialité aux échelles les plus fines. Le concept d'habitèle de sens 2 chez Boullier nous a donné les clés, presque littéralement, nous permettant d'explorer l'articulation des pratiques numériques avec la question de la vie privée. Dans le moment où nous sommes désormais, à savoir celui d'une analyse micro-spatiale des pratiques et des agencements de l'habiter s'appuyant sur les enceintes connectées et la domotique, il faut rappeler que l'habitant n'est pas le principe

[551] V. DE BRYE, « Test Bouton connecté Concierge : un assistant dont l'utilité nous échappe », *Les Numériques*, 14 décembre 2018 (en ligne : https://www.lesnumeriques.com/objet-connecte/concierge-concierge-p29407/test.html ; consulté le 23 août 2021)
[552] P. SLOTERDIJK, *Bulles*, *op. cit.*, p. 28

déterminant entièrement la forme de son logis, mais que ces deux réalités sont en co-construction permanente[553].

Les paramètres physiques à prendre en compte pour augmenter le logis d'une multiplicité d'objets connectés font cependant l'originalité de la question domotique, en réintroduisant des questions d'aménagement physique du domicile, à la dimension tout à fait concrète, là où les derniers développements des technologies numériques allaient plutôt vers un détachement des contraintes physiques. Pour autant, ce retour à l'espace résulte lui aussi d'un processus de transformation des espaces du logis et du quotidien, que je décrirais volontiers comme une forme de micro-aménagement du territoire du logis, comme le suggère également Staszak[554]. Dans *Un monde à son image*, Jean-Marc Besse décrit bien ce processus à travers le terme d'« arrangement » :

> *« Il faut prendre ce mot *arrangement* à la fois dans son sens spatial et dans son sens transactionnel : d'une part on dispose un espace pour la vie quotidienne, en rangeant et en ordonnant les choses avec lesquelles on a affaire tous les jours ou presque de notre vie, mais d'autre part on s'arrange avec ces choses, on transige avec elles. On s'accommode des choses en même temps qu'on se les accommode, dans une sorte de transaction perpétuelle entre elles et nous pour créer et entretenir le lieu propre de notre vie commune »*[555]

Il développe ensuite sur cette activité spécifique qu'est l'entretien du domicile, et qui va de l'activité la plus triviale et la plus quotidienne, le ménage, jusqu'à l'organisation ou la décoration des pièces. L'augmentation numérique d'un logis grâce à l'enceinte connectée et la domestique procède d'un premier mouvement de (re)construction du domicile (voir « L'habitant-aménageur », ci-dessous), qui doit mener en retour à la facilitation de la vie quotidienne des habitants (voir « Le majordome numérique », p. 345).

L'habitant-aménageur

La domotique est un nouveau domaine de *travail sur l'espace domestique* de l'habitant-aménageur, qui s'ajoute à d'autres tâches comme l'entretien et le ménage ou la décoration, bien

[553] Boullier, dans son texte sur le numérique habitable, se sert pour sa part de la notion de « transduction » empruntée à Gilbert Simondon pour dire que l'habitant et l'habitat ne sont pas des réalités exclusives, mais plutôt qu'elles sont toujours engagées dans un processus bijectif de construction réciproque.
[554] « l'habitant de l'espace domestique est un acteur impliqué dans l'aménagement de celui-ci » *in* J.-F. STASZAK, « L'espace domestique », *op. cit.*, p. 353
[555] J.-M. BESSE, *Habiter*, *op. cit.*, p. 18

décrites par Jean-Marc Besse. Il s'agit de faire des choix qui conditionnent des fonctionnalités, comme on l'a vu, mais qui conditionnent donc aussi un mode de vie. Plus généralement, la domotique prolonge et renforce le contrôle sur l'espace du domicile : son phonotope par les enceintes, mais aussi son atmosphère (thermostat, climatisation et chauffage, purificateur d'air…), son immunité (télésurveillance, serrure connectée…) ou sa propreté (aspirateur-robot) et ce, fait assez nouveau, à distance. On peut d'ailleurs faire un parallèle entre la sophistication croissante des capteurs et des effecteurs dont nous nous servons pour entretenir nos domiciles et la réflexion sur les capsules spatiales comme cas-limites et horizon d'attente de l'habitat humain développée par Sloterdijk dans *Écumes*. La domotisation de nos domiciles pourrait ainsi constituer une nouvelle phase de rupture et d'artificialisation de nos espaces de vie, après celle de l'air conditionné.

Dans ce nouveau travail sur l'espace domestique effectué par les habitants, deux cas paroxystiques se dégagent dans notre échantillon par l'ampleur et le soin apportés à l'augmentation de leur lieu de vie, et un troisième présente l'intérêt d'avoir été effectué hors du domicile de l'habitant-aménageur.

E14 et E15 : le contrôle de l'espace domestique

Le premier cas concerne le couple formé par E14 et E15, qui se distingue par la variété de leur installation. Il s'agit du lieu de vie que j'ai observé qui concentre le plus grand nombre de périphériques et la plus grande diversité de fonctions. Au niveau de l'utilisation de l'enceinte pour elle-même, ils se cantonnent à des usages assez classiques :

> « E15: Nous on l'utilise beaucoup pour écouter de la musique.
> E14: Le plus c'est la musique, quand même.
> E15: Pour...
> JF: Ouais.
> E15: ...contrôler les volets, les lumières... Heu... Un peu la radio, les minuteurs, enfin ouais, après, les trucs comme ça. » (entretien 9, 5 min 20 s)

Ils écoutent surtout la musique avec leur HomePod, un peu moins la radio (encore le matin même de l'entretien), s'en servent comme minuteur… Mais on commence déjà à voir dans cet extrait qu'ils ont aussi d'autres d'objets connectés à piloter : les volets roulants et les ampoules sont les premiers éléments qu'ils citent, sans doute car ils sont installés depuis les débuts de la domotisation de leur appartement actuel quatre ans plus tôt. De fait, la quasi-totalité des luminaires de leur appartement sont connectés, à l'exception de ceux de la salle de bain, mais en incluant y compris des « [petits] » luminaires d'appoint de type lampe de chevet dans le

salon[556]. Au-delà de ces premiers éléments qu'ils citent spontanément, il faut les interroger plus précisément pour qu'ils énumèrent le reste de leur installation : interrupteurs connectés, thermostats, détecteurs d'ouverture de fenêtre, une électrovanne pour l'arrosage automatique de leur jardinière extérieure, le système d'alarme, une station météorologique complète (avec thermomètre, hydromètre, anémomètre). Et, bien sûr, leur fameuse webcam de vidéosurveillance. On remarque que, dans leur cas, l'accent est particulièrement mis sur le contrôle du volume d'air du domicile, à travers la gestion de la luminosité et de l'ensoleillement avec les volets roulants ; divers capteurs comme le thermostat ou l'hygromètre qui permettent en retour la gestion du chauffage ; le détecteur de fumée ou la webcam permettant de veiller sur leur logement à distance… Ils présentent volontiers leur installation comme un jeu, comme lorsqu'ils expliquent moins recourir à certaines fonctionnalités, comme l'électrovanne.

E16 : être autonome chez lui

La logique est légèrement différente dans le deuxième cas paroxystique, celui d'E16 qui, étant affecté par une tétraplégie, a dû aménager son espace de vie de manière beaucoup plus drastique que tous les autres enquêtés. La domotique, classique ou connectée à son enceinte Google Home et à son *smartphone*, y joue un rôle majeur, qui se remarque dès les premières minutes de mon arrivée chez lui pour l'entretien :

> « E16: Tu veux de la lumière, un peu ?
> JF: Ouais, c'est là ? (désigne un interrupteur)
> E16: Non, ça va être les volets. (d'un ton de bonimenteur de foire) Ok Google, allume la cuisine ! Allez.
> [288,7] Google Home: Ok, j'allume cuisine.
> E16: Ça c'est le grand truc, parce que comme j'ai pu tout concevoir moi-même... J'ai tout prévu, au millimètre près, pour une construction, tu fais ça au mieux, le rail, tout ça (un rail au plafond qui permet de le suspendre et de le déplacer facilement entre le lit, la cuisine et la salle de bain) .
> JF: Tu veux dire dès le départ de...
> E16: (interrompant, fier) Ah, j'ai tout dessiné. J'ai pas eu besoin d'ergothérapeute, tous ces connards de charlatans… »
> (entretien 10 ; 4 min 40 s)

Il insiste sur le fait que tout a été aménagé selon ses plans, « au millimètre près », et avec un niveau de professionnalisme qu'il estime être supérieur à celui d'un ergothérapeute dont c'est pourtant le métier. Nous passons une part de l'entretien à détailler par exemple la manière dont il a planifié les passages de rails au plafond qui facilitent ses déplacements en suspension. En

[556] « E14: Ouais, y a la salle de bain qui n'est pas connectée. Autrement... je pense qu'on a tout connecté. Même les petites, là (dans le salon, donc, des petites lampes type chevet) » (entretien 9, 6 min 30 s)

outre, la plupart des ouvrants et luminaires sont motorisés ou activables à distance, pour l'ouverte des volets roulants, des portes, baies vitrées, ou plus simplement des luminaires. Il est à relever qu'il n'a pas immédiatement utilisé une enceinte connectée, son handicap ayant été antérieur à leur commercialisation. En revanche, il avait déjà commencé à expérimenter les fonctions vocales équivalentes de l'assistant vocal Siri de son téléphone et de sa tablette. Au bout du compte, c'est son frère qui lui a fait cadeau de sa Google Home à Noël en 2017, alors qu'il n'habitait pas encore dans la maison où l'entretien a eu lieu, et même s'il ne fait pas de doute qu'il en aurait acquise une de lui-même assez rapidement. L'enjeu pour E16 était légèrement différent de celui de E15 et E14, puisqu'il s'agissait moins d'améliorer la maîtrise à distance de son domicile dans lequel il passe de toute façon l'essentiel de son temps que d'y faciliter le déclenchement des appareils.

Dans ce contexte, les deux principaux apports de l'enceinte étaient d'améliorer la captation de sa voix, le *smartphone* étant un peu moins performant dans le domaine, mais également de ne pas avoir tout le temps ledit téléphone à proximité immédiate, particulièrement la nuit, pour limiter son exposition aux ondes. Plus que d'autre, il a dû tenir compte de la portée efficace des micros de son enceinte : il sait précisément moduler sa voix pour déclencher une action selon son positionnement dans son studio, et le gain d'efficacité d'écoute de l'enceinte lui a fait faire un « bond » dans son autonomie. Il explique ainsi :

> « E16: ...qui forcément font que j'ai, j'ai... comment dire, j'ai très peu d'autonomie, et pouvoir accéder à la radio, à la musique, à... savoir s'il va faire beau ou pas beau pour que je puisse m'habiller, ou juste écouter de la musique... ça a été un BOND niveau autonomie pour moi, quantitatif, clairement, dans ma vie. C'est...
> JF: Parce que tu pouvais pas le faire avant, avec un Siri ou...
> E16: C'était complexe. C'est-à-dire que mon téléphone s'il était pas assez près... ça marche moins bien, Siri peut pas commander les applications, je peux pas commander Spotify, dire de mettre telle musique...
>
> (…)
>
> E16: Oui, déjà la voix, il comprend beaucoup mieux les choses, par rapport à une distance.
> JF: Ouais.
> E16: Même à cinq mètres de moi, je peux lui dire de mettre la musique, je suis pas obligé de répéter à Siri dix fois, ou de me rapprocher de Siri pour que mon téléphone comprenne (étonnante formulation, ce serait plutôt l'inverse) . Siri faut être le nez dedans, pour pouvoir lui parler, ce qui... ce qui est comme ça, c'est pas fait autrement, point-barre. Alors que Google Home, je peux l'avoir sur le meuble, de ma chambre, et le matin j'ai pas besoin de demander à l'auxiliaire de demander me mettre le

> téléphone dans le coin du nez pour faire... quoi que ce soit. » (entretien 10, 10 min)

En somme, l'apport de l'enceinte connectée a été de lui faire gagner en indépendance en rendant tout le phonotope de son studio interactif à la voix, qui est son principal moyen autonome de projection dans l'espace. C'est aussi à travers l'exemple d'E16 qu'on mesure le mieux ce qu'est le travail de configuration et d'aménagement de l'espace domestique en fonction des objets et enceintes connectées. Il insiste particulièrement sur le fait qu'une grande partie de son temps est consacré à l'entretien de son corps avec l'aide des personnels soignants qui l'assistent au quotidien. Dans sa conception du temps, il lui faut maximiser les quelques heures d'autonomie dont il disposera dans une journée, pour lire, écouter de la musique, naviguer sur Internet ou autre. Il a, par ailleurs, des difficultés à manipuler une tablette ou un téléphone pour les configurations d'objets connectés sur une application. Qu'il s'y consacre est donc encore moins trivial pour lui, même s'il est par ailleurs très compétent techniquement. Ainsi, il n'exclut pas l'idée d'ajouter, par exemple, une enceinte fonctionnant avec Alexa à son installation, mais il faudra que ce travail supplémentaire soit utile et ne lui prenne pas trop de temps :

> « E16: Essayer, voir ce que ça donne, ce que je préfère... Voir les applications. Et puis elle peut gérer plein de trucs. Comment dire... tout n'est pas compatible. (…) il y a des fonctions qui... qui peuvent être doubles, avec plusieurs appareils, donc... Si après ça me demande pas trop de temps de configuration et d'installation, c'est tout bénef pour moi. » (entretien 10, 19 min)

E20 : aménager un lieu de vie qui n'est pas le sien

Un troisième cas de micro-aménagement domestique parmi les plus intéressants m'a été rapporté par E20, enquêtée très réticente aux enceintes connectées, et qui présente l'intérêt d'avoir imposé un changement de place d'une Google Home… ailleurs que chez elle :

> « JF: Ok. Et du coup pas de problème par rapport à toi ou par rapport à d'autres gens de... justement, de gêne par rapport au fait qu'il y en ait une.
> E20: Moi je lui ai demandé de la mettre dans le salon c'est là qu'on a découvert qu'elle marchait aussi quand elle le faisait dans le salon. Du coup je lui ai dit on peut la virer de la cuisine et juste la mettre dans le salon et en fait on a testé, ça marche aussi dans le salon donc voilà. » (entretien 13 ; 5 min)

Le premier élément intéressant est qu'elle a demandé le déplacement de l'enceinte au cours d'une soirée qu'elle passait à deux chez une amie, avec pour objectif explicite de se trouver hors du phonotope captable par l'enceinte. Installées dans la cuisine, elle espérait que la déplacer au salon préserverait leur bulle d'intimité, au moins dans l'espace de la cuisine. La

raison pour laquelle elles n'ont pas simplement coupé l'enceinte n'est pas tout à fait claire. D'un point de vue strictement pragmatique, on peut supposer qu'elles écoutaient de la musique en fond sonore, et qu'il était acceptable de recevoir le son produit par l'enceinte à condition que le son de leur conversation ne soit pas lui-même capté par les micros de la Google Home. Il semble que la volonté de tester la capacité de l'enceinte à capter le son faisait aussi partie de la démarche : il fallait s'assurer que la manœuvre soit efficace, mais je fais également l'hypothèse qu'il y avait chez E20, formée en école d'ingénieurs, la volonté de faire une petite expérience de physique, un test mu par la curiosité de connaître les capacités de l'objet technique.

> « Là c'était une soirée nanas à deux tranquilles pénards, heu en fait quand je suis chez moi j'aime bien être chez moi. Là c'est une amie très proche, enfin chez elle je me sens chez moi, quoi. C'est vrai que quand je vais chez des amis, si on fait une soirée à vingt ou à même à quatre cinq dans un appart et si c'est pas quelqu'un que je connais pas, quelqu'un de très proche, je ne vais pas non plus lui parler de son enceinte. Je m'impose pas comme ça quoi» (entretien 13 ; 7 min 30 s)

Le deuxième élément intéressant tient au fait qu'elle ait osé faire cette demande hors de son propre domicile, et que cette demande ait été favorablement reçue par son amie. E20 en donne très explicitement la clé : « chez elle je me sens comme chez moi ». Quoiqu'elle ne soit pas une résidente de l'appartement où elle a effectué ce menu réaménagement, elle en est une habitante privilégiée du fait de l'intensité de sa relation amicale avec la résidente effective. E20 complète même en expliquant qu'elle ne se serait pas permis cette demande chez quelqu'un qui ne soit pas « très proche ». Pour affiner encore l'analyse qu'elle fait de la situation, elle n'aurait pas non plus fait la demande dans un contexte social plus festif (« même à quatre cinq dans un appart »), sous-entendu dans l'appartement même de cette amie, mais avec d'autres personnes : dans ce cas, elle aurait eu le sentiment de « s'imposer ». Cette attitude à la fois pragmatique (elle tient compte de l'ensemble de la situation, et pas seulement de ses principes personnels) et sans doute un peu désabusée (elle rapporte ailleurs ne pas sentir un grand intérêt de la plupart des personnes qu'elle fréquente pour les questions de vie privée) se retrouve d'ailleurs plus tard dans l'entretien à d'autres sujets.

En tout état de cause, il reste surtout intéressant de voir que l'enceinte connectée est un objet qui semble suffisamment remarquable pour qu'une personne ne vivant pas dans un appartement ait pu justifier des capacités de l'enceinte pour demander son déplacement dans une autre pièce, exigence qui ne peut s'envisager que pour un nombre très restreint d'objets.

Le majordome numérique

Une fois effectué le micro-aménagement consistant à installer une enceinte connectée chez soi se pose la question de savoir quels vont être les effets produits par l'enceinte et sa présence anthropomorphe dans la gestion de la vie et des espaces du quotidien. De ce point de vue, le rôle que prend l'enceinte dans l'espace du domicile s'inscrit dans un continuum qui va de l'enceinte comme simple concierge à l'enceinte comme majordome ou gouvernante, voire comme membre de la famille.

Les fonctions de conciergerie sont les plus simples, et elles se retrouvent d'ailleurs dans les fonctionnalités des Concierge Bells qui, en une pression sur leur bouton d'activation, allument ou éteignent les luminaires et ouvrent ou ferment les volets. D'autres fonctionnalités spécifiques à certaines enceintes relèvent de rôle de conciergerie, comme pour les enceintes utilisant Alexa et qui permettent de prévenir leur utilisateur de l'arrivée de colis Amazon dans sa boîte aux lettres. Les enceintes Echo affichent les notifications d'expédition ou de réception des colis Amazon par un allumage de leur diode en orange, et le choix d'assigner un signal lumineux remarquable à cette fonctionnalité est révélateur du fait qu'elle est jugée importante et différenciante pour Amazon, qui s'intègre au quotidien des personnes non seulement par ses services logiciels, mais historiquement d'abord par son service de livraison. Avec un petit effort de configuration supplémentaire, il est possible aussi de demander une course en taxi ou VTC ou d'avoir des informations sur le trafic vers son lieu de travail, en plus des informations plus générales comme la météo du jour.

À un niveau supérieur d'intégration à la vie quotidienne associée dans le logis, il est possible d'accorder davantage de rôles aux enceintes pour la gestion des activités domestiques. Cela peut passer par la création de scripts par l'utilisateur, comme le déclenchement de la radio ou l'activation de la machine à café à la première interaction avec l'enceinte les matins de semaine. Cette capacité à créer des scripts intégrant des actions aux routines quotidiennes des habitants peut même être déléguée à l'assistant connecté. C'est du moins l'ambition de la fonction Hunches d'Alexa, à travers laquelle Amazon ambitionne de laisser prendre des décisions sans validation préalable de l'utilisateur[557] : on peut par exemple imaginer qu'un assistant prenne l'initiative de chauffer la salle de bain peu avant le réveil d'un utilisateur qui se doucherait habituellement le soir, mais dont l'enceinte aurait constaté qu'il ne l'aurait pas

[557] E. H. SCHWARTZ, « Alexa Can Now Adjust Your Smart Home Devices Without Needing to Ask Permission », sur *Voicebot.ai*, 26 janvier 2021 (en ligne : http://voicebot.ai/2021/01/26/alexa-can-now-adjust-your-smart-home-devices-without-needing-to-ask-permission/ ; consulté le 26 juin 2021)

fait la veille. Ces fonctionnalités d'apprentissage et de prise de décision autonomes sont encore plutôt à l'état de scénarios prospectifs pour la plupart des utilisateurs par le simple fait qu'elles requièrent une installation domotique connectée importante pour prendre tout leur sens : pour la plupart des utilisateurs qui possèdent juste quelques ampoules connectées, l'effet au quotidien sera minime. Il n'empêche que la fonctionnalité logicielle est déjà déployée depuis la fin 2021 aux États-Unis en ce qui concerne Hunches, et qu'elle constitue la nouvelle phase de développement de l'intégration de la domotique connectée au quotidien de ses utilisateurs : l'enceinte sera à terme amenée à jouer le rôle d'un véritable majordome, compris comme un domestique attaché à un maître dont il connaît les habitudes et gère le quotidien.

Si ces constats valent pour les enceintes connectées, il est nécessaire de rappeler que l'ambition des assistants connectés est plus large. Ils visent à s'intégrer au quotidien de leurs utilisateurs d'une manière extrêmement fine, et le phénomène dépasse largement le cadre domestique. Si Amazon a une stratégie plutôt axée vers le logis, stratégie dont l'acquisition de la marque d'aspirateurs-robots connectés iRobot à l'été 2022 est l'indice révélateur le plus récent[558], la logique générale des assistants est plutôt d'accompagner un devenir-cyborg axé sur l'augmentation des individus eux-mêmes, et déjà largement initié avec le développement du *smartphone*[559]. Un exemple simple permet de l'illustrer dans une communication de Google à destination de ses utilisateurs, reçue sur ma boîte électronique personnelle – et considérant que je n'étais alors pas équipé d'un Google Home, mais seulement d'un smartphone Android (voir Figure 31). Il s'agit d'une forme d'information ou de rappel sur les manières d'utiliser l'assistant vocal de Google, *a priori* plutôt pour un utilisateur de smartphone. Seuls trois items sur six choisis par les communicants de Google s'inscrivent peu ou prou dans l'espace domestique : très nettement pour le « 2 : Ajoute du jus d'orange à ma liste de course », et dans une moindre mesure pour le « 5 : Lance un minuteur de 20 minutes » (qui aurait pu être illustré, par exemple, par une personne faisant la cuisine, mais présente ici un personnage travaillant sur ordinateur, et qui pourrait être chez lui comme sur son lieu de travail) et le « 6 : Active le mode ne pas déranger » (là encore, illustré par deux personnes prenant une collation, et qui pourraient aussi bien être à domicile qu'à l'extérieur). Deux autres items sont plutôt fondés sur la logique

[558] Anon., « Amazon veut racheter iRobot, pour 1,7 milliard de dollars », *Next INpact*, 8 août 2022 (en ligne : https://www.nextinpact.com/lebrief/69771/amazon-veut-racheter-irobot-pour-17-milliard-dollars ; consulté le 28 août 2022) ; H. HADERO, « Amazon keeps growing, and so does its cache of data on you », *Los Angeles Times*, 23 août 2022 (en ligne : https://www.latimes.com/business/story/2022-08-23/amazon-keeps-growing-and-so-does-its-cache-of-data-on-you ; consulté le 28 août 2022)

[559] T. SARDIER, *Du quartier topographique au quartier topologique : Comment smartphone et réseaux sociaux redéfinissent la notion de proximité.*, mémoire de master 2, Lyon (France), ENS de Lyon, 2014

de rappel, avec la mémorisation d'un code de cadenas (le 3) et une notification pour un anniversaire d'un membre de la famille (le 4). L'item 1, qui illustre le début du courriel, présente les situations dans lesquelles l'assistant de Google peut être activé, à savoir en ramenant des courses chez soi, à vélo, ou en emballant un petit cadeau : l'idée est sans doute simplement ici d'insister sur le fait que l'assistant Google est toujours à portée de voix, y compris les mains prises, le smartphone du personnage étant posé sur une table dans deux cas, et fixé à un brassard dans l'autre. Au bout du compte, ce petit extrait de la communication de l'entreprise permet de mettre en perspective notre discours sur les assistants vocaux activés à travers une enceinte en rappelant que ce mode d'interaction s'inscrit dans une stratégie qui dépasse largement ces objets ou l'espace strictement domestique. Même si les enceintes connectées visent d'abord ce type d'espaces, c'est bien l'ensemble de l'espace et des pratiques quotidiennes que des entreprises comme Google ou Amazon cherchent à augmenter.

Figure 31 - Exemple de communication adressée par Google à un utilisateur relativement à son assistant personnel (III/2022)

Un dernier point, pour l'heure tout à fait hypothétique, que l'on peut enfin soulever ici est que, si aménager son logis avec des enceintes et objets connectés permet sans doute de s'approprier davantage son lieu de vie et que l'augmentation du confort contribue sans doute à renforcer l'attachement au lieu, on peut aussi envisager que certaines pratiques permises par cette assistance numérique tendent à nous rendre indifférents à notre logis. Évoquer la figure du concierge comme le fait explicitement l'entreprise éponyme, c'est ramener à l'imaginaire de l'hôtel et des lieux de vie dépersonnalisés, dont la gestion est déléguée à d'autres dans une relation commerciale asymétrique bien décrite par Dominique Boullier : « Dans certains cas, cependant, la conception des logements peut empêcher d'habiter, ou tout au moins le rendre très difficile. Ces situations sont ordinaires d'ailleurs, comme lors de notre séjour à l'hôtel, où tout le pouvoir d'agir est largement asymétrique en faveur de l'hôtelier et du bâtiment qui nous est attribué provisoirement », espace dans lequel, en conséquence, « nous ne faisons que loger, sans pouvoir réellement nous approprier la chambre. »[560] Ainsi, en nous libérant, par exemple, de contraintes ménagères comme le fait de passer l'aspirateur ou de s'assurer que volets et portes d'entrée sont bien fermées, il n'est pas exclu de penser que ces nouveaux dispositifs nous détachent quelque peu que ce soit de nos lieux de vie. En y supprimant certaines habitudes, la domotique connectée pourrait ainsi diminuer notre sentiment de les habiter.

II - MAITRISER SON DOMICILE DEPUIS L'EXTERIEUR

Si les enceintes connectées permettent une maîtrise de et dans l'espace domestique, leur connexion à Internet permet aussi de les contrôler depuis l'extérieur, ce qui constitue un changement majeur dans notre appréhension de l'espace privé, et tend à rendre plus poreuse la limite entre l'espace de l'intimité domestique et l'espace extérieur de la vie sociale et publique.

Le domicile : des limites à la fois plus poreuses et plus fortes

« Dans les maisons les plus cossues, il y avait toujours une pièce "muette", depuis laquelle il était impossible de capter une quelconque donnée personnelle. »
François Houste sur le compte Twitter de @mikrodystopies le 26 août 2021

[560] D. BOULLIER, « Rendre le numérique habitable : l'habitèle », *op. cit.*, p. 2

En agençant sa domotique, l'habitant-aménageur doit bien évidemment s'appuyer sur les limites architecturales existantes de son logis, comme le mur qui clôt son phonotope, ou les cloisons qui limitent la portée d'une connexion sans fil. Au-delà de leur présence tangible qui organise l'espace géométrique du logement, ces limites s'en trouvent ainsi renforcées par les pratiques qu'elles permettent exclusivement dans ce lieu. Imaginons que les interfaces vocales se développent au point de devenir aussi ubiquitaires que les connexions de données : je pourrai considérer être un habitant ou un familier là où je peux parler à des enceintes, où je suis phoniquement habitant ou invité et reconnu comme tel, de la même manière que dans les lieux où j'ai un accès facile à une connexion de données en Wi-Fi. Sur un plan symbolique, la conscience immunitaire qu'ont les individus de ces limites explique en partie la sidération avec les publicités télévisées qui activent les enceintes : la voix diffusée par mon téléviseur n'est pas censée pouvoir activer mon domicile augmenté, elle n'y a pas été invitée, je suis censé être maître de mon intérieur. Il y a dans cette interaction imprévue comme une trahison, de mon téléviseur et/ou de mon enceinte, un sentiment de dépossession de mon propre aménagement intérieur, l'usurpation d'une clé de mon habitèle ou, en somme : une atteinte à mon immunité.

Ce sentiment est encore plus fort pour le phonotope que pour les objets connectés précédents. Si l'on reprend le cas du Wi-Fi, la question immunitaire était certes déjà de savoir à qui confier le code d'accès à mon réseau, mais le Wi-Fi traversant quelque peu les murs, il n'active pas symboliquement une limite aussi forte que l'enveloppe extérieure du logement, à savoir les murs d'enceinte, sol et plafond. Il fait plutôt prendre conscience du voisinage immédiat, dans la mesure où les portées efficaces des box Wi-Fi de logements proches tendent à se chevaucher. On peut facilement connaître le SSID des réseaux voisins (pour *service set identifier* , le nom identifiant le réseau), ne serait-ce qu'en cherchant à se connecter soi-même à son propre réseau. On peut en subir la nuisance à travers les interférences qui diminuent les débits de réseaux saturant un même volume d'air, et parfois aussi en tirer avantage pour partager à plusieurs voisins une même connexion. Pour autant, même les connexions Wi-Fi, grâce aux codes d'accès, constituent un point de repère du logement individuel. Un des marqueurs de la familiarité dans l'usage du Wi-Fi est d'ailleurs précisément le fait qu'il n'est pas nécessaire d'entrer un code dans les lieux que nous habitons régulièrement : le domicile, le bureau, une résidence secondaire ou le logement de familiers. Mais le Wi-Fi ne marque pas aussi clairement la limite du logis, comme l'explicite ici E14 :

> « E15: Ici, nous, chez nous, faut rentrer chez nous pour utiliser la domotique. En tout cas, avec l'enceinte ou... avec le, enfin avec le téléphone, non.

E14: Bah le Wi-Fi dans le couloir tu captes, hein.
E15: Oui.
JF: Oui.
E14: Ca m'arrive des fois d'ailleurs de... je sais pas, d'éteindre un truc... Je sais plus ce que j'ai fait l'autre jour en domotique, là. Dans le couloir. » (entretien 9, 57 min 30 s)

Ainsi, et malgré le fait que son conjoint voulait précisément expliquer que leur réseau informatique était bien isolé de l'extérieur (raison pour laquelle il se refuse par exemple à installer même une simple sonnette connectée), E14 montre bien que le Wi-Fi n'opère pas une distinction franche des espaces domestiques et communs.

A contrario, le phonotope captable pour une enceinte connectée est forcément égal ou inférieur au volume d'un logement, en l'état actuel des capacités techniques des microphones. En somme, il ferme pratiquement et symboliquement l'espace du logis sur lui-même davantage que les autres technologies sans fil utilisées dans le cadre domestique.

Plus largement, les limites pratiques de diffusion et de captation des technologies numériques domestiques, Wi-Fi ou phonotope captable par l'enceinte, participent et dépendent de la fonction immunitaire du mur, si l'on admet que « (…) les murs ne sont que la cristallisation de la distance »[561]. Ici, il s'agit d'une distance mise entre l'espace personnel des individus et l'espace qu'ils partagent avec d'autres. Or, les objets connectés actuels, pour être efficaces dans le lieu où ils sont déployés, sont aujourd'hui amenés à collecter toujours plus d'informations fines sur la configuration des lieux, informations qu'ils peuvent communiquer à des tiers. Une gêne forte a par exemple été exprimée, dans la presse comme par certains enquêtés, vis-à-vis de la question de la cartographie du domicile opérée, par exemple, par des aspirateurs-robots :

« E6: C'est comme les aspirateurs connectées, je sais plus qui m'a dit ça ? Si c'est Valou ou...?
E7: Ils collectent tes infos.
JF: Oui.
E6: Ils collectent les informations de ta maison en repérant la disposition, quelles pièces tu as, combien de m²... Et en gros, le constructeur peut savoir combien... Il le vend ensuite à des fournisseurs de meubles, par exemple, qui fait des pubs ciblées.
E7: (acquiesce) Ouais. Mais c'est tout publicitaire ?
E6: Ouais, tant que c'est publicitaire ça me dérange pas. Au contraire, même, ça m'aide à avoir des publicités ciblées que...
(…)
E7: Non, j'y pense, quand même ! Je me dis, bon, ça me saoule, enfin... Même si

[561] A. A. MOLES et E. ROHMER-MOLES, *Psychosociologie de l'espace*, *op. cit.*, p. 38

c'est pas grave, ça me gonflerait que mon aspirateur sache où je mets tous mes trucs, enfin... Parce que derrière moi je sais pas à qui il l'envoie, ce qu'il en fait, pour quelles pubs...
(entretien 3 ; 30 min)

E7 est particulièrement gênée par l'idée que son domicile puisse être cartographié, même si elle revient à la crainte assez simple du fait que ce soit utilisé à des fins publicitaires. Il est par exemple possible d'inférer les revenus d'une personne à partir de la superficie et de la localisation de son domicile, ou son style cognitif au nombre de ses meubles ou encore à l'encombrement ou à la saleté de son espace de vie. Pour son compagnon, le problème ne se pose pas vraiment tant que c'est consenti ; il n'a d'ailleurs rien contre la publicité ciblée si elle optimise ses pratiques de consommation. En revanche, il fait lui directement le lien avec un objet connecté qui lui déplaît nettement plus parce qu'il n'a pas eu le choix de son installation ou non : le compteur Linky de l'appartement qu'ils louent :

« E6: (interrompant) C'est comme ça (désignant le compteur sur le mur à côté de moi) .
E7: C'est comme le Linky.
JF: Ah, c'était ma question d'après ! (rires)
E6: Ca ça me gêne plus. Parce que ça on ne l'a pas demandé. Et pour le coup, ça ça m'embête beaucoup.
JF: Plus que le...
E6: Plus.
E7: Plus que le truc que t'as introduit toi-même, forcément tu... tu relativises.
E6: Tu peux savoir ce que tu lui dis. Aussi. Alors que ça pour le coup...
E7: (à E6) Ben tu sais pas, hein, imagine elle écoute en continu ?
E6: Au pire il y a le bouton Mute. Ou tu peux le débrancher.
E7: Oui, je suis d'accord.
E6: T'as le contrôle dessus. Ça t'as pas du tout le contrôle, et ça me gêne beaucoup. (E7 acquiesce) »
(entretien 3 ; 31 min)

C'est d'abord et avant tout la question du consentement qui justifie sa défiance envers l'objet : il croit n'avoir « pas du tout le contrôle » sur les données collectées et transmises par cet objet connecté particulier, et n'a pas choisi de l'installer lui-même. Il n'y a pas d'atteinte immunitaire en soi : le Linky installé chez lui communique sans doute infiniment moins d'informations pertinentes à son égard que ses objets connectés, enceinte en tête, mais c'est bien la transmission de données de l'objet qu'il n'a pas choisi d'installer qui constitue pour lui une atteinte immunitaire :

« E6: Le fait qu'on m'ait imposé ça, alors que je suis locataire. Bon, je suis pas propriétaire. Déjà c'est moins pire.
E7: Les propriétaires on leur impose bien aussi.
E6: Oui si t'es une petite session (?) . Moi ce qui me gêne vraiment c'est que t'es arrivé là, t'as ça qui te piste, tu peux rien y faire. Ça ça m'embête.
JF: (petite pause) Mais... pour le coup, le... l'argumentaire se tient aussi. Pourquoi ils installent des trucs comme ça, c'est pour mieux organiser la charge sur le réseau etc. (ils acquiescent) Donc la raison est... je pense qu'elle est recevable.
E6: La raison elle est...
E7: C'est comme quand on te piste avec ta carte Navigo (intéressant, elle serait de région parisienne ?) , enfin...
E6: Google Maps.
E7: ...ta carte de transport, ou...
E6: Ouais, je sais pas... (ils se coupent la parole)
E7: Après est-ce qu'on doit tous être contents quand même, je sais pas, quoi.
E6: En tout cas ça me plait pas, Linky. Je dirais pas que je suis mécontent, mais je suis, suspicieux, quoi.
JF: Oui, tu le regardes pas d'un bon œil, le... (le boîtier)
E6: C'est ça. Je l'aime pas trop, quoi. » (entretien 3 ; 32 min)

Même l'évocation des bénéfices sur la gestion du réseau électrique et les économies d'énergie, qui pourraient séduire E6, ne suffisent pas à le convaincre du bien-fondé de l'installation d'un Linky sans son consentement explicite. Il mobilise la question de son statut de locataire dans cette gêne : cela indique que lui aussi a un rapport pour ainsi dire protecteur vis-à-vis de son domicile, malgré sa grande libéralité dans la diffusion de ses données personnelles en général, et qu'il semble estimer que ses prérogatives de résident sont bafouées par l'installation d'un compteur de ce type, parce qu'il serait locataire et non propriétaire. Ce réflexe de distinguer entre statut de locataire et de propriétaire est intéressant précisément parce qu'il ne tient pas, comme sa compagne le lui fait remarquer (« Les propriétaires on leur impose bien aussi »), ce qu'il concède immédiatement : cette distinction parle en fait moins d'un statut ou de prérogatives légales que d'un sentiment de contrôle sur et dans son logement, et *in fine* de l'empêchement qu'il ressent dans sa construction immunitaire.

Il n'est donc pas important en soi de savoir à quel point les limites du domicile de l'ère numérique sont devenues poreuses que de savoir comment cette porosité peut être intégrée de façon satisfaisante par les habitants, et dans quelle mesure elle permet encore ou non les processus immunitaires nécessaires à l'habiter. Nicolas Nova fait une lecture proche de la manière dont le smartphone permet à la fois de s'ouvrir et de se protéger des interactions avec autrui : « Avec le thème de la bulle protectrice privative, j'ai ensuite souligné dans la partie six

la tension ouverture/fermeture liée à l'usage constant de ce dispositif qui le rend tant objet amplificateur de socialisation que bouclier protecteur contre les sollicitations hors-ligne ou en ligne. »[562] Cette même logique joue pour la domotique connectée, à ceci près qu'elle s'applique à l'espace domestique au sein duquel sont ancrés, contrairement au smartphone, l'enceinte connectée et ses périphériques domotiques.

Télécommander et télésurveiller l'espace domestique

L'augmentation des espaces domestiques par le numérique augmente la porosité de leur enceinte architecturale pour des tiers, comme l'entreprise de distribution électrique RTE *via* les compteurs Linky, ou un Google ou un Amazon *via* leurs enceintes connectées, mais elle réduit par la télécommunication la distance à l'espace domestique pour les habitants eux-mêmes. Si le téléphone permettait depuis plusieurs décennies la télécommunication avec les habitants d'un logement, la nouveauté introduite par la domotique connectée est de permettre désormais une télécommunication avec, pour ainsi dire, un lieu, ou plus prosaïquement avec des capteurs et des effecteurs présents dans ce lieu. Cette nouveauté permet ou renforce deux pratiques nouvelles vis-à-vis de l'espace domestique : il est désormais possible de le télécommander (grâce aux effecteurs) et de le télésurveiller (grâce aux capteurs). L'exemple le plus patent ici est celui de E15 et de ses quarante modules lui permettant de réguler l'atmosphère intérieure ou d'agir sur l'arrosage des plantes, l'approvisionnement en nourriture de la gamelle de son chat…

De ce point de vue, la domotique connectée peut engendrer des atteintes à la vie privée vécus sur le mode de l'atteinte immunitaire autant qu'elle peut renforcer les processus immunitaires d'appropriation et d'entretien des espaces domestiques. Les tendances ne sont pas mutuellement exclusives, y compris dans le discours et les pratiques d'un même individu. La volonté de contrôler et de veiller sur l'immunité et l'intégrité du domicile, y compris à distance, est même pour plusieurs enquêtés un des motifs de l'adhésion à la tendance à l'augmentation numérique du domicile. C'est par exemple le cas de E14, qui explique :

> « E14: On voit si les fenêtres sont ouvertes ou pas, ça peut être intéressant, l'autre jour on se demandait si on avait bien fermé la fenêtre de la chambre en partant.
> E15: Du coup on peut vérifier.
> E14: On peut vérifier.»
> (entretien 9, 9 min 15 s)

[562] N. NOVA, *Figures mobiles: une anthropologie du smartphone*, *op. cit.*, p. 267

Même lorsque ces pratiques de surveillance, chez eux très poussées, ont mené à des moments d'inquiétude du fait de faux positifs renvoyés par leurs capteurs d'inondation et de chaleur, ni E15 ni E14 ne les ont remises en question :

> « E15: Moi ce qui m'avait fait peur c'est le détecteur de, d'inondation, qui disait qu'il y avait une... température, heu... extrêmement élevée, et que c'était anormal.
> E14: Après je sais pas si...
> E15: (interrompant) Et j'étais au boulot, donc là...!
> E14: ...sur l'enceinte connectée ou sur la domotique ?
> JF: Ca peut... oui.
> E14: Les deux, okay.
> JF: Mais c'était faux (à E15) .
> E15: (acquiesce)
> E15: Heureusement que du boulot je vois l'appart ! (rire) S'il y avait de la fumée ! » (entretien 9, 13 min 13 s)

Comme ils le disent à plusieurs reprises, en évoquant notamment la situation de leur voisine, leur plus grande crainte est surtout d'être cambriolés. L'immixtion dans l'espace physique d'un logement dans lequel ils se sont visiblement beaucoup investis, que ce soit à travers leurs aménagements domotiques ou plus simplement l'ameublement et la décoration, est le principal risque qu'ils estiment devoir limiter. Étant entendu qu'ils n'ont pas de crainte particulière en termes d'exploitation de leur surplus comportemental par des entreprises privées, ou même de leurs géolocalisations respectives l'un par l'autre, la domotique connectée est pour eux plutôt un progrès qu'une régression (dans la posture critique) ou une inévitable concession (dans la posture pragmatique).

Cette tendance, si elle est minoritaire dans mon échantillon, est très probablement beaucoup plus forte en population générale. En témoigne le fait que l'un des principaux développements de la domotique à distance en France avant l'avènement des objets connectés et pilotables par Internet concernaient la pose de systèmes d'alarmes. Le groupe de recherche Habiter Demain 2000 (HD 2000) fondé par Gaz de France / Ouest en 1989 pour servir de démonstrateur et de lieu de test à proximité de l'université de Rennes[563], projet qui rappelle la *Aware Home* à bien des égards, a ainsi été rapidement racheté et intégré par le groupe Securitas, aujourd'hui devenu Verisure, et qui est la principale entreprise européenne en matière de sécurité domestique. Verisure alloue d'importants moyens à sa communication externe, et produit régulièrement de nouveaux spots publicitaires diffusés à des heures de grande écoute qui donnent à voir les leviers psychologiques sur lesquels elle agit pour attirer de nouveaux clients. Le trope de l'intrus nocturne effarouché par l'alarme est récurrent, de même que les images rassurantes de mise en communication avec les agents de l'entreprise. Mais à l'été 2020, au sortir du premier confinement de la population dans le cadre de l'épidémie de Covid-19, le discours mettait davantage l'accent sur la liberté de déplacement retrouvée… et le besoin concomitant de surveiller à distance un lieu de vie que nous nous étions habitués à avoir constamment sous les yeux. En somme, la surveillance est devenue le pendant sécuritaire du secteur commercial montant valorisant la vie quotidienne au domicile et le *cocooning* (voir « De la maison au cocon », p. 113).

Verisure est une entreprise spécialisée dans les alarmes de domicile. Elle est l'héritière de l'entreprise suédoise Securitas. Le siège international est aujourd'hui situé à Versoix, à proximité de Genève (Suisse). Présente dans seize pays en Europe et en Amérique du Sud, elle a quatre millions de clients. Le marché français est le deuxième du groupe avec 600 000 clients en 2022. La branche française a été créée à la suite du rachat d'une entreprise rennaise, Habiter Demain 2000, fondée en 1989 par le groupe Gaz de France/Ouest afin de piloter sa recherche en matière de domotique.

[563] D. SERRAND, « HD 2000 - Une "première" unique en Europe », *Réseau - Mensuel de l'innovation régionale*, décembre 1989, p. 1-2 (en ligne : https://www.espace-sciences.org/sites/espace-sciences.org/files/images/sciences-ouest/numeros/r_051_12_1989.pdf)

Par la télécommande et la télésurveillance que permet désormais la domotique connectée, il s'agit moins de surveiller que de télé-veiller-sur son lieu de vie, de s'assurer qu'aucun accident ou acte de malveillance n'y est en cours. En somme, il s'agit de se projeter par les sens, grâce à des outils de télécommunication et des capteurs, dans un espace dans lequel on ne peut être présent, pour s'assurer de sa bonne tenue de la même façon qu'en y étant physiquement. Mais il est évident que ces dispositifs de contrôle, même lorsqu'ils sont censés être tournés vers les lieux, peuvent aussi être tournés voire détournés vers leurs résidents.

Vidéoprotéger les siens

La surveillance du domicile comme espace n'est évidemment pas le seul aspect du télé-veiller-sur. Il peut s'appliquer aussi aux personnes qui les fréquentent – y compris de manière régulière, et pas uniquement en cas d'intrusion. Étonnamment, un cas très couramment évoqué par les enquêtés ne concernait pas des familiers humains, mais le ou les chats de la maison. Le cas est évoqué par E7, E14, E15 et E8 :

> « E7: Ils le développent aussi beaucoup avec les alarmes, aussi maintenant. Ils installent ton alarme, et aussi de quoi regarder...
> E6: Oui. Je sais pas trop quoi en penser.
> E7: T'as des trucs pour parler à ton chien ou à ton chat... » (entretien 3, 44 min 50 s)

E7 est la première enquêtée à évoquer ces dispositifs, dont elle sait par ailleurs qu'il ne s'agit pas uniquement de capteurs (pour veiller sur l'animal) mais aussi d'effecteurs (pour le nourrir à distance). Quoique très technophobe en général, je la sens initialement plus ouverte vis-à-vis de ce type d'objets connectés, avant qu'elle ne décrive la pratique comme relevant de la « psychose » quelques minutes plus tard (« ...ben oui mais en même temps le chat il survit tout seul, les chiens ils survivent tous seuls... Je crois que ça crée de la psychose encore de mettre des caméras... »). Chez E14 et E15, la pratique n'est pas seulement évoquée, mais bel et bien mise en place :

> « E14: Oui nous on en a une qu'on met dans la chambre plus pendant les vacances, plus pour filmer le lit et comme ça on voit que notre animal est vivant.
> E15: Vu qu'il est tout le temps dans le lit ! Quand on est pas là (rire) » (entretien 9, 12 min 35 s)

Ce petit récit, assez léger, les amuse visiblement. Il est tout de même à noter que, s'ils présentent la chose avec humour, cela signifie tout de même qu'ils disposent de deux webcams de surveillance si l'on tient compte de celle qui est dissimulée dans la pièce à vivre. Derrière

l'apparence de l'anecdote, on retrouve ici le sérieux profond avec lequel ils ont augmenté leur lieu de vie. Chez E3, enfin, le récit prend une autre tournure :

> « E3: En fait on avait réfléchi... alors c'était connecté mais pas avec cette intelligence-là, parce que quand on part en vacances on laisse nos chats et je me suis toujours posé la question... de mettre une caméra pour pouvoir surveiller ce qui se passe. Parce qu'on fait appel, soit à des amis, soit à des intervenants extérieurs, et du coup tu as toujours la crainte... est-ce qu'ils viennent vraiment ? En même temps quand tu reviens de vacances tes chats sont en bonne santé, donc tu sais qu'ils sont bien nourris. Mais tu te poses quand même des questions. » (entretien 1, 56 min 55 s)

La conversation part de l'utilisation d'une webcam pour veiller sur le chat, qu'ils ont visiblement envisagée eux aussi avec sérieux, avant de se rétracter pour les raisons déjà présentées – E3 a déjà piraté un système de vidéosurveillance dans une entreprise et ne fait pas confiance à ces dispositifs. Mais le fait réellement intéressant ici est que, s'il envisageait d'utiliser une webcam, c'était moins pour veiller sur les chats que pour surveiller les veilleurs des chats, « amis » ou « intervenants extérieurs » à propos desquels il a « toujours la crainte... est-ce qu'ils viennent vraiment ? ».

Nous retombons ici sur un vieux trope de l'installation de caméras domestiques. Le trope était par exemple déjà exploité dans un épisode de la série étatsunienne à succès *Malcolm in the middle* en 2000, épisode au cours duquel le jeune héros, embauché par une riche famille comme baby-sitter, finit par découvrir que des caméras sont dissimulées partout dans la maison – et que ses employeurs collectionnent des cassettes où sont enregistrées des passages où, se croyant seul, il se tourne en ridicule. Selon Janos Mark Szakolczai, « leur utilisation est devenue une caractéristique normative et bien intégrée de la vie quotidienne domestique »[564], du moins dans le contexte britannique. Cela semble aussi être le cas dans le contexte nord-américain, une nourrice interrogée sur cette pratique ayant par exemple déclaré : « À mes débuts, il était très étrange de voir une caméra dans une maison, et cela signifiait que la famille ne vous faisait pas confiance. Mais c'est devenu quelque chose d'extrêmement banal aujourd'hui »[565]. C'est sans doute moins vrai dans le contexte français, quoique des cas de mise en œuvre de cette pratique

[564] « *their use has become a normative and well-integrated characteristic of everyday domestic life* » (trad. pers.) *in* J. M. SZAKOLCZAI, « 'What have you caught?': Nannycams and hidden cameras as normalised surveillance of the intimate », dans *The Technologisation of the Social*, 1re éd., Londres (Royaume-Uni), Routledge, 2021

[565] « *Earlier in my career, it was very odd to see a camera in a house, and it meant that a family didn't trust you. But now it's become so much more commonplace* » (trad. pers.) *in* J. BERND *et al.*, « Balancing Power Dynamics in Smart Homes: Nannies' Perspectives on How Cameras Reflect and Affect Relationships », s. l., 2022, p. 691 (en ligne : https://www.usenix.org/conference/soups2022/presentation/bernd ; consulté le 10 août 2022)

ont été documentés[566]. E7, qui fait beaucoup de *baby-sitting* en plus de ses études, y est par exemple nettement opposée.

Nous pouvons, là encore, finir par le cas de E16 que nous avons déjà longuement évoqué. C'est finalement son père qui a renoncé à utiliser la caméra qu'il avait un temps installé dans le salon, avec l'accord de son fils. Si E16 n'était pas non plus enthousiasmé par la présence du dispositif (voir « Le voyeur numérique », p. 283), il n'y était donc pas formellement opposé. Dans la même séquence d'entretien, E16 évoque également de manière tout à fait compréhensive le cas d'une vieille patiente, également prise en charge par la société d'aide à domicile qu'il emploie, à proximité de Lyon, et dont le fils travaillant en Suisse recourt d'autant plus à la veillance-sur électronique qu'il est le plus souvent loin de sa mère.

La serrure connectée : une réticence provisoire ?

Jusqu'ici, nous nous sommes intéressés à la relation entre capteurs et effecteurs à l'intérieur du domicile en ce qu'ils permettent une interaction avec les habitants depuis l'extérieur de leur domicile. Il existe cependant un type particulier d'effecteurs qui présente un cas-limite : la serrure connectée. Là où les autres objets connectés interrogent la porosité des murs d'enceinte du logis, la serrure-connectée en conditionne littéralement l'ouverture et la fermeture. Elle ne permet pas seulement le transfert d'informations à travers les murs sous forme de captats ou d'ordres, mais elle peut ouvrir ou fermer physiquement l'accès au lieu. La serrure connectée est un cas tout à fait singulier parmi les objets connectés en ce qu'elle commande un dispositif tout à fait singulier lui aussi dans l'espace domestique : la porte d'entrée, et donc le seuil de l'appartement ou de la maison. Jean-Marc Besse en propose une description stimulante :

> *« Les seuils, on le voit, sont les lieux d'une sociabilité particulière. S'y effectuent les rituels de l'accueil et de la prise de congé, propres à l'hospitalité. Mais s'y déroulent aussi les rites de voisinage, qui vont du bavardage à l'entretien en commun d'un chemin, d'une haie, d'un fossé, d'un trottoir, ou des parties communes d'un immeuble. Ni totalement extérieur, ni totalement intérieur, le seuil est une zone de transition. En tant qu'il permet de régler les bonnes distances et les bonnes proximités, il est, précisément, une figure de ce que j'ai appelé plus haut l'espacement*

[566] OUEST-FRANCE, « La baby-sitter maltraitait l'enfant : les parents posent des caméras pour la filmer », *Ouest-France*, 1er août 2011 (en ligne : https://www.ouest-france.fr/europe/france/la-baby-sitter-maltraitait-lenfant-les-parents-posent-des-cameras-pour-la-filmer-72017 ; consulté le 29 août 2022)

habitable. Entre l'espace privé et l'espace public, le seuil est l'une des premières conditions spatiales concrètes et symboliques de la rencontre humaine.

Mais surtout, le seuil est un bord. Un double bord. Être sur le seuil, c'est être au bord de l'espace privé, d'un côté, et de l'espace public et ouvert, de l'autre. [p. 53] En ce sens, il possède deux fonctions symétriques. D'une part, le seuil est comme un sas ou un tampon qui a pour but d'amortir le passage d'un espace à l'autre (…) [D'autre part, le seuil est aussi une zone de départ vers l'extérieur] »[567]

Reprenons les points saillants de cette définition de Besse pour explorer les conséquences identifiables à l'augmentation d'un tel type de lieu :

1. Comme « lieux de sociabilité », les seuils augmentés d'une serrure connectée créent un nouvel interlocuteur pour les visiteurs. L'intérêt pour le résident est de pouvoir interagir avec l'extérieur sans s'y exposer, comme le permettent déjà les interphones dans une moindre mesure, mais surtout de déléguer les « rituels de l'accueil » à un tiers logiciel. Ici, la serrure connectée, *a fortiori* si elle est équipée d'un assistant vocal ou si elle peut porter la voix d'un assistant vocal, joue pleinement le rôle de concierge. Il n'est d'ailleurs pas étonnant que le dispositif soit aujourd'hui généralisé, sous une forme rustique fondée sur l'usage de cartes à puces, sur les portes de chambres d'hôtel ;

2. Plus trivialement, équipant le « double bord » entre espace privé et espace public, la serrure connectée, on l'a vu, peut contrôler le passage de l'un à l'autre en actionnant le verrou de la porte ;

3. Enfin, si le seuil est « un sas ou un tampon », il ne l'est pleinement que lorsqu'un habitant est là pour actualiser cette fonction du lieu, qui ne reste sinon qu'en puissance : une porte fermée et qui n'est pas susceptible de s'ouvrir ne fait pas du seuil un sas, elle joue à plein son rôle de barrière, et ne reste qu'une continuation des murs qui bordent ses montants. Or, on va le voir, les serrures connectées actuelles sont généralement conçues en association avec une webcam, qui augmente considérablement l'intérêt du seuil comme sas dans le cas, par exemple, de la livraison à domicile.

[567] J.-M. BESSE, *Habiter*, *op. cit.*, p. 53-54

Paradoxalement, c'est une enquêtée dans l'ensemble technophobe qui est parmi les plus convaincus de l'intérêt d'une serrure connectée. Lorsque nous évoquons la question de la serrure connectée associée à la vidéosurveillance telle qu'elle est pratiquée par Amazon pour ses livraisons, E7 est particulièrement diserte. Cette séquence sur les serrures connectées est d'ailleurs l'une des plus longues d'un seul tenant lors de l'entretien 3, durant près de dix minutes sur les 2h15 totales. D'une part, elle identifie immédiatement la pratique malgré la formulation laborieuse de ma question, remarquant que cela se fait déjà aux États-Unis. Mais surtout, E7 résume en une tirade l'ambivalence de la question :

> « E7: Non, parce que... le concept est pas idiot non plus. On se fait livrer ses courses, même pour le AirBnB (petite pause, le rapport des arguments présentés par les fabricants ont fait mouche) Je sais pas. T'as plus de propriété privée, c'est tout ! (rire) Enfin si parce que tu surveilles quand même. » (entretien 3 ; 39 min 20 s)

Elle commence, comme souvent, par marquer une très forte réticence au dispositif. Pourtant, après que je lui ai présenté quelques-uns des arguments des fabricants, comme le fait qu'une serrure connectée associée à la vidéosurveillance du pas de porte facilite grandement certaines opérations, comme les livraisons ou l'ouverture des appartements de location, elle s'ouvre davantage à cette possibilité technique. Immédiatement, elle se reprend, arguant que ce serait la fin de « [sa] propriété privée », le contrôle de l'ouverture de son domicile lui semblant en effet un marqueur crucial de possession ou de jouissance des lieux. Elle finit néanmoins sur un deuxième contre-pied : puisque la surveillance de l'ouverture reste possible pour l'occupant principal de l'appartement, qui a la haute main sur l'activation de la serrure et surtout sur la captation vidéo du pas de porte, alors la remise en cause de la « propriété privée » ne lui semble pas si complète. E7 ne pousse pas la logique jusqu'au bout, mais son cheminement de pensée assez rapide me semble bien illustrer l'idée que les pratiques liées à la domotique connectée peuvent renforcer l'appropriation par leurs habitants des espaces domestiques.

L'adhésion de E21 au concept est moins surprenante. Il s'agit pour elle, comme toujours, de maximiser le « confort », de simplifier tous les processus en automatisant ou en déléguant à des machines ce qui peut l'être pour libérer du temps humain à des fins plus épanouissantes :

> « E21: (interrompant) Si techniquement c'est faisable, et qu'on peut enregistrer la voix bien sûr dans les paramètres sécuritaires pour que tout le monde ne se fasse pas cambrioler etc., moi je trouve ça excellent. C'est ce que je te disais tout à l'heure : tout ça c'est pas des tâches qui sont nécessaires d'être... humaines. Voilà : pourquoi

faire se déplacer quelqu'un pour donner les clés, aller ouvrir etc. (sur un ton de lassitude) , si on est capables de donner les clés à distance, pourquoi ne pas le faire. Ça nous permet nous d'avoir ce temps-là pour faire des choses intéressantes. » (entretien 14, 1 h 44 min)

Sa première réaction est marquée par l'exemple que je lui ai donné plus tôt, à savoir l'ouverture d'un logement hôtelier de type AirBnB. Elle avait d'abord pensé aux serrures connectées des voitures – en fait, plutôt des télécommandes – et lui donner un exemple plus précis était nécessaire pour recentrer son propos. Pour autant, on peut faire l'hypothèse que, dans son cas, il n'y a pas de spécificité à ce que sa porte d'entrée soit commandée par une serrure connectée plus que sa portière de voiture par une télécommande. Elle prend la précaution oratoire de rappeler que les « paramètres sécuritaires » doivent être solides, mais elle ne prolonge pas du tout cette réflexion.

A contrario, les autres enquêtés les plus technophiles et les plus compétents en matière informatique sont, eux, nettement plus réticents quant aux serrures connectées. Ni E3 et E4, ni E14 et E15, ni E8 n'envisageaient d'en installer une au moment de leurs entretiens. Le ratio bénéfice / risque est trop mauvais selon eux entre la possibilité de se faire *hacker* et l'enjeu à protéger, à savoir leur logement :

« E3: Après il y a déjà eu des preuves que c'est pas sécurisé complètement...
E4: ...ouais...
E3: ...ça a déjà été hacké...
E4: ...moi j'aurais peur de ça.
E3: Et autant hacker mon enceinte pour qu'on m'écoute, alors là je me dis mais vas-y, si t'as que ça à faire dans ta vie (en blaguant) . Hacker mon enceinte pour écouter ma vie, que le soir on va regarder Pékin Express, ben franchement c'est cool, tu t'es amusé. Mais ça va rien changer à ma vie. Mais me hacker ma serrure, et du coup il rentre chez moi...
E4: ...pour cambrioler...
E3: ...là non, c'est beaucoup plus traumatisant. Gamin, j'ai vécu un cambriolage, gamin je l'ai mal vécu. Je pense qu'aujourd'hui je le vivrais mal aussi.
JF: Oui, bah oui.
E3: Donc serrure connectée...
E4: ...non.
E3: ...non. Pas en France. Peut-être dans des pays où, je sais pas, il y a pas de... violence, genre Nouvelle-Zélande et leurs 0,01% de criminalité. Je laisserais ma porte ouverte, du coup ! » (entretien 1, 52 min 25 s)

E3 reprend une réflexion qu'ils m'avaient déjà faite en substance sur l'innocuité du piratage de leur phonotope (« Hacker mon enceinte pour écouter ma vie, que le soir on va regarder Pékin

Express, ben franchement c'est cool, tu t'es amusé. Mais ça va rien changer à ma vie. », voir aussi p. 281, « L'image considérée comme plus critique que le son »), auquel il oppose le grand « [traumatisme] » que constituerait un cambriolage. Au-delà de la seule sécurité informatique du dispositif, on voit dans cet extrait et plus encore dans celui qui suit qu'ils sont aussi méfiants vis-à-vis du contexte social du pays dans lequel ils vivent :

> « JF: Et sur les serrures connectées, je sais pas si tu vois... Amazon Key...
> E3: Les serrures connectées... Ca me dérange plus, enfin, au sens où, en fait, bah potentiellement... Le concept est bon, dans l'idée...
> E4: ...pas pour la France.
> E3: Pas pour la France, oui.
> JF: Pourquoi pas pour la France ?
> E3: Bah parce qu'en France il n'y a que des racailles.
> E4: On est des voyous, les Français.
> [3056,8] E3: On est des latins. Les latins c'est des voleurs, par essence.
> JF: Parce que le principe, en tout cas pour Amazon, c'est... vous voulez dire par rapport au livreur qui entre ?
> E3: Par rapport au livreur qui entre, mais même. Oui.
> JF: Parce qu'il y a la caméra, quand même.
> E3: Alors je sais pas si tu t'es déjà fait livrer par un livreur Amazon.
> JF: Oui, ça m'est arrivé.
> E3: Amazon Logistics.
> JF: Heu... je sais pas.
> E3: Parce qu'en fait Amazon, ils ont leur truc, Amazon Logistics, et en fait ces livreurs-là, c'est des mecs qui sont dans des voitures banalisées, qui je pense arrondissent leurs fins de mois. Et franchement, quand... c'est ceux qui te livrent le soir entre 19h et 22h.
> E4: (rire gêné / moqueur un peu prolongé)
> E3: Et quand tu les vois les mecs, alors... Enfin, je dis pas que... c'est des racailles, mais franchement j'aimerais pas les croiser le soir tout seul, quoi. C'est, c'est... franchement c'est des mecs, ouf !
> E4: Après ça s'est toujours très bien passé. » (entretien 1, 50 min 30 s)

Sans préjuger de la validité de leurs réticences quant à l'honnêteté des livreurs d'Amazon Logistics, l'extrait a surtout pour intérêt de révéler qu'ils sont de fins connaisseurs du fonctionnement d'Amazon Key. Comme on l'a vu dans le troisième point de la définition de Besse, la porte définit autant une limite ponctuelle qu'un espace de transition, un « sas » entre l'espace extérieur et l'espace privé. C'est précisément ce type micro-spatial du seuil que la serrure connectée revivifie, *a fortiori* telle qu'elle est développée par Amazon. Pour cette entreprise dont le métier historique est la livraison à domicile, il est en effet très intéressant de

pouvoir permettre à ses livreurs d'entrer chez les particuliers pour y déposer des colis, colis qui ne risquent alors plus de devoir être ramenés à l'entrepôt ou d'être volés sur le porche en cas d'impossibilité de remise en mains propres – même si, pour E3 et E4, la différence culturelle serait trop grande pour transposer en France cette pratique désormais usuelle aux États-Unis.

Chez E14 et E15, la peur du cambriolage est là encore très présente, surtout du fait de l'expérience malheureuse de leur voisine. En ce qui concerne E14 plus spécifiquement, une volonté de sécuriser au maximum leur réseau informatique et l'accès à leur domicile transparaît plus nettement :

> « E14: Mais faut que ça soit blindé, le truc, en termes de sécurité, c'est comme la domotique ici, c'est mis à jour tout le temps, le système, normalement je, je leur fais confiance. Après on l'ouvre pas sur l'extérieur, à part sur des tunnels sécurisés, mais...
> E15: Bah, oui, si quelqu'un connaît le mot de passe, il peut fermer ou ouvrir les volets chez nous.
> E14: Ouais.
> JF: Ce qui est encore... pas si grave ?
> E14: (acquiesce)
> JF: Sauf si... la porte c'est quand même un truc, vous feriez plus attention...?
> [3403,4] E14: Moi, moi je ferais plus gaffe avec la porte, oui.
> E15: Bah la porte, oui. C'est plus... c'est... (il ne poursuit pas)
> E14: Par exemple la sonnette connectée j'y avais pensé, mais pour le faire il faut juste que je mette un module dans l'interrupteur dans le couloir et rien que ça ça me gênait, déjà.
> JF: Ah bon ? Pourquoi ?
> E14: Ouais je sais pas, je me dis le module, enfin... Fallait que j'ouvre l'interrupteur dans le couloir et que je mette le module, dedans. Pour relier la sonnette après, et après on reçoit la notif. Mais je me dis, après, voilà, si on arrive à... se brancher dessus, je sais pas...
> JF: Tu veux dire accéder au réseau, en interne ?
> E14: Ouais.
> JF: En passant par le...
> E14: Par le truc, ouais. Bon, après c'est peut-être pas fondé, hein. Mais... (petite pause) »

Il faut que la sécurité du réseau soit « blindé[e] ». Il transpose immédiatement la question de l'accès physique au domicile grâce à une serrure connectée à la sécurité des flux de données de leur IoT domestique, qui ne sortent de chez eux que par un « tunnel sécurisé », à savoir une connexion en VPN. De même, les micrologiciels de leurs appareils sont scrupuleusement tenus à jour, selon un principe de base de sécurité informatique. Dans cette perspective, installer un

module physique à l'extérieur de l'appartement puis le connecter à leur réseau ne le met pas du tout à l'aise. De fait, cela révèle un désir de sécurité particulièrement fort, d'autant plus intéressant qu'il contraste avec le fait que, à l'intérieur de l'appartement, la difficulté est plutôt de trouver un objet qui ne soit *pas* connecté. Il faut en outre signaler que nous parlons ici non pas d'une serrure connectée, qui permettrait d'ouvrir la porte d'entrée dans le pire des cas, mais bien seulement d'une sonnette connectée – le pire danger évoqué par les enquêtés en cas de piratage étant d'offrir la possibilité à un attaquant d'ouvrir et fermer à sa guise leurs volets roulants. Il va sans dire que leur réticence à l'installation d'une serrure connectée était, au moment de l'entretien, totale.

Chez E8 enfin, c'est plus prosaïquement l'idée qu'on puisse, tout court, entrer chez lui à la suite d'un piratage ou d'un « [bidouillage] » qui le rend méfiant vis-à-vis des serrures connectées :

> « E8: Non, là c'est un truc où j'hésite quand même beaucoup, parce que... enfin, je connais pas encore tout à fait le sujet.
> JF: (acquiesce)
> E8: Je ne me suis pas trop trop mis dessus. Heu... Ça reste électronique, donc... bidouillable.
> JF: Oui.
> E8: Là, pour le coup, j'ai... pour tout ce qui va concerner la sécurité de la maison en tant que telle, je suis un peu dubitatif.
> JF: Donc même le volet roulant, tu accepterais peut-être...?
> E8: Ouais, parce que le volet roulant... C'est juste pour le fermer ou l'ouvrir quand tu as des volets électriques comme ici. Je veux dire, ça ne sera pas... plus difficile ou plus facile à ouvrir, à soulever que...
> JF: Ouais.
> E8: Par contre, la serrure, si tu arrives à... à griller le Wi-Fi ou à avoir un truc, tu peux ouvrir sans souci, quoi.
> JF: (acquiesce) Tu connais des cas, ou c'est une crainte que tu as en général ?
> E8: Non, c'est une crainte. C'est une crainte. C'est plutôt une crainte. Je suis pas... j'ai pas suffisamment confiance pour ça. » (entretien 4, 10 min 40 s)

Ses formulations laissent davantage entendre une valorisation de la « maison » physique en soi. Ainsi, il ne considère pas que le piratage de son réseau d'objets connectés ou l'accès à son phonotope compromettent la « sécurité de la maison en tant que telle ». De même, il n'évoque pas le cambriolage, ou la possibilité de manipuler ses effecteurs – comme E15 évoquant la possibilité d'actionner leurs volets. À propos des volets, justement, E8 est là encore pragmatique : il n'est pas opposé à les connecter dans la mesure où ils sont déjà électriques, et

que les soulever (là encore, physiquement) ne pose pas plus, sinon moins, de difficultés que de tenter de les pirater.

En somme, la serrure connectée semble encore aujourd'hui plutôt décriée dans le contexte français. Il y a chez la plupart des enquêtés un attachement au contrôle sur les accès de leur domicile qui tempère l'enthousiasme de beaucoup des plus partisans de la domotique connectée. Tous les enquêtés ne sont cependant pas opposés au dispositif, en particulier E21, mais aussi E7 dans une moindre mesure. Il est difficile de dire s'il s'agit déjà d'un signal faible, mais il n'est clairement pas à exclure que les serrures connectées finissent par se répandre en France, quoiqu'à un rythme et avec un taux de pénétration inférieur à ce qui s'observe déjà sur le marché étatsunien.

*

Contrairement à d'autres objets techniques comme l'ordinateur personnel ou, dans une certaine mesure, le *smartphone*, les enceintes connectées et la domotique connectée contemporaines ont des fonctions bien balisées et dont il est difficile de sortir. Les configurations, spatiales comme logicielles, peuvent être extrêmement nombreuses ou très fines, mais les objets sont finalement beaucoup moins ouverts au détournement ou à des usages inattendus. Les trois principales raisons à cet état de fait sont la fermeture matérielle et logicielle des objets, la dépendance aux serveurs des divers fabricants et à leurs logiciels (surtout pour l'assistance vocale), et plus simplement l'interface vocale en elle-même qui introduit la contrainte de la vocalisation linéaire des commandes. Un bon indice de ces limitations est le fait que tous mes enquêtés utilisaient leur matériel de façon finalement assez conventionnelle, sans détournement de leur design initial, même quand ces enquêtés faisaient partie de milieux professionnels ou d'intérêt autour de l'ingénierie et du *hacking*. L'informatique ou Internet, *a contrario*, ont été développés de façon très ouverte, sans qu'on sache avec exactitude à quoi allaient servir ces infrastructures nouvelles. Et ce, en provoquant des réactions culturelles fortes et multiples : Fred Turner raconte avec détail comment l'informatique émergente au deuxième XXe siècle aux États-Unis a pu être d'abord être associée à la technocratie d'État la plus rigide avant de connaître son plein développement à travers les contributions des milieux communalistes des années 1970, en rupture de ban avec la société de leur temps[568].

[568] Il parle plus exactement de « contre-culture cybernétique », voir F. TURNER, *Aux sources de l'utopie numérique*, *op. cit.*, p. 89.

Aucune question de cette ampleur ne semble posée par les enquêtés, qui réagissent uniquement aux propositions qui leur sont faites par l'industrie elle-même. Ils peuvent être pour ou contre le fait de chercher à se faciliter la vie à travers une interface vocale et l'automatisation, ils peuvent être inquiets ou non des conséquences sur la vie privée des personnes, mais ils ne s'emparent pas pleinement de l'outil. En conséquence, il est d'autant plus important d'être attentifs aux discours et aux propositions des fabricants, qu'elles soient explicites ou implicites, pour bien comprendre quels effets sociaux sont recherchés et peuvent être attendus en matière de domotique connectée.

De ce point de vue, c'est la stratégie d'Amazon qui est aujourd'hui la plus remarquable. Si tous les acteurs jouent ici sur le désir d'assistance à la gestion de la vie quotidienne et participent au mouvement de revalorisation de la sphère domestique, Amazon va encore plus loin. Alexa et les autres produits de l'entreprise entraînent l'espace domestique vers le sécessionnisme des *gated communities*, et cherchent à accomplir l'idéal du domicile comme « une forteresse domestique irriguée par les services à domicile et le téléachat »[569]. Ce sécessionnisme ne s'étend pas seulement au domicile, du moins aux États-Unis pour l'instant, puisqu'il touche également les environs du domicile et le quartier environnant à travers les sonnettes et serrures connectées Ring et les partenariats avec les polices locales. Ensuite, il faut signaler qu'Amazon et Google/Alphabet se distinguent tous deux en matière de rapport aux données personnelles et aux profils numériques de leurs utilisateurs. Plus que chez Apple et pour les plus entreprises proposant des solutions d'assistance vocale locale, Amazon et Alphabet cherchent à travers leurs enceintes servant de *hub* à la domotique connectée à transposer leur hypercentralité sur Internet dans toutes les médiations de la vie quotidienne. Il ne s'agit pas seulement ici de maîtriser un espace physique, une atmosphère ou un phonotope[570], en somme d'un concierge ou d'un majordome. Il s'agit aussi désormais de capter les actions les plus banales mais aussi les sociabilités du domicile, en y introduisant comme un nouveau membre de la famille.

[569] M. LUSSAULT, *L'homme spatial*, *op. cit.*, p. 318

[570] Dans *Bulles*, Peter Sloterdijk développe son idée que la capsule spatiale est le cas-limite et le paroxysme de l'habitat contemporain, en insistant notamment sur le besoin de soutien à distance des astronautes dans les capsules spatiales.

Chapitre 4 - UNE NOUVELLE PRESENCE

« E21: Non, je pense que c'est plus le contact. D'être dans le contact, heu... humain, dans le toucher, et donc j'ai besoin de la sensation, de visualiser, heu... l'objet. J'ai besoin de... du matériel, encore. De le matérialiser. De la localiser. Ça me dérangerait qu'il soit dématérialisé, qu'il soit... comme ça, diffus (geste de la main vers la pièce) »
(entretien 14, 2 h 29 min)

Au-delà de la dimension technique de l'objet technique comme hub plus ou moins sophistiqué à l'interface des spatialités corporelles et numériques des personnes et des objets connectés avec lesquels elles cohabitent, la *présence* d'un objet doté d'une voix et de capacités conversationnelles au sein du logis pose la question de son statut social. De même qu'un majordome ou une gouvernante ne sont pas de simples effecteurs facilitant la vie de leur maître ou maîtresse comme des robots, les robots à proprement parler ne sont-ils pas eux-mêmes plus que de simples effecteurs aux yeux de leur utilisateurs ?

Nous verrons d'abord que la question d'une présence robotique ou informatique quasi humaine dans le logis est un vieux fantasme technique, déjà exploré par la science-fiction notamment, et qui est largement évoquée par les enquêtés. La domotique connectée actualise donc un motif récurrent de la littérature et du cinéma d'anticipation, et elle invite les individus à rejouer des postures oscillant entre le désir et la crainte vis-à-vis de ces technologies (partie I). Il nous faudra donc voir quels choix de design ont été faits au moment de donner une voix à un objet pour satisfaire ces attentes et apaiser ces peurs (partie II). Après avoir vu quelles formes prennent les interlocutions avec ces objets (partie III), nous verrons que leur fixité ne les engage pas moins dans des relations proxémiques avec les habitants qu'ils servent (partie IV).

I - UN FANTASME TECHNOPHILE EN COURS D'ACTUALISATION

Domotique connectée et science-fiction

Le motif d'une intelligence artificielle capable de converser en langage naturel avec des humains est ancien et récurrent, en particulier dans les univers de science-fiction. L'assistant connecté met en œuvre des idées, voire des fantasmes de machines anthropomorphes qui sont

très anciens[571]. Dans la science-fiction contemporaine, des références mobilisées par les enquêtés ont été à l'intelligence artificielle appelée Jarvis, qui équipe la maison et l'armure du super-héros Iron Man, ou encore à l'ordinateur HAL pilotant le vaisseau spatial du film *2001, l'Odyssée de l'espace*. E13 déclare même ouvertement :

> « E13 : (…) Oui moi j'attends un Jarvis, j'attends un Jarvis. C'est pour ça que pour l'instant il y a encore des étapes.
>
> E12 : le jour où ça, ça existe, là ! (il s'exclame) je commencerai à m'y intéresser plus sérieusement. Pour l'instant. Je surveille, mais… » (entretien 8, 13 min)

Il mobilise cette référence après une longue séquence ou lui et E12, pourtant technophiles, déploraient que les enceintes connectées et les agents conversationnels ne soient pas encore aussi sophistiqués qu'ils le voudraient. Précisément parce qu'ils sont technophiles et amateurs de science-fiction, leur attente vis-à-vis de la domotique connectée est beaucoup plus forte que ce que la réalité technique contemporaine rend possible. Dans leur cas, le fantasme se heurte à une réalité décevante. Malgré tout, et plus prosaïquement, les assistants vocaux intégrés dans des enceintes ou d'autres objets du mobilier actualisent le potentiel de l'*everyware*[572] et des « murs connectés »[573]. Et quoiqu'ils ne satisfassent pas encore aux attentes les plus fortes, ils n'en sont pas moins identifiés par les enquêtés comme les prémisses d'une actualisation de certains fantasmes technophiles.

La série de science-fiction britannique dystopique *Black Mirror*, très en vogue au moment de la campagne d'entretiens, est souvent évoquée aussi. Dire d'une situation qu'elle est « à la Black Mirror » est devenu synonyme d'un avenir indésirable ou effrayant, et en fait

[571] Pour l'Europe, on peut le faire remonter au moins au Turc mécanique de la fin du XVIIIe siècle, à savoir un pseudo automate de forme humaine prétendument capable de jouer aux échecs. En réalité, le Turc mécanique était une marionnette et non un automate, le meuble le supportant contenait un compartiment cachant un joueur humain.
[572] A. GREENFIELD, *Every[ware]*, *op. cit.*
[573] W. J. MITCHELL, *City of bits*, *op. cit.* ; R. KITCHIN et M. DODGE, *Code/space: software and everyday life*, Cambridge, Mass., Etats-Unis d'Amérique, MIT Press, 2014

bien souvent déjà en place dans notre société actuelle[574]. E8 l'évoque dans cette acception, par rapport aux questions de circulation et d'utilisation des données personnelles[575] :

> « JF: Donc ce que tu fais comme différence c'est que tant que ça reste, on va dire, de la proposition, ça va...
> E8: (interrompant) C'est ça.
> JF: ...mais si c'est de la coercition ou un truc imposé...
> E8: Exactement, exactement.
> JF: Et tu vois le parallèle, tu penses qu'on va aller vers ça, mais tu ne le souhaites pas, pour le coup ?
> E8: Ouais, pour moi on va aller vers ça, comme dans les séries comme Black Mirror etc., on va clairement aller dedans, c'est clair.» (entretien 4, 31 min 20 s)

Quand nous abordons quelques minutes plus tard la question de l'utilisation de l'utilisation des captats audios collectés par l'enceinte, en l'espèce dans le cadre d'une enquête de police, il évoque cette fois la figure de Big Brother et *1984*, le roman d'anticipation lui aussi dystopique de George Orwell :

> « JF: D'accord. Mais tu ne verrais pas un régime un peu comme la perquisition, qui permet à la police de rentrer dans ton domicile, mais pour tes données personnelles ? Ça te paraîtrait pas... Sous le contrôle d'un juge et tout, hein.
> E8: Ouais, c'est un peu 1984, là, Big Brother. Mais pour le coup ce serait plus du... Heu... Il y aurait une différence entre aller chez toi pouvoir saisir des affaires... Alors c'est déjà quelque chose qu'ils font, hein, quand ils saisissent des téléphones, des choses comme ça. Dans le cadre d'une enquête.» (entretien 4, 34 min)

Ces références sont souvent utilisées de manière assez peu précise, voire contradictoire, comme dans cette évocation de *1984* qui n'était pas la plus appropriée dans le contexte de la question : il s'agissait de savoir s'il voyait un problème spécifique à ce que les données personnelles produites par l'utilisation de la domotique, et notamment les captats audio, entrent dans le cadre des données accessibles par des enquêteurs diligentés par un juge. Dans *1984*, la situation est

[574] Comme le rapporte Jérémy Cornec à propos d'une fausse affiche de la série diffusée par des étudiants madrilène, et qui est en fait essentiellement couverte d'un matériau réfléchissant inscrivant directement notre monde dans le cadre dystopique de la série : « Les questionnements sur le devenir de l'espèce humaine et de la société contemporaine sont au cœur de l'actualité, et la fiction apparaît alors comme une réponse possible ou un point de départ pour une réflexion commune, en témoigne la campagne promotionnelle créée par des étudiants à Madrid, dans laquelle ils suggèrent que le monde actuel est devenu aussi dystopique que l'anthologie Black Mirror » *in* J. CORNEC, *Imaginaires de la dystopie et du posthumain dans les séries d'anticipation science-fictionnelles contemporaines (2009-2019)*, thèse de doctorat en langue et littérature anglophone, Brest (France), Université de Bretagne occidentale - Brest, 2021, p. 253

[575] Données personnelles qu'il distingue assez nettement de la vie privée en général, qui pour lui renvoie avant tout à la vie familiale en général, et qui se rapproche plus de la logique du cocon en ce qui concerne son espace domestique.

celle d’un État policier pouvant arbitrairement s’immiscer visuellement et phoniquement dans l’espace domestique au moyen du « télécran » de ses citoyens. Elles n’en révèlent pas moins que l’imaginaire général est largement nourri par ces références.

Une innovation désirée

Paradoxalement, c’est E5, l’enquêté le plus farouchement opposé aux enceintes connectées, qui décrit sans doute le plus finement le désir que peuvent susciter les nouveaux objets connectés quand je lui demande s’il pourrait concevoir d’acquérir une enceinte connectée. Il mobilise directement le registre du « fantasme » et de la « science-fiction » :

> « E5: (saisissant la balle au bond, vivement) Non ! D'un point de vue abstrait, ou extérieur, ou un autre objectif, ça peut avoir une attractivité. C'est un gadget, c'est un petit jeu... Il y a certainement, pour beaucoup, une réalisation d'un fantasme de la science-fiction depuis des décennies.
> JF: (acquiesce)
> E5: (courte pause) Un objet, une interface avec qui, avec la possibilité d'interagir en interface naturelle, le langage, qui saisit, qui répond et qui agit, surtout ; qui réalise quelque chose de physique, parce que ça c'est éventuellement la partie qui peut être la plus fascinante, c'est que ça sort du juste ordinateur.
> JF: Ouais.
> E5: Même si c'est du numérique, ça allume la lumière chez toi. C'est, c'est... pour ça, je vois que c'est un jeu quand même qui fait de l'effet. (…) »

Dès les premières minutes de l’entretien, il identifie les enceintes connectées comme un fantasme technophile issu de la science-fiction, puis propose une explication très pertinente à leur « attractivité » : elles ne seraient pas de « simples ordinateurs », au sens où elles ne permettraient que de manipuler de l’information numérique. Leur principal atout serait selon lui d’être des *hubs* domotiques permettant d’activer, à la voix, des objets physiques tels que des ampoules connectées. Dans le même temps, il évoque spontanément la dimension « gadget » de la chose, et déconsidère « le petit jeu » de la commande vocale. E5 est d’ailleurs catégorique quand je lui demande si, malgré tout, il ne serait pas séduit ou séductible lui-même :

> « (…) JF: Même pour toi ça pourrait être séduisant, au moins pour le côté gadget.
> E5: Non, non non.
> JF: Le côté gadget...
> E5: Non, ça ne m'intéresse pas du tout.
> JF: Du tout, du tout, du tout.
> E5: Non. Je vois pourquoi ça peut séduire.
> JF: Abstraitement, mais pas... okay.
> E5: Non. Moi ça ne m'intéresse pas. Eventuellement je pourrais dire "ah ouais, c'est

drôle", mais...»
(entretien 5 ; 11 min)

Il admet à la rigueur que la commande vocale a quelque chose de « drôle », mais insiste sur le fait qu'il n'y voit aucun intérêt pour lui-même. Outre sa problématique personnelle de défense de la vie privée, il n'y voit donc pas non plus d'intérêt pratique, quoiqu'il comprenne l'attrait des enceintes connectées chez d'autres personnes.

Cette vision de la domotique connectée comme incarnation d'un fantasme de science-fiction est également mobilisée par E17, jusque dans son discours de vente à des clients du magasin où il travaille. M'étant approché de lui et des deux clientes avec laquelle il discutait autour d'une boîte de Google Home, j'ai pu constater qu'il évoquait par exemple l'ordinateur Jarvis, également cité par E8, pour expliquer pourquoi de tels objets étaient à la fois attirants et repoussants (« c'est génial ! mais ça peut faire peur aussi »). C'est d'ailleurs ce discours en rupture avec une explication promotionnelle classique qui m'a incité à approfondir la question avec cet enquêté. L'intérêt de son propos était de comprendre ce qui faisait l'intérêt et la curiosité d'acheteurs potentiels, tout en leur faisant part des réserves possibles vis-à-vis de ces objets, dans une logique sincère de conseil technique. Il est à relever qu'E17 partage lui-même ce désir comme amateur déclaré de littérature et de cinéma de science-fiction :

« E17: Il y a toujours ce truc. (digression sur le magazine *Décroissance*) . Et souvent ce que je dis aux clients, c'est que la science-fiction devient réalité. Ça, j'adore cette formule. »
(entretien 11, 58 min)

Mais c'est donc aussi comme amateur de science-fiction qu'il exprime avant tout des craintes quant aux technologies numériques et à Internet – singulièrement vis-à-vis des enceintes connectées, dans l'extrait suivant :

« Mais, non, c'est que... j'ai trop lu de science-fiction, j'ai trop lu certaines publications, je... je sais. J'ai trop lu de... même pas seulement de la science-fiction, mais des, des gens qui s'intéressent à l'intelligence artificielle, ou DITE artificielle pour... pour ne pas en avoir envie. Maintenant je dis : si j'étais handicapé etc., oui, mais là, non. Ça ne m'intéresse pas.»
(entretien 11, 4 min 50 s)

Une innovation crainte

Si E17 partage ce désir pour les objets connectés, il a pendant longtemps aussi mis les potentiels acheteurs en garde sur l'utilisation qui sera faite des données qui seront produites à leur utilisation d'une enceinte connectée qui, selon lui, « peut faire peur ». Dans son discours

technique aux clients, il explique en effet que ce qui fait la force des enceintes, le profilage de leurs utilisateurs, peut aussi être un motif d'inquiétude. Lorsque je l'ai vu présenter une Google Home, il fait même le parallèle avec le moteur de recherche de l'entreprise, dont l'efficacité croit avec son utilisation – et qu'il trouve tout aussi « génial » quand nous l'évoquons par la suite en entretien. Les qualités perçues d'un dispositif comme une enceinte connectée lui semblent indissociables de contreparties qu'il lui semble nécessaire de connaître et de faire connaître. E17 refuse pour lui-même le *trade off* proposé par Google, malgré son désir pour le produit. Il me rapporte d'ailleurs dans notre conversation suivant cette vente qu'il n'a pas de *smartphone* pour les mêmes raisons, et malgré une certaine fascination pour cet objet. Entre cette prise de contact dans son magasin et l'entretien à proprement parler que nous ferons un an plus tard, il finit néanmoins par s'équiper d'un *smartphone* tant sa curiosité et son intérêt étaient grands. Il m'a par exemple rapporté avoir longtemps été fasciné par la propension de ses collègues à passer la moindre de leurs pauses sur leur *smartphone,* et dans son cas personnel ce sont les perspectives sociales offertes par cet objet qui l'ont convaincu :

> « Mais maintenant, là où j'ai... je suis moins, heu... (petite pause) moins virulent... (y compris dans son discours aux clients)
> JF: (acquiesce)
> E17: ...c'est que d'une part, j'ai un smartphone. Et ça change des choses. Dans mes habitudes. C'est-à-dire que j'avais des a priori. Par exemple, que ça coupe, heu... ça éloigne, qu'on s'éloigne. En fait, moi ça m'a rapproché avec ma famille qui est [à l'étranger]. Je les vois presque jamais, et avec WhatsApp, des trucs comme ça, on rit, on truc et ça rapproche. Donc déjà, je me dis "tiens, c'est pas ce que je...", voilà. » (entretien 11, 17 minutes)

Son intérêt pour la socialisation avec le *smartphone* transparaît aussi dans un moment de l'entretien où il me vante, très impressionné, la capacité de l'application Google Translate à traduire à la volée une conversation relativement complexe entre deux interlocuteurs s'exprimant chacun dans sa langue. Il est intéressant de noter que son utilisation d'un *smartphone* a fini par tempérer ses réticences envers les enceintes elles aussi, comme par contagion, sans qu'il aille jusqu'à envisager de s'en équiper, et quoiqu'une partie de sa famille dispose de Google Home – mais ce dernier désir semble chez lui plus facile à réfréner que celui pour le *smartphone*. Au bout du compte, il résume lui-même la dichotomie entre crainte et désir dans laquelle il se trouve :

> « Donc je suis quand même... je trouve ça à la fois, "j'en veux pas", et à la fois je sais que je suis fasciné, je le sais.
> JF: Oui.

E17: Et je sais que si je l'avais je voudrais... (il commence à rire)
JF: Qu'elle fasse tout et...
E17: Qu'elle fasse tout ! Qu'elle... (il repart d'un rire) Je suis horrible ! Je suis contradictoire ! Entre ça et cette... Voilà. » (entretien 11, 33 min)

Quant aux potentiels acheteurs d'enceintes connectées auxquels il a tenu son discours dans sa version plus « virulente », il me rapporte en entretien qu'aucun n'en a jamais été dissuadé de cet achat.

On retrouve la dichotomie d'E17 chez E7. Elle ne la verbalise pas aussi clairement, mais le paradoxe en filigrane revient tout au long de l'entretien : l'affirmation véhémente de sa « technophobie » ou de son « côté réac », qu'elle remet néanmoins assez facilement en cause lorsqu'elle passe d'un discours général sur les technologies de la *smart home* à une réflexion plus pratique sur les usages qu'elles permettent. Le plus intéressant dans son cas est que ce balancement s'exprime plus particulièrement en parlant des serrures connectées. On a vu que ces dernières étaient encore aujourd'hui le dispositif-limite à propos duquel même les enquêtés les plus enthousiastes exprimaient des réticences (voir « La serrure connectée : une réticence provisoire ? », p. 359). Elle-même commence plutôt par dire qu'elle est contre par principe :

« E7: A voir si ça se développe à quoi ça ressemble. Mais là comme ça... Je trouve pas ça très intéressant et j'aimerais pas l'avoir, en tout cas. (rire un peu gêné) » (entretien 5, 39 min 35 s)

Son compagnon, qui a plutôt un profil technophile et ouvert à de nouvelles pratiques numériques, est quant à lui réticent tout le long de cette séquence d'entretien : avec le compteur connecté Linky, c'est un dispositif-limite pour lui. Pour Linky, c'était le fait qu'il soit imposé aux locataires qui lui déplaisait. Pour la serrure connectée, il est dans le registre déjà identifié de résistance immunitaire et de *cocooning*. E7 est visiblement partagée durant la séquence, expliquant que cette défense immunitaire stricte du foyer vaut moins pour elle – elle déclare qu'elle pourrait envisager de mettre leur appartement en location temporaire sur AirBnB. Sa posture d'opposition s'infléchit assez vite :

« E7: Ouais, moi aussi mais j'aime pas trop mais je sais pas trop pourquoi, j'arrive pas à conceptualiser. J'ai vu des reportages sur des gens qui livrent des courses pendant que t'es pas là... (elle pouffe et ne finit pas vraiment sa phrase) » (entretien 5, 42 min 30 s)

Elle verbalise ici les conditions dans lesquelles le *trade off* de vie privée pourrait lui sembler acceptable vis-à-vis des serrures connectées, à savoir à la condition qu'elle y gagne nettement

en confort de vie : en n'ayant pas à gérer des clés en cas de location sur AirBnB, ou pour faciliter les livraisons de courses. Quoique son adhésion au dispositif ne soit pas franchement exprimée, elle oppose d'elle-même un contre-argument technique à son compagnon :

> « E7: (l'interrompant, de nouveau sur une comparaison très pratique) En même temps on peut te voler ta clé, on peut ouvrir la porte avec une radio...» (entretien 5, 41 min 45 s)

Elle lui oppose même ensuite que sa posture est paradoxale en cela que son principal argument relatif aux questions de vie privée – la question de son consentement éclairé – ne se poserait pas vis-à-vis d'une serrure connectée et de l'ouverture du domicile à un tiers, qui serait ici entièrement sous son contrôle. En somme, E7 a une posture de principe plutôt technophobe, mais elle est tout à fait capable de se dédire une fois qu'elle envisage des situations pratiques où l'utilisation de dispositifs de *smart home* lui semblent avantageux. *A contrario*, E6 peine à expliquer sa réticence face à la serrure connectée alors qu'il est enthousiaste par principe envers ces dispositifs tant qu'ils ne lui sont pas opposés. Il est tout à fait possible qu'il n'ait pas eu le temps de développer sa réflexion à ce stade de l'entretien, on peut notamment supposer qu'un temps de réflexion plus poussé l'aurait amené aux mêmes justifications que les autres enquêtés technophiles et réticents aux serrures connectées, à savoir une défiance envers le niveau de sécurité informatique d'un dispositif exposant un enjeu important, son logis, à un grave aléa à son échelle, une intrusion (voir « La serrure connectée : une réticence provisoire ? », p. 359).

Un dernier registre de craintes évoquées par les enquêtés concerne enfin les enceintes et la domotique connectées en tant qu'innovations en soi. Une première crainte assez bien partagée dans l'échantillon est celle que l'assistance offerte par ces dispositifs fasse tomber leurs utilisateurs dans l'assistanat, comprise comme une accoutumance à la facilité et la paresse. Il s'agit du discours aussi banal qu'ancien sur un lien supposé entre technique et paresse, déjà évoqué par Platon dans le *Phèdre* à propos des méfaits de l'écrit pour la mémoire et le pensée dialogique[576], critique qui est aujourd'hui étendue au *smartphone* qui induirait même une « avarice cognitive » selon Barr *et al*[577]. En ce qui concerne les technologies du logis connecté, la critique porte plus spécifiquement sur l'encouragement à la paresse physique : l'utiliser

[576] J. LABARBE, « De l'oral à l'écrit dans la Grèce archaïque », *Bulletins de l'Académie Royale de Belgique*, vol. 67, nº 1, Persée - Portail des revues scientifiques en SHS, 1981, p. 65 (en ligne : https://www.persee.fr/doc/barb_0001-4133_1981_num_67_1_55494 ; consulté le 6 décembre 2022)

[577] « *We frame Smartphone use as an instantiation of the extended mind—the notion that our cognition goes beyond our brains—and in so doing, characterize a modern form of* ***cognitive miserliness****.* » (trad. pers.) *in* N. BARR *et al.*, « The brain in your pocket: Evidence that Smartphones are used to supplant thinking », *Computers in Human Behavior*, vol. 48, 1er juillet 2015, p. 473-480 (en ligne : https://www.sciencedirect.com/science/article/pii/S0747563215001272 ; consulté le 6 décembre 2022)

d’interrupteurs logiciels et d’effecteurs remplaçant l’action du corps, et abolissant, dans une certaine mesure, les micro-distances du logis. Cette critique avait déjà porté dans les décennies précédentes sur l’usage de la télécommande pour la télévision[578] , par exemple, dans le contexte de l’espace domestique. Pour E20, une enceinte connectée est certes « pratique » justement dans cet usage comme télécommande, mais elle tient aussi à rappeler avec humour qu’il ne coûte finalement que « deux squats » de se lever de sa chaise pour le même résultat :

> « E20: Oui il y a toujours du pratique et du technique. Comme par exemple, une enceinte c’est pratique mais c’est gadget. Enfin je veux dire c’est pratique mais ce n’est pas nécessaire. Mettre ta musique etc. c’est quelque chose que tu peux faire autrement sans plus consommer ou même en... faisant du sport (rire), tu te lèves de ta chaise, donc ce n’est pas plus mal. (…) C’est des squats c’est deux squats, un pour se lever et un pour s’asseoir. » (entretien 13, 1 h 30 min)

Chez E5, ce discours est comme souvent développé jusqu’à un haut niveau de généralité :

> « (…) un des enjeux des enceintes connectées, c'est de capter les activités commerciales ou de proximité. Et donc, que tes achats que tu ferais chez BioCoop (où nous avons été en arrivant, quand je l'ai croisé en bas de chez lui), tu les aurais faits directement chez Amazon parce que de toute façon c'est plus facile, tu n'as qu'à le dire à ton enceinte conne... à Alexa. Ça c'est une autre raison. Parce que ça ça déconstruit la société. La souveraineté aussi. Parce que la question de l'impôt, etc. Un autre enjeu que j'ai sur les enceintes connectées c'est la question écologique. A la fois de la consommation ET de la production. Enjeu que j'ai plus en général avec l'informatique ou les services via l'informatique. Toute cette informatique qui vient jusqu'à chez toi pour te dire "tu n'as que à cliquer là ou là".
> JF: (acquiesce)
> E5: "Regarde, c'est à deux centimètres et tu auras tous les choix ! Tu n'as même pas à cliquer trop loin !". Un enjeu de cette informatique, c'est l'enjeu de la facilité. La facilité c'est un discours pour t'apporter le produit et te convaincre.» (entretien 2, 1 h 32 min)

Sans entrer ici avec lui dans la thématique du lien social, il pointe de manière critique la promesse qui est faite aux utilisateurs de l’informatique de services contemporaine de tout pouvoir commander de chez soi, sans effort, en économisant jusqu’aux clics (« Tu n'as même

[578] « En abolissant la distance entre soi et l’écran, elle autorise la superposition fantasmatique de l’écran et de soi. En raccourcissant, au point qu’on puisse l’imaginer aboli, le temps de réaction de l’objet, elle laisse penser que le monde est, en quelque sorte, connecté directement à notre cerveau. Rejoignant ainsi les figures les plus emblématiques de la science-fiction : quand l’homme impose sa pensée au monde sans la moindre médiation et, dans un dernier sursaut pour concurrencer la divinité, fait du monde l’expression de son propre et seul esprit » *in* P. MEIRIEU, « La télécommande et l’infantile », *Médium*, vol. 2, nº 1, Association Médium, 2005, § 13 (en ligne : https://www.cairn.info/revue-medium-2005-1-page-44.htm ; consulté le 6 décembre 2022)

pas à cliquer trop loin ! »). Il met moins en cause la paresse des individus qui souscrivent à ces services que la stratégie commerciale construite autour de la paresse, utilisée comme un ressort facilitant les achats compulsifs et instituant le domicile comme un nouveau marché – ou plutôt, comme un nouveau canal commercial – à conquérir ; thématique qu'il développe davantage à d'autres moments de l'entretien autour de la question alors très discutée de savoir quels services seraient proposés par défaut aux utilisateurs d'enceintes lors de leurs commandes à caractère commercial. Cette mise en accusation de la paresse à laquelle inviterait la domotique connectée est reprise par tous les types d'enquêtés, mais on la retrouve plutôt chez les réticents – les enthousiastes peuvent aussi confesser faire preuve d'une trop grande propension à la facilité, mais cette facilité reste un des arguments de vente et de défense des enceintes connectées.

La deuxième crainte évoquée relativement à l'enceinte connectée comme innovation est celle de la réticence ou de la peur face à la nouveauté. On devine qu'elle concerne cette fois plutôt les enthousiastes, qui la mobilise notamment lorsqu'ils tentent d'expliquer la réticence de certains de leurs contemporains à utiliser ces dispositifs. E71, rencontrée alors qu'elle venait acheter une Google Home pour ses parents âgés, exprime clairement cette idée qu'il y aurait une peur irraisonnée relativement aux données personnelles, qui serait davantage à chercher du côté d'une peur de l'innovation pour elle-même :

> « JF: Vous trouvez que c'est excessif, ce discours [qu'elle vient de faire par rapport à la protection de la vie privée], vous, par exemple ?
> [391,7] E71: (plus hésitante) Bah... il faudrait que ce soit appuyé sur des éléments vraiment... bien précis. J'ai l'impression que ça part un peu dans tous les sens.
> JF: Trop parano...?
> E71: Une espèce de peur qui est un peu... individuelle, et puis un peu humaine, du changement aussi. Heu... que les choses évoluent. D'avoir la peur d'être piégé (elle insiste sur ce dernier mot) .
> JF: (acquiesce)
> E71: Que je pense qu'on peut assez vite développer, voilà, chaque être humain, la peur d'être dépassé, de pas maîtriser quelque chose... Dans le temps d'avant, on faisait tout à la main, enfin bon... okay ! » (entretien 6, 8 min)

Elle poursuit une vingtaine de minutes plus tard sur cette thématique, en évoquant un côté « vieux cons » que nous aurions tous, et qui consisterait à fantasmer une époque passée où nous aurions été plus indépendants de la technologie :

> « En plus c'est ça, y a une peur, un peu, on fait aussi les vieux cons (je pouffe) , c'est-à-dire qu'on dit "ah c'était mieux avant !" parce qu'on aimait bien (sur un ton un peu rigolo) maîtriser les choses, on aimait bien, voilà, on avait un peu peur qu'un

jour il y ait une coupure de courant et qu'on sache plus rien faire. Et qu'on dit "bah avant, couper des patates, on savait faire, maintenant tout est...".
JF: Automatique et tout.
E71: Ouais. Après je veux pas tomber dans tout ça, mais... c'est vrai que des fois...» (entretien 6, 32 min)

Quoiqu'E71 s'inclue elle-même dans cette propension qui serait générale (« humaine », pour reprendre l'extrait précédent), son propos distingue malgré tout explicitement ceux qui passeraient outre leur peur de l'innovation et ceux qui se laisseraient guider par elle, à contre-sens d'un progrès qu'elle présente comme inexorable et, *in fine*, plus désirable. E3 exprime sensiblement la même chose lorsqu'il déclare « Aujourd'hui on fait pratiquement tout sur Internet et du coup... pour moi, enfin... j'ai pas vraiment peur » (entretien 1, 39 min 35 s). C'est également le terme de « peur » qu'on retrouve chez E21 lorsque nous évoquons les personnes qui pourraient être séduites par des enceintes connectées fonctionnant en local :

« E21: Moi non, parce que du coup ça limite le... ça limite les... mes demandes à Alexa. Moi j'utilise ça, mais j'utilise autre chose. (incompréhensible) , Kindle, le son, voilà. Comme j'ai une utilisation plus large d'Alexa, forcément j'ai pas envie... X [son fils] par contre lui il serait quand même... il veut pas justement être branché sur une, une enceinte connectée, il veut justement pouvoir l'utiliser que pour l'aspect domotique, contrôle général, heu, sur une application.
JF: A la voix, le confort et tout, mais en local.
E21: Voilà. Lui c'est juste ce genre de confort-là. Pour ce genre de personne, ça plairait.
JF: (acquiesce)
E21: Et ça ferait moins peur, je pense, tout le monde serait plus équipé. Parce que tout le monde, heu, a envie d'avoir un confort, tout le monde aime ça. Donc je pense que ça marcherait bien, il y aurait moins de questions à se poser. » (entretien 14, 1 h 57 min)

Là encore, on retrouve une opposition entre un progrès inexorable et universellement désirable (« tout le monde, heu, a envie d'avoir un confort, tout le monde aime ça ») et une peur de l'innovation (ici, comme prédatrice de la vie privée des individus). De même, certains embrasseraient comme elle pleinement cet avenir, à raison, quand d'autres se priveraient ou se « [limiteraient] » dans l'utilisation de cette innovation (en n'utilisant pas les fonctions des enceintes requérant une connexion à Internet, en l'espèce). On peut lire une certaine condescendance dans cette description des réfractaires à la domotique connectée, qui est à

mettre en miroir d'une fierté assez bien partagée des utilisateurs interrogés à ne pas être *peureux* et à faire partir des pionniers de cette technologie[579], ce qui est très net chez E21 :

> « E21: Et ça va évoluer. Tu as vu qu'en France on est très peu équipés, encore, hein.
> [35,1] JF: Ah oui, c'est un marché émergent.
> E21: Je suis une des seules à être vraiment... je suis une des premières, hein.
> JF: Bah les enceintes, on en trouve quand même. Je me rappelle plus les dernières... les derniers chiffres. Je crois qu'on n'est pas au million, mais quand même.
> E21: Mais si tu mets les chiffres en comparaison d'un portable, d'un ordinateur...
> JF: Ah bah oui ! Mais le marché commence à se structurer.
> E21: Mais il est encore loin d'être développé, à ce niveau-là.»
> (entretien 14, début de l'entretien)

Du reste, un discours récurrent sur la peur éprouvée face aux nouveaux objets connectés est qu'elle repose sur une base irrationnelle. Sur un mode mineur, il s'agit toujours de rappeler que personne ne pourrait aujourd'hui raisonnablement échapper à tout traçage numérique, ce qui nous ramène à la thématique du fatalisme que nous avons déjà explorée. Sur un mode plus véhément, il s'agit de montrer que cette résistance au changement relèverait au mieux d'un manque d'information, au pire d'une inconséquence coupable :

> « « E21: Les gens le disent. Tous. Avant de mettre Alexa "tu sais qu'il t'écoute ?", et des jeunes, que j'ai dans mon entourage, en sport, des jeunes qui pourtant sont... branchés iPhone 24h/24 me disent "ah t'as Alexa, mais tu sais qu'il t'écoute, il sait tout, il enregistre, ohlala". Oui. Et alors ? Alors que la personne là ne sait même pas qui je suis. Voilà, c'est un... c'est pour dire que, on a beau dire ça, c'est un peu ce qui est véhiculé avec ce genre d'appareils : les gens les plus secrets, comme moi, ça les empêche pas d'être branchés sur ce genre de technologies.
> JF: Et puis eux ça les empêche pas d'avoir un téléphone, heu...
> E21: Oui, ils sont plus sur leur téléphone, sur Insta... D'ailleurs ils donnent leur image à Insta à chaque (incompréhensible) , "ah moi j'ai fait ça, je suis là", Insta à fond, Insta, Snapchat etc., alors qu'ils n'ont pas Alexa parce qu'ils ne veulent pas être écoutés, parce qu'ils ne veulent pas donner leurs données. Je comprends pas bien. »
> (entretien 14, 2 h 1 min 50 s)

La démarche de E21 est rhétoriquement intéressante, puisqu'elle oppose des pratiques devenues banales, à savoir l'utilisation d'un iPhone et des applications Instagram et Snapchat, avec l'utilisation d'une enceinte connectée. Elle rend compte d'un préjugé répandu contre les assistants vocaux (« tu sais qu'il t'écoute ? », sous-entendu en permanence), mais rétorque que les autres pratiques numériques contemporaines plus répandues ne sont pas moins propices à la

[579] C'était encore assez vrai au moment de cet entretien en mars 2020.

dissémination des « données ». L'argument n'est pas un homme de paille : la situation est non seulement vraisemblable, mais aussi récurrente à n'en pas douter. Il ne s'agit pas non plus d'une attaque *ad personam* : elle ne discrédite pas ses interlocuteurs pour eux-mêmes, mais bien pour l'incohérence de leurs remarques au regard de leur utilisation intensive d'un dispositif qui est sans conteste plus intrusif encore. Il ne serait d'ailleurs pas même étonnant que certaines de ces personnes utilisent aussi l'assistant vocal de leur *smartphone*. Le « je comprends pas bien » de E21 est donc tout à fait justifié dans les cas qu'elle décrit. Cependant, elle place ici le débat dans un cadre où sa position est forcément la meilleure : quoique nous en soyons à deux heures d'entretien et que des cas de réfractaires comme celui de son fils aient été évoqués, le fait que les efforts de certains pour limiter leur exposition en ligne puissent avoir une quelconque efficacité ou même soient simplement sincères est évacué. Nous avions déjà vu ce discours par exemple chez E8, qui affirme :

> « E8: Donc tout est déjà utilisé. Donc pour moi, la notion de données personnelles, c'est déjà une notion qui est... Les gens ont peur que les données personnelles soient prises et utilisées, mais c'est déjà le cas, quoi. C'est déjà le cas. Donc... ouais.» (entretien 4, 36 min 30 s)

Dans tous ces cas, il y a au bout du compte plus qu'un simple fatalisme en retrait de ce discours : la réticence exprimée contre la domotique connectée étant considérée comme insensée, dans un contexte d'érosion immunitaire de la vie privée présentée comme inéluctable, les réfractaires ne peuvent qu'être inconscients ou simplement *peureux*, rétifs par principe au changement. L'adhésion enthousiaste à l'utilisation d'un maximum d'objets connectés, au contraire, serait la marque d'une ouverture d'esprit et d'une meilleure connaissance des enjeux de l'ère numérique. *In fine*, pour leurs utilisateurs enthousiastes, il se rejoue donc autour des enceintes connectées guère autre chose qu'une nouvelle occurrence de la querelle des anciens et des modernes, ou de la réaction contre le progrès.

*

Si la science-fiction avait largement préparé les esprits à l'arrivée d'objets conversationnels dans le quotidien, et déjà mis en scène l'opposition entre le désir et la crainte qu'ils suscitent, quels choix en matière de design vocal ont été faits pour accompagner l'*incorporation* de ces nouveaux objets dans les logis ? quelles réactions ont les enquêtés à leur égard ?

II - **DONNER DE LA VOIX**

La voix d'un robot n'est pas nécessairement robotique

Commençons ici par revenir sur une expression courante de la langue française : parler d'une voix robotique. Paradoxalement, elle s'emploie avant tout pour décrire la manière de s'exprimer d'un humain qui s'exprimerait de façon automatique, sur un ton monocorde et égal, sans manifester d'émotion ou de chaleur particulière. Cette expression a pu avoir du sens pendant un temps, lorsque la synthèse vocale était limitée à la juxtaposition de mots et de sons pré-enregistrés. Dans le contexte français, un exemple typique en est la « voix » de la SNCF, dont les annonces en gare sont montées depuis 1981 à partir de multiples enregistrements vocaux dits par la comédienne Simone Hérault[580], avec un style uniforme caractérisé par ses variations prosodiques (d'intonation, de rythme et d'intensité) très limitées. Pour autant, on peut faire deux objections à cette notion de voix robotique. D'abord, les voix robotiques ne sont pas nécessairement inexpressives : un exemple fameux fourni par la science-fiction est celui du robot R2-D2 dans les films *Star Wars* de George Lucas, dont les bips et les trilles très variés parviennent à exprimer les émotions du personnage – quoique sans recours à un langage articulé. Ensuite, les limites techniques de la synthèse vocale en matière d'expressivité et de naturel sont aujourd'hui levées, au moins pour les registres d'échange attendus de la part d'une enceinte connectée. Selon Morel et Bänziger, la prosodie est l'élément fondamental du « naturel » d'une voix synthétisée : « Pour les systèmes de synthèse de la parole, la prosodie est un enjeu important car elle représente une grande part de ce qui est humain dans la parole. La prosodie doit donner du relief à la voix et être jugée naturelle, sinon celle-ci paraît mécanique. Mais ce relief n'est pas disposé au hasard : pour une bonne intelligibilité, la prosodie doit transmettre des informations syntaxiques (découpage, hiérarchisation), sémantiques et pragmatiques (…). Pour une bonne expressivité, il est souhaitable également que la prosodie soit en mesure de communiquer des attitudes et des émotions. »[581] La deuxième limite au naturel de la synthèse vocale est le timbre, c'est-à-dire les qualités harmoniques du son produit, timbre qui permet donc de distinguer quel instrument ou quelle voix a produit une même note[582]. Ces deux limites ont été levées au cours de la décennie 2010 par l'utilisation de grands jeux de données et

[580] C. GUE, « Simone, la voix des gares », *leparisien.fr*, 24 janvier 2004 (en ligne : https://www.leparisien.fr/economie/simone-la-voix-des-gares-25-01-2004-2004707818.php ; consulté le 22 décembre 2022)
[581] M. MOREL et T. BÄNZIGER, « Le rôle de l'intonation dans la communication vocale des émotions : test par la synthèse », *Cahiers de l'Institut de Linguistique de Louvain*, vol. 30, nº 1-3, Peeters, 2004, p. 92-93 (en ligne : https://hal.archives-ouvertes.fr/hal-00100347 ; consulté le 22 décembre 2022)
[582] *Ibid.*, p. 109

d'algorithmes de *deep learning* qui ont permis de dépasser les techniques de montage plus classiquement utilisées, comme dans le cas des annonces de la SNCF.

Aujourd'hui, un logiciel de synthèse vocale comme Polly, utilisé par Amazon pour produire la voix d'Alexa, ne requiert plus d'intervention humaine directe ni d'acteur pour émuler une voix paraissant naturelle. Il est même possible de faire parler des voix différentes et dans différentes langues. Google est même allé jusqu'à proposer un service, Duplex, utilisant la synthèse vocale de Google Assistant pour passer des coups de fil à des commerces physiques, par exemple pour prendre un rendez-vous chez le coiffeur, comme lors d'une démonstration publique remarquée du CEO de l'entreprise Sundar Pichai en 2018[583]. La technologie n'était pas encore parfaitement au point encore en 2019, des opérateurs humains devant parfois reprendre la main[584], mais la faisabilité du procédé est prouvée. L'horizon d'attente proposé par le film *Her* de Spike Jonz (2013) dans lequel Joaquin Phoenix finit par s'éprendre de l'agent conversationnel joué par Scarlett Johansson n'est cependant pas atteint : les assistants vocaux ne sont encore capables que de conversations stéréotypées. En particulier, ils requièrent des tours de parole clairs, et peinent par exemple à interrompre ou à être interrompus au cours d'une phrase – pratique qu'on peut parfois déplorer, mais qui est une des caractéristiques de la conversation humaine. Au sein d'un couple d'enquêtés utilisateurs d'une Google Home, E7 rapporte ainsi que leur enceinte devient régulièrement « folle » et que son compagnon doit « la faire taire tout le temps » :

> « E7: Quand elle devient folle, la pauvre, il la fait taire tout le temps.
> E6: Il y en a trop (de blabla). »
> (entretien 3 ; 24 min 50 s)

Cette situation est souvent rapportée par des enquêtés, je l'ai également observée lors des démonstrations au cours des entretiens, ou dans les relations des personnes vivant avec moi et l'enceinte Alexa mise en test dans mon propre logement : les agents conversationnels se lancent dans une longue tirade sans intérêt pour leur interlocuteur humain, par exemple en répétant le même long message d'erreur en réponse à plusieurs sollicitations successives, ou plus simplement en cherchant à fournir trop d'informations en réponse à une question simple. Là où

[583] A. HARTMANS, « Google unveiled a new "experiment" that will impersonate a human to make restaurant reservations for you over the phone », *Business Insider*, 8 mai 2018 (en ligne : https://www.businessinsider.com/google-assistant-makes-phone-calls-schedules-appointments-reservations-google-duplex-google-io-2018-5 ; consulté le 22 décembre 2022)
[584] B. X. CHEN et C. METZ, « Google's Duplex Uses A.I. to Mimic Humans (Sometimes) », *The New York Times*, 22 mai 2019 (en ligne : https://www.nytimes.com/2019/05/22/technology/personaltech/ai-google-duplex.html ; consulté le 22 décembre 2022)

il serait facile de demander le silence ou la parole à un autre humain, il faut généralement attendre la fin de la tirade de l'enceinte ou l'interrompre en couvrant sa voix par une requête de type « mot de réveil, stop » pour réussir à la « faire taire ».

Pour autant, E6 et E7 estiment que ces moments de « [folie] » restent rares, et comparent d'eux-mêmes leur enceinte à un animal, autrement dit à un être doté d'une intentionnalité, à défaut d'une intelligence humaine pleinement développée :

> « E6: Mais ça fonctionne globalement bien, je trouve.
> E7: Franchement, ouais. Elle fait rien de trop bizarre.
> E6: Ouais. On dirait un animal, tu sais (nous pouffons)
> E7: Ouais c'est vrai ! Elle écoute, elle est sage (rire) »
> (entretien 3 ; 6 min 40 s)

Malgré le fait que l'enceinte soit ici dotée d'une intentionnalité ou d'une personnalité en mode mineur, c'est-à-dire animales plutôt qu'humaines, le fait de la caractériser par une valeur morale (« elle est sage ») et de lui accorder la capacité d'une véritable action (« elle écoute ») signale clairement qu'elle est considérée à tout le moins comme un être animé. Nous allons voir maintenant à quel point les enquêtés inscrivent leur relation à leur enceinte dans une logique anthropomorphique ou proto-anthropomorphique.

La tentation anthropomorphique

Dans son ouvrage majeur *Par-delà nature et culture*, l'anthropologue Philippe Descola propose une typologie des relations « ontologiques » aux autres « existants », objets et forces naturelles qui entourent les humains (voir Tableau 8 ci-dessous)[585]. Pour dépasser le dualisme occidental entre nature et culture, il propose plutôt de lire le rapport des cultures au monde selon les axes de l'intériorité et de la physicalité. L'intériorité renvoie à la vie psychique, la possession d'une forme d'âme à travers des intentionnalités et des émotions, ou encore la maîtrise du langage. La physicalité renvoie à la vie physique, aux processus métaboliques, à la forme des corps. Le croisement de ces structures permet de dégager quatre grands types dans le rapport ontologique au monde.

[585] P. DESCOLA, *Par-delà nature et culture*, Paris (France), NRF : Gallimard, 2005

*Tableau 8 - Les quatre ontologies de Philippe Descola (*Par-delà nature et culture*, p. 220)*

Ressemblance des intériorités	Animisme	Totémisme	Ressemblance des intériorités
Différences des physicalités			Ressemblance des physicalités
Différences des intériorités	Naturalisme	Analogisme	Différences des intériorités
Ressemblance des physicalités			Différences des physicalités

La pensée occidentale tend nettement vers le naturalisme : elle postule la ressemblance des physicalités en cela qu'elle est moniste et matérialiste, mais aussi la différence des intériorités en cela qu'elle donne une place prépondérante à l'intellect humain, dont une large partie de sa tradition consiste à établir la singularité dans l'ordre des choses. L'un des points les plus ardemment défendus depuis l'Antiquité grecque est que l'humain serait le seul être à véritablement maîtriser le langage et à être un animal politique. L'émergence d'agents conversationnels de plus en plus convaincants tend à réduire la différence des intériorités perçue par les humains dans leur rapport aux machines, qui évolue vers l'animisme ou le totémisme. L'attitude animiste consisterait à considérer les enceintes connectées comme des étants plus ou moins réflexifs, tout en conservant pour soi la nette perception d'une différence physique (ou plutôt physiologique) avec ce qui reste une machine, un dispositif technique. L'attitude totémiste consisterait à gommer à la fois la différence d'intériorité et de physicalité pour considérer les enceintes connectées comme des totems, c'est-à-dire des agents agissants et quasi humains – même sans aller jusqu'à la figure du robot androïde, cette attitude est par exemple encouragée lorsque l'assistant vocal est doté d'une voix dont le timbre et la prosodie imite plus parfaitement la voix humaine. Pour le non-anthropologue, et en trahissant quelque peu Descola en ne le suivant pas jusqu'au bout de sa logique de déconstruction de ce terme, ces deux attitudes peuvent être décrites comme anthropomorphiques ou proto-anthropomorphiques au sens où l'imitation de la voix et de la conversation humaines en sont le principe. Les types proposés par Descola permettent néanmoins de spécifier parmi les attitudes

anthropomorphiques le degré de distinction de l'essence du robot et de l'humain, comme le résume le montre le Tableau 9 suivant :

Tableau 9 - Degrés de l'anthropomorphisme vis-à-vis des enceintes connectées (JFP, 2022)

Différence des intériorités maintenues	**Ressemblance des intériorités mieux ou tout à fait acceptée**	
Naturalisme	Animisme	Totémisme
L'enceinte connectée est fondamentalement une machine, mimant plus ou moins mal les interactions humaines.	L'enceinte connectée est une machine étonnamment convaincante dans son imitation des interactions humaines.	L'enceinte connectée est une présence (quasi-)consciente qui occupe une véritable place dans la sociabilité domestique.

Cette partition se retrouve en mon sens dans les différentes voix proposées par les trois principaux assistants vocaux du marché. Après écoute des voix disponibles en anglais des États-Unis et en français de France, j'ai dressé un tableau décrivant mon appréhension subjective de ces voix comme étant robotique ou naturelle. Une voix féminine et une voix masculine sont généralement proposées, sauf pour Google Assistant en français, dont la voix est forcément féminine. Dans quatre des cinq cas restants, il semble à chaque fois qu'une voix soit robotique et l'autre plus naturelle, avec une mention spéciale à la voix féminine anglaise d'Alexa qui est particulièrement convaincante et n'a qu'exceptionnellement achoppé sur certains sons.

Tableau 10 - Sonorité des voix masculines et féminines des assistants vocaux en français et en anglais

	Anglais US - féminine	Anglais US - masculine	Français - féminine	Français - masculine
Siri	Robotique	Robotique	Robotique	Naturelle
Alexa	Naturelle	Robotique	Robotique	Naturelle
Google Assistant	Robotique	Naturelle	Robotique	∅

On peut se demander avec Dominique Boullier dans son article « Objets communicants, avez-vous donc une âme ? » s'il est préférable ou non de marquer la nature synthétique de la voix qui parle dans les haut-parleurs d'une enceinte connectée : « La performance ou la facilité d'usage d'une interface (ici vocale) peut ainsi entrer en contradiction avec l'asymétrie souhaitée entre humain et machine. »[586]. Il peut être souhaitable de ne pas chercher à mimer à la perfection une voix humaine pour les concepteurs d'enceintes connectées ou, autrement dit, à ne pas chercher forcément la totémisation de l'enceinte. Retenir une logique animiste consisterait ici à volontairement conserver une voix robotique à l'assistant, par exemple pour inciter l'utilisateur à bien articuler ses requêtes, ou encore pour ne pas troubler ceux qui préfèrent avoir clairement affaire à une machine. C'est par exemple le cas de E21 :

> « JF: Ouais. (pause) Et justement, ça me permet de rebondir sur quelque chose qu'on disait tout à l'heure, c'est que Alexa en français, la voix est assez métallique, c'est quelque chose que tu préfères, ou... heu... je pense pas que ce soit une limite technique, en Français peut-être encore, mais par exemple la voix en anglais est hyper naturelle, heu, pour Alexa d'Amazon. En anglais, pour le coup, on peut pas avoir de conversation, on est d'accord, mais les réponses se font avec une tonalité hyper humaine.
> E21: Heu... le fait que ça reste comme ça, assez métallique, ça permet de ne pas oublier que, heu, c'est un objet, elle est branchée, et qu'elle peut avoir, heu... une influence néfaste. Et je préfère que ça reste comme ça, sinon si ça devient plus naturel, on peut s'attacher, se laisser influencer, et ça peut être encore... une déviance, peut-être plus facilement.
> JF: D'humaniser la machine...?

[586] D. BOULLIER, « Objets communicants, avez-vous donc une âme ? », *Les Cahiers du numerique*, vol. 3, nº 4, 2002, § 9 (en ligne : http://www.cairn.info/revue-les-cahiers-du-numerique-2002-4-page-45.htm ; consulté le 20 septembre 2021)

E21: Oui, d'humaniser.»
(entretien 14, 1 h 40 min 50 s)

Pour elle, il est important que la voix de son Alexa en français reste « métallique », et elle n'éprouve aucune envie pour la tonalité beaucoup plus naturelle de la version anglophone. Plus encore, elle considérerait « l'[humanisation] » de son Alexa comme une « déviance » présentant des risques bien supérieurs à l'avantage d'une conversation plus humaine, et précisément du fait que cette conversation serait plus humaine, qu'il s'agisse de risques d'attachement ou d'influence. Il n'est d'ailleurs pas anodin que cette réflexion ait été faite au moment de l'entretien où elle me parlait des robots androïdes de la série *Real Humans*, qui avait exercé sur elle une fascination certaine.

En tout état de cause, il semble que les deux options ont finalement été retenues par les développeurs dans la plupart des cas : il est possible de choisir entre des voix des deux sexes, mais dans le même temps aussi entre une voix plus naturelle et une voix plus robotique – si l'on excepte le cas de Siri en anglais. Il me semble exister à chaque fois une option à la sonorité robotique et une autre à la sonorité naturelle. La sonorité des voix féminines en français, qui sont les voix par défaut, me semble à chaque fois robotique. Il s'agit peut-être d'un choix des fabricants pour cette langue, mais il est impossible de dire si ce design répond à une intention ou à des contraintes techniques. Quoi qu'il en soit, on peut remarquer que le fait que les voix masculines en français sonnent plus naturellement n'a pas eu d'impact sur le fait que le choix par défaut de la voix soit au féminin pour Alexa et Google Assistant, ni pour Siri jusqu'en 2021 (le choix étant maintenant demandé à la première utilisation pour les appareils d'Apple).

Un autre indice de cette faculté d'anthropomorphisme variable selon les assistants vocaux se lit plus facilement chez les utilisateurs de plusieurs marques, qui peuvent alors comparer la personnalité de chacun d'eux. Au-delà de la seule question technique des qualités sonores ou d'ouverture logicielle de l'enceinte (voir « Choisir son maître d'orchestre », p. 320), et même de l'efficacité du TALN de l'agent conversationnel, il s'agit bien ici de distinguer entre les différents assistants vocaux du point de vue de leur personnalité entendue dans un sens très humain, en l'espèce à travers leur style de réponse aux sollicitations. E16 déclare ainsi préférer nettement discuter avec Siri plutôt qu'avec Google Assistant, même si c'est bien sa Google Home qui lui rend techniquement le plus de services au quotidien :

« Ouais, Google a.... quand on fait un comparatif avec Siri a moins ce côté rigolote, répondant, par rapport à Siri qui est un assistant vocal qui...
JF: Qui a plus de personnalité ?

E16: Qui a plus de personnalité, qui va se foutre un peu de ta gueule, rigoler, machin, truc, alors que Google c'est "j'ai pas compris, j'ai pas compris, j'ai pas compris". Ce qui devient un petit peu... agaçant.
JF: (pouffe)
Google Home: Cela arrive même aux meilleurs d'entre nous. Est-ce que je peux vous aider pour autre chose ?
E16: (amusé) Voilà ! Ferme ta gueule ! (nous rions) Bon, ça elle comprend, mais rien, alors que Siri t'aurait mis un petit mot, genre "très bien" (imitant un air pincé qu'il prête à Siri). »
(entretien 10 ; 28 min 10 s)

Sa principale critique envers Google Home est le caractère répétitif de la réponse « je n'ai pas compris », qu'il prononce trois fois pour marquer le caractère trop habituel de ce retour vocal de l'assistant. Il ne s'agit même pas ici pour E16 de se plaindre du fait que son enceinte ne le comprend souvent pas, mais bien de dire que c'est la forme de la réponse qui manque de personnalité – terme que je lui suggère, mais qu'il reprend sans hésiter. Là où Siri lui semble plus amusant et plus varié dans ses réponses, Google Assistant répète inlassablement la même réplique. Pour autant, E16 a bien conscience de verser ici dans l'anthropomorphisme, et ajoute aussitôt après :

« E16: C'est vraiment... pff. C'est vraiment un côté très, comment dire... très... très subjectif et humain de penser qu'une machine peut avoir un caractère. On se dit "tiens, ce serait rigolo qu'elle ait un peu plus de caractère", mais à la fois ce serait aussi un peu troublant. »

Il utilise cette fois le terme de « caractère », pour marquer l'idée qu'il voudrait que Google Assistant lui réponde de manière plus spontanée, voire avec un peu de véhémence, à l'instar d'un être humain qui se rebifferait lui-même contre des questions répétées ou le manque d'articulation de son interlocuteur. Mais surtout, E16 désamorce lui-même la critique en anthropomorphisme en parlant d'un désir très « subjectif » et « humain » de sa part. De fait, il pourrait même trouver « troublant » que la machine soit justement trop anthropomorphe. Il y a là une véritable ambivalence du désir et du désarroi : il est à la fois déçu et rassuré que son enceinte lui réponde à la manière d'un robot. Il faut également signaler que la synthèse vocale de Google en français sonne de manière plus robotique que celle de Siri, au niveau de la prosodie et du timbre. Il est d'ailleurs à remarquer que, au moment même de critiquer l'absence d'originalité des réponses de Google Assistant, l'enceinte fasse par erreur une réponse originale à ce qu'elle interprète comme une interpellation de la part de E16 (« Google c'est "j'ai pas compris, j'ai pas compris, j'ai pas compris" »). Plutôt que de lui faire une réponse générique ou de se taire, l'assistant choisit ici au contraire une réponse étonnamment humaine, en tentant de

réconforter l'interlocuteur humain dont elle interprète les « j'ai pas compris » comme une adresse à son égard. Répondre « cela arrive même aux meilleurs » est en fait une très bonne réponse d'un point de vue conversationnel humain : l'enceinte a bien compris qu'il n'y avait aucune requête directe dans cette interpellation, l'a malgré tout interprétée comme une manifestation de détresse, et a fait une réponse fonctionnellement inutile, mais dans un registre émotionnel. Autrement dit, c'est au moment de critiquer le caractère trop robotique d'un agent conversationnel qu'une des réponses les plus humaines possibles a été donnée par celui-ci au cours de l'entretien – si l'on omet le fait que l'enceinte n'a pas compris qu'on parlait d'elle, et non pas à elle.

Ce paradoxe – voire ce pied-de-nez involontaire du logiciel ! – n'a pas été relevé par E16, qui se contente ici de s'agacer avec humour de cette intervention de Google Home dans la conversation, à qui il répond de « fermer sa gueule ». Une première interprétation pourrait être qu'il est gêné d'être détrompé en direct par son enceinte, ce qui expliquerait qu'il la rabroue immédiatement. Une deuxième interprétation pourrait être qu'il continue de trouver cette réponse peu humaine, soit parce qu'elle résulte malgré tout d'une erreur de lecture de la conversation par Google Assistant, soit parce qu'elle correspond effectivement à ce qu'il veut signifier comme étant le caractère trop peu humain et personnalisé de l'enceinte. Si ce n'est pas le contenu de la réplique qui le gêne, c'en est alors la forme. Et, de fait, si l'on poursuit la comparaison avec Siri, deux éléments de différenciation vocale jouent ici. D'une part, la diction plus robotique de Google Assistant, comme on l'a vu. D'autre part, le fait que son Siri a une voix masculine, son Google Assistant une voix féminine, distinction qui peut jouer comme nous le verrons dans « Genre et assistants vocaux » p. 398.

Il faut enfin signaler chez certaines personnes une aversion affirmée aux formes mêmes mineures d'anthropomorphisme proposées par les enceintes. C'est le cas de l'épouse de E8. E8 est un modérateur du groupe Facebook « Les Alexiens » qui dispose de cinq enceintes d'Amazon chez lui, et en est un possesseur des plus précoces car il a participé au *beta test* de l'enceinte en français. Peu avant ce moment de l'entretien, il me demande si j'ai lu un petit texte humoristique qu'il a lui-même rédigé sur les relations parfois difficiles des conjoint·e·s aux enceintes connectées. Dans cet extrait, il me rapporte la position de son épouse, qui est « [gênée de] parler à une machine » :

> « JF: Et elle, elle est plus... tu avais mis "technophobe" ?
> E8: Ouais... C'est pas qu'elle est technophobe, mais elle ce qui la gêne c'est... parler à une machine.

JF: Ouais.
E8: C'est l'appeler avec... un nom, un prénom, quoi.
JF: Oui, tu avais dit que tu avais mis "Echo" pour que ce soit moins...
E8: Voilà, c'est ça, j'ai mis "Echo" parce que ça passait mieux comme ça.» (entretien 4, 15 min 10 s)

C'est bien ce fait même qui est à la source de la gêne de son épouse, sans aucune considération d'ordre pratique, technique, de protection de la vie privée ou autre. Elle est simplement réticente au fait de s'adresser à une machine, ou plus précisément de s'adresser à une machine comme elle s'adresserait à un humain. La solution relative apportée par E8 a été de changer le mot de réveil de ses enceintes Echo. Plutôt que de conserver le prénom Alexa, « Echo » a semblé plus acceptable à son épouse. L'anthropomorphisme est bien le nœud de ce problème, puisque c'est en réduisant la personnification de l'assistant vocal qu'il est parvenu à emporter l'adhésion – à défaut de l'enthousiasme – de son épouse vis-à-vis de cette installation.

*

Dans un texte de 2002 déjà, Dominique Boullier s'interrogeait : « Objets communicants, avez-vous donc une âme ? », et il postulait en particulier que « La performance ou la facilité d'usage d'une interface (ici vocale) peut ainsi entrer en contradiction avec l'asymétrie souhaitée entre humain et machine. »[587] Au bout du compte, malgré les promesses d'interactions vocales naturelles mises en avant par les constructeurs, il semble que des choix aient été faits pour permettre aux utilisateurs de limiter le niveau d'anthropomorphisme de leur enceinte pour ce qui concerne la (ou les) voix de ces dernières. Offrir aux utilisateurs un éventail de possibilités allant d'une présentation robotique à une présentation quasi humaine des assistants vocaux est sans doute le choix de design le plus judicieux, même s'il reste intéressant de voir quels choix ont été faits pour les modes par défaut. En tout état de cause, cette gradation de (l'apparence de) l'humain à la machine se traduit-elle également dans le contenu des échanges et dans le rapport social à l'enceinte ?

[587] *Id.*

III - L'ENCEINTE, UNE NOUVELLE INTERLOCUTRICE A LAQUELLE S'ADRESSER

« - OK Civine, ferme le volet roulant ! je lance à l'encan, sans trop y croire, en grimpant fissa le colimaçon du duplex.

- Pouvez-vous vous identifier s'il vous plait ? *répond une voix très claire, qui semble tomber du plafond.* Je suis Civine, pour vous servir.

- Bonjour Civine... Je suis... Paul Traqué.

- Bonjour Paul, enchantée de faire votre connaissance. Que puis-je pour vous ?

- Je souhaiterais que vous fermiez le volet roulant de la terrasse...

- Vos désirs sont des ordres... *cajole l'intelligence artificielle.*

Programmation dite de complicité. Sensualité discrète. Certainement en standard pour les lofts de célibataire. »[588]

Dans cet extrait des *Furtifs* d'Alain Damasio (2019), le protagoniste s'introduit dans un appartement vide d'un immeuble neuf et cossu pour se dérober à une arrestation policière. Il cherche alors à fermer le volet roulant pour cacher sa présence, et tente « sans trop y croire » une commande vocale. L'agent conversationnel Civine lui répond. Il lui demande de s'identifier, n'ayant pas encore été configuré, et répond à sa requête. La voix par défaut est celle d'une femme, comme c'est généralement le cas aujourd'hui, mais le texte laisse supposer qu'il s'agit ici d'une adaptation au profil du personnage, un homme d'une quarantaine d'année qui viendrait d'acheter un « loft de célibataire », ce qui explique le choix d'une « programmation dite de complicité » à la « sensualité discrète ». Damasio illustre dans ce passage sa thématique du « technococon » en insistant ici sur la question du style conversationnel, dans le contexte de l'ouvrage où la personnalisation de chaque interaction humain-machine est poussée à l'extrême. Au-delà de la seule question du naturel de la voix de l'agent conversationnel, ce texte d'anticipation explore ici l'horizon suivant de développement de ces logiciels, à savoir leur capacité à s'adapter à leur interlocuteur et à faire varier leur propre tonalité. Autrement dit, à mimer non plus seulement une conversation d'ordre strictement pratique fondée sur la vocalisation de *feedbacks* à des ordres domotiques ou à des questions simples, mais à mimer

[588] A. DAMASIO, *Les furtifs*, Clamart (France), La Volte, 2019, p. 211

une relation émotionnelle à leurs utilisateurs. Nous allons voir ici que les enceintes connectées et les assistants vocaux plus largement sont de plus en plus conçus dans une logique d'interlocution qui dépasse le principe initial rudimentaire d'interrupteur ou de télécommande vocale.

Converser avec un objet

Les capacités conversationnelles des enceintes connectés sont encore assez rudimentaires, *a fortiori* en langue française, mais elles sont de plusieurs degrés supérieures aux cas très simples évoqués par Boullier en 2002. Les retours du type « je n'ai pas compris » ou « reportez-vous à l'application » sont nombreux. Pour autant, la voix n'est pas le seul moyen d'interlocution des enceintes. Comme on l'a vu, des éléments de design permettent néanmoins de renforcer la sensation qu'on s'adresse à l'objet, à la manière des premiers Echo qui, par un jeu astucieux de variation de couleur et d'intensité lumineuse de la diode circulaire qui les couronnent, permet de signifier que l'enceinte « écoute » son interlocuteur humain (voir Photographie 13), puis qu'elle « réfléchit » à la réponse qu'elle va lui faire (Photographie 12). Cette logique a été prolongée, toujours chez Amazon, dans les *smart displays* Echo Show de dernière génération : cette fois, c'est l'écran monté sur l'enceinte qui lui sert d'axe qui pivote dans la direction de l'interlocuteur. L'article du site de tests *Les Numériques* dédié à ce modèle titre d'ailleurs « le smart display qui nous fait tourner la tête »[589]. Si dans ce dernier cas l'effort de design d'Amazon visait sans doute aussi beaucoup à faciliter la lecture de l'écran[590], il n'en reste pas moins que cela renforce chez l'interlocuteur humain la sensation de s'adresser et de converser avec son appareil. Les designers d'Amazon n'ont pas fait le choix de donner une apparence humaine à leur dialogueur : ils auraient pu après tout ajouter des yeux physiques mobiles à leur appareil[591], ou plus simplement afficher à l'écran un visage de synthèse représentant leur dialogueur. L'approche est ici plus subtile, car elle mime tout de même une

[589] F. AGEZ et V. DE BRYE, « Test Amazon Echo Show 10 : le smart display qui nous fait tourner la tête », *Les Numériques*, 8 mai 2021 (en ligne : https://www.lesnumeriques.com/assistant-domotique/amazon-echo-show-10-p60107/test.html ; consulté le 3 septembre 2021)

[590] Les journalistes des *Numériques* suggèrent ainsi que la fonction permettrait, par exemple, de continuer à suivre facilement la vidéo d'une recette de cuisine pendant des déplacements autour du plan de travail.

[591] C'est un choix qui a été fait pour certains robots anthropomorphes interagissant avec des humains, comme le robot dit « d'hospitalité » Pepper. Ses applications sont notamment d'accueil à la clientèle (Z. AL BARAKEH *et al.*, « Pepper Humanoid Robot as a Service Robot: a Customer Approach », Paris (France), 2019, p. 1-4) ou de complément d'ordre thérapeutique par la stimulation des capacités conversationnelles de personnes âgées ou de patients atteints de troubles neurologiques comme la maladie d'Alzheimer (I. NPOCHINTO MOUMENI et F. MOUREY, « Intérêt en EHPAD du robot émotionnel Pepper dans les troubles neurocomportementaux de la maladie d'Alzheimer », *NPG Neurologie - Psychiatrie - Gériatrie*, vol. 21, nº 121, 1er février 2021, p. 11-18 (en ligne : https://www.sciencedirect.com/science/article/pii/S1627483020301598)).

réaction, une forme de langage corporel à vocation phatique, mais sans pour autant grimer l'appareil, qui conserve une apparence tout à fait mécanique.

De fait, et contrairement à la voix de Civine dans l'extrait des *Furtifs* « qui semble tomber du plafond », les agents conversationnels restent aujourd'hui nettement associés à un objet comme les enceintes et écrans connectés. L'explication en est avant tout technique et commerciale : dans l'état actuel de la technologie du microphone, il faudrait penser une intégration de l'assistant vocal dès la construction d'un logement pour qu'il soit possible de s'adresser à lui en tout lieu comme si l'on s'adressait simplement à ses murs. Il faudrait en effet au moins un microphone par pièce, et souvent davantage, alimentés en électricité et dotés d'une bonne connexion réseau, le tout sans qu'il n'y paraisse – comme le réseau électrique aujourd'hui dont l'installation se fait à la suite du gros œuvre, et avant les finitions. En l'absence d'un standard en la matière et plus encore de normes de construction qui permettrait cette intégration (un promoteur devra-t-il installer Alexa ? Google Assistant ? ces choix seront-ils réversibles et pérennes ?), ce genre d'installations ne devrait pas voir le jour hors de projets individuels *ad hoc*[592] ou dans des cas comme le projet urbanistique de Sidewalk Labs à Toronto – qui aurait donc intégré les dispositifs de sa maison-mère, Alphabet/Google. Nous n'en sommes donc pas encore à pouvoir parler à nos intérieurs à la manière de Tony Stark s'adressant à Jarvis.

Il n'est cependant pas certain que ces limites techniques vaillent d'être dépassées dans le cas général de personnes n'ayant pas forcément pour fantasme de converser avec leurs murs. E21, malgré son discours sur la « fluidité » offerte au quotidien par son Alexa, est par exemple opposée à ce que cette assistance soit ambiante plutôt qu'intégrée à un appareil bien identifié :

> « JF: Parce que c'est sans doute ce qui va, à terme, se... qu'il n'y ait même plus l'objet, visible, que on parle aux murs, en somme. Ce serait une limite ? Une possibilité ?
> E21: (petite pause) Alors...
> JF: Ce serait encore plus fluide !
> E21: Oui, ce serait encore plus fluide. Et j'aime bien tout ce qui est (incompréhensible) . Heu... pour l'instant, je suis pas prête.
> JF: (acquiesce)
> E21: J'ai encore besoin de m'adresser à quelqu'un. A un objet.
> JF: A un objet, oui.

[592] Au premier rang desquels celui de Mark Zuckerberg lui-même, qui a littéralement nommé Jarvis l'assistant personnel qu'il a développé pour sa propre maison. Voir AFP, « La famille Zuckerberg a un nouveau "majordome virtuel", Jarvis », *RTBF*, 20 décembre 2016 (en ligne : https://www.rtbf.be/article/la-famille-zuckerberg-a-un-nouveau-majordome-virtuel-jarvis-9485677 ; consulté le 28 décembre 2022)

E21: C'est encore un besoin. Parce que je suis aussi quelqu'un de contact. Là tu parles à quelqu'un qui est de contact, de par mon métier. J'ai besoin de l'échange, de la proximité, c'est pour ça, aussi. Tu interrogerais quelqu'un qui n'est pas dans ce métier-là, ça ne le dérangerait pas de parler à un mur... non...
JF: Une pièce ?
E21: A un espace. Moi j'ai quand même besoin encore de m'adresser... à elle.» (entretien 14, 1 h 33 min)

L'anthropomorphisme chez E21 n'est pas tout à fait complet, alors même qu'elle est l'enquêtée chez qui cette tendance est la plus forte. Elle parle de s'adresser à « elle », mais marque une hésitation avant de ce faire. En revanche, elle insiste nettement sur le besoin qu'elle ressent de s'adresser à une entité matérielle clairement identifiée dans la pièce, et se sentirait mal à l'aise de « parler à un mur ». Il lui semble très net que, même en proposant une interaction souvent défaillante en termes d'efficacité de l'échange, son Alexa reste bel et bien « une présence » qui est « plus qu'un objet »[593], mais le fait que cette présence soit aussi physique n'est apparemment pas anodin pour E21. Il est probable que cette réticence contre une assistance vocale ambiante puisse être battue en brèche par l'habitude si cet usage devait se développer, mais l'état actuel de développement technique et commercial des assistants connectés, qu'il est difficile de rendre véritablement ambiants, devrait plutôt contribuer à maintenir dans les années qui viennent l'intérêt pour la présence physique de l'objet.

Avec leur présence quasi humaine liée à leur capacité vocale et davantage encore à leurs capacités de conversation, même rudimentaires[594], les assistants vocaux posent à leurs utilisateurs des problèmes habituellement réservés aux interactions humaines. On ne se pose pas la question de la politesse avec laquelle on actionne un interrupteur. En revanche, faut-il dire « s'il vous plait » à un assistant vocal à qui on demande d'éclairer la pièce ? E3 déclare par exemple avoir envie de remercier son enceinte après une requête :

[593] « E21: Ah. Parce que là je lui demande d'allumer la lampe 1, divan, et la lampe 2, divan, elle comprend pas, parce que je lui donne deux ordres. C'est lampe 1, après "Alexa, allume lampe 2". Donc bon, on n'est pas dans la conversation, mais c'est une présence. Je pense que ça pourrait aider les personnes en... C'est quand même un objet, heu, c'est pas que un objet, c'est une présence, quand même, parce qu'il y a une réponse. Direct. Moi je lui ai demandé : "Alexa, est-ce que je suis gentille". Et elle m'a répondu, et ça avait un rapport... Je sais plus, elle m'avait répondu "tout le monde a le droit à une seconde chance", quelque chose comme ça. Des fois, elle est pourrie, finalement, dans ses réponses.
JF: Oui, elle peut être... taquine.
E21: Voilà, donc ça veut dire qu'elle répond, quand même... c'est une présence, c'est plus qu'un objet. » (entretien 14, 1 h 36 min 30 s)

[594] Il aura par exemple fallu attendre 2020 pour que la fonction « hunches » d'Alexa soit implémentée et lui permette de poser ses propres questions, par exemple pour préciser un paramètre pour donner suite à une requête. Voir D. PRIEST, « Alexa is starting to ask questions. How should we respond? », *op. cit.*

> « Je sais pas... Pas assez.... humain (il enchaîne très vite) en fait Alexa je trouve ça rigolo parce que... moins maintenant, mais t'as envie de lui dire "merci", de lui parler comme à un humain. Tu as envie d'être gentil avec. Alors que "Ok Google" ça fait trop machine pour moi.
> JF: Oui, ça c'est...
> E3: Et du coup ben... c'est moins fun. » (entretien 1, 9 min 40 s)

Cette envie est complètement liée selon lui au niveau de personnification de son appareil, et il évoque d'ailleurs la question à un moment où nous évoquons la possibilité de changer le mot de réveil de son enceinte Amazon, qu'il a finalement laissé sur Alexa. Il fait la comparaison avec Google Home, dont le « Ok Google » de réveil lui semble « [faire] trop machine », là où le prénom « Alexa » serait plus « fun » et lui donnerait envie d'être « gentil » avec « elle » - formulation là aussi anthropomorphique. Il évoque également la « [sensibilité] » de sa compagne envers l'enceinte, qui lui souhaite bonne nuit :

> « ma femme aime bien... est très sensible avec l'enceinte, elle lui dit bonne nuit. "Alexa, bonne nuit". Moi je trouve ça mignon. » (entretien 1, 44 min 10 s)

« Bonne nuit » est un type de commande classique des enceintes, qui permet de lancer plusieurs actions en même temps : baisser le chauffage et les volets, couper l'alimentation de certains objets, allumer une veilleuse… Ce n'est pas le cas ici, et E4 semble sincèrement souhaiter bonne nuit à sa machine, machine qui lui répondra simplement bonne nuit en retour par défaut si l'un des scénarios précédents n'est pas configuré. Le fait que ce « bonne nuit » soit apparemment récurrent montre qu'il s'agit d'un vrai souci de E4 envers son enceinte, souci étant entendu non au sens de problème qu'au sens de se soucier des personnes et des choses, dans une logique de soin et d'empathie.

À l'inverse, la manière qu'ont les assistants vocaux de s'adresser aux humains et de s'intégrer au phonotope de leurs conversations n'en pose pas moins problème également, comme nous l'avons déjà vu. En public, l'interaction vocale avec une enceinte connectée est souvent perçue comme agaçante, impolie, ou encore ridicule. Nicolas Nova observe que cela vaut également, et probablement davantage encore, pour l'utilisation des assistants sur *smartphone*[595]. Mark Zuckerberg lui-même préfère les interactions textuelles avec le système

[595] « Malgré les limites inhérentes à l'utilisation de la commande vocale mentionnées par les informateurs (perturbation du fait du bruit ambiant, regard des autres, problèmes d'interprétation de l'assistant soi-disant intelligent), les usages de cette possibilité d'interaction sont de plus en plus importants comme en attestent les études réalisées par les industriels du secteur, ou par les enquêtes de terrain (Santoloria 2016). » N. NOVA, *Smartphones*, *op. cit.*, chap. Laisse

domotique qu'il a développé pour sa maison, arguant que cela dérangerait moins sa famille au quotidien. Cette gêne est d'autant plus forte quand l'enceinte devient « folle », comme l'avait déjà remarqué E7 :

« E7: Quand elle devient folle (?) , la pauvre, il la fait taire tout le temps.
E6: Il y en a trop (de blabla?) .
E7: Et il éteint la musique tout le temps.
E6: J'aime le silence.
E7: (rire) et moi j'aime pas le silence.
E6: Oui. C'est un peu un conflit.
E7: Il fait juste taire ma Google, c'est tout.
E6: Sinon, non.
JF: Pas plus spécifiquement à ça (l'enceinte) que...
E7: Oui, c'est le silence, quoi. Le bruit, c'est pas lié (rire) .
JF: Si c'était sur une enceinte normale, ce serait pareil, quoi.
E6: Oui. Exact.
E7: Ce serait pareil. »
(entretien 3, 25 min)

On le voit avec la suite de l'extrait déjà cité, l'enjeu est bel et bien ici l'occupation du phonotope domestique par l'enceinte, qui pousse visiblement E6 à faire taire l'enceinte de façon régulière. E7 explique que cela concerne surtout ses moments de « [folie] », mais il semble aussi que cela concerne des moments où E7 a elle-même déclenché l'enceinte, quoiqu'elle minimise cet aspect-là des interruptions de E6 – ce passage de l'entretien fait suite à ma question sur les conflits autour de l'enceinte. Si l'on admet que c'est bien surtout dans les moments de « folie » de l'enceinte que E6 intervient, cela confirme en tout cas que l'occupation du phonotope par ce dispositif est clairement circonscrit à son utilité effective. E6 déteste notamment les longs monologues qu'il juge inutile, par exemple pour décrire une erreur ou pour inviter l'utilisateur à se rendre sur l'application, autant de messages qui ne satisfont pas ou pas directement à une demande directe. Le fait qu'il valorise le silence en général ne fait ici que renforcer cette propension qui est sans doute très générale parmi les enquêtés, et qui a par exemple également été observée dans les nombreux cas de vocalisations non sollicitées par une enceinte au cours des entretiens où un mot de réveil avait été indûment interprété.

La question de la politesse ne concerne donc pas que les humains vis-à-vis de leur enceinte. Pour reprendre Boullier, « Les objets communicants devront donc éviter de devenir des objets bavards et devront apprendre à ne pas couper les conversations, bref apprendre le

savoir-vivre, ce qui est après tout une bonne définition de la communication. »[596] Outre la question de la politesse humaine à avoir envers les enceintes, leur introduction dans nos phonotopes humains introduit également un nouveau régime de politesse cette fois propre aux enceintes elles-mêmes. Comment concevoir une enceinte qui ne soit pas une gêne, une *impolie*, qui ait du « savoir-vivre » ? D'après les retours des enquêtés de la présente thèse, le principal point sera donc de s'assurer que les réponses des enceintes soient les plus pertinentes possibles, d'abord, c'est-à-dire qu'elles occupent le moins inutilement possible leur part du phonotope au moment de s'exprimer. Une autre réponse, déjà apportée par certains fabricants, est de chercher à limiter tant que possible le temps sonore occupé par les enceintes. Il existe par exemple une fonction « réponses brèves » dans les paramètres d'Alexa permettant d'éviter qu'elle ne monopolise le phonotope trop longtemps. En somme, il faut à la fois maximiser le bénéfice tiré d'une intervention de l'enceinte, et minimiser en général son temps d'expression.

Un dernier point, ou plutôt un dernier contre-point, n'est évoqué comme souvent que par E5 : il est relatif à l'attitude de cet interlocuteur particulier qu'est l'assistant personnel, que E5 préfèrerait paradoxalement moins machinique :

> « Et il y a un autre élément, ça me semble... sociologiquement, psychologiquement ou anthropologiquement poser question. Heu... De mettre la facilité... Là t'as un interlocuteur qui est toujours favorable, qui ne te dit jamais non. Heu, ça me semble poser question de s'habituer à une confrontation avec...
> JF: Ouais.
> E5: ...un interlocuteur, parce que ça l'est, même si ce n'est pas une intelligence derrière ou une personne, heu...
> JF: Par le choix de design...
> E5: ...qui est toujours à ton ordre. (…) Un interlocuteur... S'habituer à des interactions dans lesquelles on te dit oui, ou ton interlocuteur ne peut que satisfaire, ne peut pas te remettre en question, dire "non, pourquoi tu fais ça ?".
> JF: (acquiesce)
> E5: "Non, on ne va pas allumer les lumières ! Non, on ne va pas allumer la clim ! Con, là il fait 24 degrés, voilà, il n'y a pas besoin !". Ça ne va pas te dire ça. Ça, ça pose question. »
> (entretien 2, 2 h 51 min)

S'interrogeant là encore sur les effets sociaux de la technique, E5 pointe ici que le fait qu'un assistant vocal cherche à ou doive toujours satisfaire aux requêtes de son propriétaire est en soi un problème. Cette attitude est clairement celle qui est attendue d'une machine, et E5 est gêné que l'anthropomorphisme de l'enceinte n'aille pas jusqu'à lui permettre de refuser un ordre ou

[596] D. BOULLIER, « Objets communicants, avez-vous donc une âme ? », *op. cit.*, § 9

de se rebiffer. Cet entre-deux lui semble problématique en cela qu'il habitue l'interlocuteur humain d'un assistant vocal à se voir répondre avec déférence et docilité, à ceci près que cette déférence et cette docilité qu'on peut juger utilement propres aux machines s'expriment ici avec les dehors de l'humanité. E5 craint en fait une transposition moins de l'attitude humaine sur la machine qu'une transposition de l'attitude humaine envers une machine pseudo-humaine vers des êtres humains effectifs. Il est encore difficile de dire à quel point cette crainte est ou sera justifiée.

Au-delà de ce cadrage général sur la conversation avec un objet, deux points plus spécifiques ont été évoqués en entretien de façon plus limitée : la question du genre, et celle de la prononciation et de la langue dans les requêtes aux assistants vocaux.

Genre et assistants vocaux

La question du genre a été assez peu abordée frontalement par les enquêtés. Au-delà de la question du genre par défaut de la voix des assistants (voir « La voix d'un robot n'est pas nécessairement robotique », p. 381), qui occupe davantage les réflexions savantes autour du design, la question de la différence entre voix masculines et féminines n'a été abordée spontanément que sous l'angle de la qualité de la reconnaissance vocale selon la voix de l'utilisateur ou de l'utilisatrice. E7 rapporte ainsi spontanément avoir remarqué que leur Google Home réagissait mieux aux voix graves :

> « E7: C'est marrant, elle n'entend pas les gens qui parlent aigu, aussi.
> E6: Oui, aussi.
> E7: Il faut parler avec une voix grave.
> E6: Elle a dû s'habituer à une voix grave.
> JF: Une voix de crooner !
> E7: Je sais pas, j'ai une pote avec une voix assez haut perchée, et quand elle lui parlait: pfffft (bruit avec la bouche signifiant un "bide") .
> E6: Du coup elle essayait de parler grave, et ça marchait. » (entretien 3 ; 6 min 05 s)

Son compagnon, E6, abonde aussitôt en son sens, mais ne l'aurait peut-être pas précisé de lui-même. Ni l'une, ni l'autre ne proposent immédiatement d'explication. Quand je leur suggère que cela peut tenir aux limites techniques des microphones, ils acceptent sans difficulté cette possibilité, là où le bagage technique d'E6 lui aurait vraisemblablement permis de suggérer également que cette meilleure compréhension des voix masculines pouvait également tenir aux biais d'apprentissage de l'IA de Google Assistant : il se contente d'évoquer la possibilité

qu'« elle » se soit « habituée à une voix grave », sans que le « elle » renvoie clairement à leur enceinte ou à Google Assistant en général.

La thématique du genre n'a donc pas réellement d'importance marquée pour les enquêtés, et n'a par ailleurs pas fait l'objet d'une question spécifique de ma part dans le guide d'entretien.

La question de la prononciation et de la langue

Bien que les fabricants d'enceintes connectées mettent en avant le naturel et la fluidité de la langue parlée pour interagir avec leurs produits, de nombreux éléments d'observation ou de retours des enquêtés laisse à penser que les enceintes amènent au contraire les utilisateurs à adopter une manière singulière de parler pour se faire comprendre de leur assistant.

Le phénomène est le plus manifeste sur l'expression du mot d'appel, qui est à la fois le plus décisif, puisque c'est lui qui permet de lancer l'interlocution, et aussi le plus couramment employé. À force de répétitions et d'échecs, les utilisateurs apprennent littéralement une façon efficace de s'adresser à leur enceinte, qui dépend notamment des limitations techniques de cette dernière. Quel que soit l'agent conversationnel, quelques constantes se dégagent :

- Le fait de parler à haute et intelligible voix ;
- Un ton relativement monocorde, voire robotique, qui fait comme un étonnant écho par anticipation avec la voix souvent robotique de l'agent conversationnel lui-même ;
- Une uniformité phonétique entre les différentes adresses, remarquable notamment quand la personne doit répéter plusieurs fois le mot d'appel. Même quand l'agacement commence à poindre dans le timbre de la personne, le réflexe est généralement de persévérer dans la même façon de parler, en haussant plus ou moins le volume de sa voix.

À titre personnel, j'ai également le réflexe de m'approcher de l'enceinte plutôt que de hausser la voix, pour peu que je sois déjà debout. Durant l'entretien 12, E18 a fait l'exemple malgré lui de la difficulté qu'il y a parfois à activer un assistant vocal, en l'occurrence sur son téléphone, répétant à de nombreuses reprises le mot d'éveil « Ok Google » sur un ton égal :

> « E18: (à son téléphone) Ok Google. Là il me dit, il me l'affiche.
> JF: Mais il ne réagit pas quand il est inerte ?
> [2962,0] E18: (il teste pendant quelques secondes) Ok Google. Ok Google. Non,

faut que je l'ouvre. (il continue de tester, et pour le coup ça fonctionne mal même quand l'appli est ouverte)
JF: On va découvrir que le téléphone est en panne.
E18: (nous rions) C'est ça !
[2981,8] E19: Ou qu'il est déchargé, parce que... (elle rit)
E18: Ok Google. Ok Google.
E19: Bon, écoute, il n'en veut pas, aujourd'hui.
E18: Quel est l'âge de François Hollande ? C'est actif. Ben, comment ça se fait, ça ? (il bidouille, ça ne répond pas)»
(entretien 12 ; 48 min 55 s)

Agacé de l'absence de réponse de son téléphone, il continuera à s'obstiner pendant que nous poursuivons l'entretien avec son épouse, finissant par obtenir la réponse à sa question.

Plus subtilement, il peut également s'agir d'adapter son accent pour être mieux compris de l'assistant vocal. E7 déclare ainsi son agacement vis-à-vis de Google Home lorsqu'elle souhaite lancer une chanson au titre en anglais sur Spotify : il lui faut alors prononcer le titre en anglais… mais avec un accent français.

« E7: En fait souvent je la contrôle limite avec le portable, parce que des fois ça me saoule de lui demander des chansons sur Spotify, parce qu'il faut lui parler avec un accent français.
JF: Faut lui demander une chanson en anglais, avec l'accent français ?
E7: Elle comprend pas, faut lui parler en français. Avec un bon accent. Du coup, ouais, souvent je la contrôle avec le portable, ce qui n'est pas du tout... utile, mais bon. »
(entretien 3 ; 9 min 12 s)

Il est difficile de confirmer ou d'infirmer ce ressenti, mais on peut faire l'hypothèse que les données d'entrainement des dialogueurs ont pris en compte l'accent français pour les requêtes en anglais faites à la version francophone des assistants vocaux, ou en tout cas ici de Google Assistant.

*

In fine, et contre la tendance parfois fantasmée à l'anthropomorphisme de ces nouveaux interlocuteurs, qu'il soit projeté *sur* ou *depuis* l'assistant vocal, il semble aujourd'hui que les formes spécifiques du « savoir-vivre » qui continuent d'être attendues par les humains vis-à-vis de ces objets les inscrivent toujours bel et bien dans le non-vivant.

IV - UNE NOUVELLE DIMENSION PROXEMIQUE DE LA FAMILIARITE

Quoique la conversation avec une enceinte et des objets connectés ne soit pas tout à fait assimilée à une interaction humaine, même chez les utilisateurs les plus enthousiastes, leur présence n'en est pas moins intégrée dans une forme de sociabilité quasi humaine. Cet état de fait est manifeste dans la conversation, mais qu'en est-il des micro-rapports spatiaux au sein du logis ? Comment sont gérées les relations avec les autres utilisateurs et membres de la famille en présence d'une enceinte connectée ?

Impacts sur la proxémie familiale

On l'a vu avec l'exemple de la *Aware Home* initialement pensée pour le maintien à domicile de personnes âgées, la question du *care* et de la famille sont aux prémisses des expérimentations sur le logis connecté. De fait, dans la culture occidentale, « l'espace domestique est familial. C'est celui du ménage, du foyer peut-on dire plus justement pour prendre en compte les personnes qui vivent seules »[597]. Il n'est donc pas étonnant que la domotique connectée traite volontiers de la question des rapports entre membres de la famille au sein de cet espace. La gamme d'objets connectés de la marque Mother, articulés autour d'un *hub* qui évoque fortement une enceinte connectée, en est emblématique. Ils permettent par exemple d'associer des *tags* à des objets (ou des personnes, et singulièrement des enfants) pour pouvoir les retrouver plus facilement, à la manière des Air Tags popularisés tout récemment par Apple. Dans les cas les plus extrêmes, la supervision des enfants peut même être déléguée à des objets connectés, comme des lampes de bureau surveillant les enfants pendant leurs devoirs et pouvant même répondre à des questions simples pour les y aider[598]. Ces pratiques s'inscrivent donc non seulement dans la conversation familiale, mais aussi dans sa proxémie, comprise comme « la gestion et la représentation par les individus des distances acceptables et souhaitables entre eux et les autres », qui se donne à lire à travers les pratiques spatiales résultant notamment des « schèmes culturels en cours dans la société » considérée[599].

L'augmentation de l'espace et des spatialités par des médiations numériques vaut aussi pour la proxémie en tant qu'elle est une des formes des pratiques spatiales. Cette augmentation de la proxémie peut engendrer des pratiques de surveillance nouvelles, dont le *proctoring* des

[597] J.-F. STASZAK, « L'espace domestique », *op. cit.*, p. 345
[598] L. LIN, « A Smart Lamp That Watches Kids When They Study Is a Hit in China », *Wall Street Journal*, 31 mai 2021 (en ligne : https://www.wsj.com/articles/a-smart-lamp-that-watches-kids-when-they-study-is-a-hit-in-china-11622466002 ; consulté le 29 décembre 2022)
[599] M. LUSSAULT, « Proxémie », dans J. Lévy et M. Lussault (éd.), *Dictionnaire de la géographie et de l'espace des sociétés*, Paris (France), Belin, 2003, p. 750-751

enfants par la lampe connectée sus-citée n'est qu'une déclinaison. Mais il s'agit là d'un cas qui, pour avoir fait sensation en Chine, ne se retrouve pas dans les entretiens. En réalité, l'essentiel des pratiques évoquées par les enquêtées sont encore aujourd'hui assez banales. J'ai déjà évoqué les questions de concurrence pour le phonotope qui ne diffèrent pas sensiblement de cas déjà connus comme la question de la maîtrise de la télévision et de sa télécommande dans une pièce comme le salon, qui peut rassembler des habitants comme en inciter d'autres à quitter la pièce. Plus spécifiquement aux assistants vocaux des enceintes connectées, deux effets proxémiques émergent dans les entretiens.

Le premier relève de la convivialité, du jeu en famille avec l'enceinte. Ce moment est marquant surtout au moment de l'installation de l'enceinte, qui suscite toujours la curiosité et divers jeux. Il s'agit alors d'apprivoiser l'appareil en lui posant pléthore de questions, sérieuses ou farfelues, afin d'en tester l'intérêt, les limites ou encore l'humour. Ce moment paroxystique n'a qu'un temps, éventuellement renouvelé lors de la visite de personnes étrangères au foyer et à l'utilisation d'enceintes connectées, qui peuvent être tentées de jouer à leur tour cette scène initiatique. Ce moment est crucial : les usages possibles de l'enceinte identifiés dans les premières heures d'utilisation sont les plus susceptibles d'être utilisés par la suite, les utilisateurs installant peu de nouvelles applications et découvrant peu de nouvelles requêtes par la suite. De fait, une fois intégrée au quotidien, l'enceinte ne suscite plus autant d'intérêt. Ponctuellement, des jeux pourront à nouveau rassembler des membres du foyer autour de l'enceinte, en particulier en présence d'enfants. E3 rapporte ainsi utiliser volontiers l'enceinte avec son nouveau-né pour lui faire écouter les cris de tels ou tels animaux.

Le deuxième relève de la diffusion d'informations d'intérêt familial dans la maisonnée. Plutôt bien mise en avant dans la communication des fabricants, cette fonction n'est utilisée dans notre panel que par E8, qui est le seul à pouvoir tirer parti de cette fonctionnalité avec son réseau de cinq ou six Echo répartis jusque dans les chambres de ses enfants. Il s'agit par exemple d'appeler tout le monde à table, de prévenir de son retour, etc. Les enceintes jouent ici un rôle de haut-parleur qui a davantage de sens dans les intérieurs vastes et/ou avec plusieurs étages, comme dans le cas de son pavillon en banlieue d'une métropole du sud-ouest de la France. Quoique banal et apparemment très limité, cet usage reste intéressant en cela qu'il montre quel est l'intérêt et la forme d'une augmentation proxémique grâce au numérique : il s'agit ici de ne pas se déplacer physiquement de pièce en pièce, mais de diffuser tout de même une information d'intérêt général sous forme vocale *via* les enceintes de chacun. On pourrait objecter que, dans la majorité des logements, héler la famille produit le même effet sans besoin

de médiation numérique. L'usage de l'enceinte a néanmoins pour intérêt, qui devrait plus se faire sentir à terme, d'interrompre les activités liées à chaque enceinte dans chaque pièce. Le cas le plus courant actuellement est l'écoute de musique : un enfant qui écouterait de la musique à fort volume pourrait ne pas entendre (ou prétendre ne pas entendre) l'appel de ses parents. S'il écoute sa musique sur une enceinte connectée du même réseau, cette notification lui sera transmise en baissant momentanément le son de la musique qu'il écoute. Si les enceintes ou leurs équivalents futurs devaient se généraliser, et si leur rôle de *hub* pour l'IoT (et pas seulement la domotique) se pérennisait voire se renforçait à mesurer que de plus en plus d'objets y seront connectés, les parents pourraient avoir à terme un pied numérique dans chaque pièce équipée d'une enceinte, et une certaine maîtrise sur les objets liés. L'enceinte connectée pourrait ainsi amplifier considérablement les pratiques dites de contrôle parental, sans nécessiter la présence physique du parent qui pour vérifier quelle émission est regardée ou écoutée dans telle chambre, ou pour imposer un couvre-feu des outils numériques dans telle autre. De même que l'intégration d'une enceinte dans un foyer y fait pénétrer les acteurs extérieurs ayant accès aux capteurs et effecteurs qui lui sont liés, chaque pièce individuelle équipée d'une enceinte y fait pénétrer la ou les personnes ayant les droits informatiques les plus élevés dans ce réseau local domestique.

La question des tiers dans un espace de captation sonore et vidéo

Outre les membres de la famille, qui sont concernés au premier chef par les usages des enceintes connectées, se pose également la question du traitement des tiers relativement à l'IoT domestique. On a vu que divers dispositifs permettaient de gérer le seuil du logis (voir « Le domicile : des limites à la fois plus poreuses et plus fortes », p. 349). Une fois à l'intérieur, comment se règlent les rapports aux tiers ?

La présence de tiers active puissamment la thématique immunitaire et la question du consentement. Il est acquis qu'un intrus n'a pas son mot à dire sur la captation de données le concernant. Le droit consacre même la possibilité pour les particuliers de surveiller leur propriété, y compris au moyen de la vidéo, et cette pratique soutient un opulent marché fondé sur la vidéosurveillance et les alarmes. Cette libéralité ne s'étend en revanche pas au traitement et à la diffusion de ces données, comme cela a été évoqué par E14 et E15 dans l'entretien 9, à propos d'un voleur de boîtes aux lettres dans le hall de leur copropriété, dont ils ont pu observer les agissements sans pouvoir faire autre chose que de transmettre les bandes à la police. Si l'on excepte les cas d'intrusion, la situation devient moins claire, mais plus riche.

D’abord, la question du consentement peut se poser pour le tiers invité à entrer. Le droit européen entérine le fait que chacun doit être informé et libre de refuser le traitement de ses données personnelles. L’habitant d’un logement connecté est responsable du traitement des données relatives à ses invités. Dans les faits cependant, le problème relève moins de la loi que du savoir-vivre. Tous les enquêtés utilisateurs d’enceinte avec qui le sujet a été évoqué ont spontanément ou sur demande affirmé qu’ils étaient tout à fait disposés à couper leurs appareils connectés captant des données sur demande. Il s’agit même d’une recommandation des fabricants d’objets connectés. Une page du site de support technique pour les produits de la gamme Nest de Alphabet/Google, qui inclut des outils de surveillance, décrit de manière étonnamment détaillée comment « respecter la vie privée d'autrui lorsque vous utilisez les produits Nest[600] ». Pour autant, E5 est sceptique sur le fait que les utilisateurs feront attention à prévenir leurs hôtes.

> « JF: Je ne sais pas, tu ne penses pas que ça pourrait se régler comme par exemple, je sais pas, tu as des amis musulmans qui viennent chez toi et qui te demandent "est-ce qu'il n'y a pas de porc ou quoi que ce soit dans les plats, etc.". Ça pourrait devenir une espèce de règle de politesse.
> E5: Ça pourrait devenir (il insiste sur devenir) . Je ne pense pas que aujourd'hui il soit jouable de rentrer chez quelqu'un et de dire "tu le débranches ? il est connecté ? non ? je veux bien que tu le débranches". Heu... [1007,4] Bon, je pense que les gens qui adoptent ça ont une posture technophile, enthousiaste, qui est soit insouciante, soit assumée, qui est orthogonale à ce genre de préoccupations (…)

Selon lui, personne ne posera jamais vraiment cette question. Il me donne l’exemple de son frère, utilisateur de Siri sur son téléphone :

> « (…) Heu, voilà. Je sais que, à un moment donné mon frère, mon frère il est... enthousiaste de tous les produits Apple. Mon frère à un moment donné un jour a... a parlé à Siri qui était sur son téléphone, à deux mètres de lui. Donc aucune interaction (physique) , Siri répond, et moi je suis resté un peu... je me suis raidi. Et... [1061,5] voilà, parce que ça voulait dire que Siri était constamment en train d'écouter pour réagir à une impulsion. C'était pas comme ça, au début, en fait. Au début c'était... il fallait une action physique sur le dispositif.
> JF: (acquiesce)
> E5: Et c'est quoi, depuis deux ans, un an et demi que c'est comme ça...?
> JF: Je ne sais plus, mais effectivement maintenant...
> E5: Je pense que c'était, ouais, 2015 que c'est arrivé, ça.
> JF: Ou tu lui dis juste "dis Siri", il s'active...

[600] « Conseils pour respecter la vie privée d’autrui lorsque vous utilisez les produits Nest », sur *Aide Google Nest*, s. d. (en ligne : https://support.google.com/googlenest/answer/9247517?hl=fr-LU ; consulté le 19 mars 2022)

E5: Ouais ! »
(entretien 2 ; 16 min 20 s)

Le téléphone n'est certes pas du tout un dispositif aussi suspect, on l'a vu, que l'enceinte. Il se fond aujourd'hui davantage dans le quotidien, mais E5 est suffisamment bien informé pour savoir que les enjeux techniques sont les mêmes qu'avec une enceinte. Comme E5 avec son frère, E1, un des enquêtés de la phase préparatoire du guide d'entretien, a aussi eu une réaction épidermique à la présence d'un Echo dans mon propre appartement lorsque je l'ai activé en sa présence, et alors même qu'il était au courant du fait que j'avais une enceinte connectée en test chez moi. Pour autant, E5 a sans doute raison quant au fait qu'il sera bientôt saugrenu de faire de telles demandes concernant les enceintes. Les deux seuls cas où des enquêtés-utilisateurs ont évoqué sérieusement le fait de désactiver leur assistant vocal concernaient la confidentialité de leur travail, lors de réunions où des téléphones se sont manifestés par hasard, ou des discussions politiques dans une famille où des ambitions et une stratégie électorales précises ont été exprimées. Mais dans la vie quotidienne, il est peu probable qu'ils informeront leurs visiteurs de la collecte de données dont ils pourraient faire l'objet. De même, pour les personnes ne souhaitant pas être soumises à une captation de données, il est peu probable qu'elles feront la démarche de réclamer la déconnexion d'une enceinte connectée ou même d'une webcam. E20, qui manifeste pourtant de l'assurance durant son entretien, rapporte ainsi qu'elle a demandé à une amie proche de déplacer son Echo dans une autre pièce lors d'une visite (voir « E20 : aménager un lieu de vie qui n'est pas le sien », p. 343), en croyant régler le problème par une mise à distance des micros. Pour autant, elle est aussi convaincue de ne jamais oser une telle demande chez une personne moins familière :

> « Là c'était une soirée nanas à deux, tranquilles pénards, heu en fait quand je suis chez moi j'aime bien être chez moi. Là c'est une amie très proche, enfin chez elle je me sens chez moi, quoi. C'est vrai que quand je vais chez des amis, si on fait une soirée à vingt ou à même à quatre cinq dans un appart et si c'est pas quelqu'un dont je suis très très proche, je ne vais pas non plus lui parler de son enceinte. Je m'impose pas comme ça, quoi. »
> (entretien 13, 7 min 30 s)

Je fais donc l'hypothèse que, quoique de telles requêtes sont donc plausibles entre familiers et/ou dans les cas d'activation directe d'un assistant vocal ou de tout autre objet connecté pouvant collecter des données en présence d'un tiers réticent, la normalisation des enceintes connectés devraient bientôt faire apparaître ces demandes de désactivation comme saugrenues.

Dans un registre non-conflictuel, ensuite, la manière d'adapter sa *smart home* à ses invités pourrait devenir au contraire un nouvel outil social permettant de marquer la familiarité, en intégrant des non-résidents dans l'utilisation de l'IoT domestique. Qui me rend suffisamment visite pour qu'il ait fini par enregistrer le mot de passe de mon routeur Wi-Fi ? À qui vais-je accorder un usage « invité » sur mes appareils ? À qui vais-je laisser utiliser mon enceinte, voire offrir de se créer son profil vocal ? E18 et E19, qui sont pourtant très méfiants vis-à-vis des détournements de données personnelles, voire de l'outil informatique en général, me rapportent ainsi qu'ils n'ont eu aucun problème à confier à leur fils leurs identifiants et à lui laisser un accès total à leur ordinateur, comme s'il s'agissait d'une évidence du savoir-vivre[601]. Plus prudents et très au fait du paramétrage de leurs outils informatiques, E14 et E15 mettent quant à eux leur HomePod en mode invité quand ils organisent une fête, afin de ne pas polluer leur profil Spotify à partir des requêtes d'autrui. On peut cependant imaginer que ne pas activer ce mode en présence de personnes choisies pourrait aussi devenir à terme une marque d'affection ou une façon de renforcer le lien.

Mettre l'autre à distance par les objets connectés

Hors du cercle des habitants et de leurs familiers, la mise à distance d'autrui me semble même être une des principales finalités de la domotique connectée. C'est le cas par exemple avec les compteurs connectés comme Linky, qui permet de ne pas avoir à accueillir et à interagir avec un agent d'Enedis pour la relève du compteur. C'est aussi bien sûr le cas avec les digicodes et plus encore aujourd'hui avec les sonnettes et serrures connectées, qui permettent même d'ouvrir à distance à un livreur sans avoir à se rendre jusqu'à la porte d'entrée. Le journaliste Andrew Gebhart décrit cette fonction des Doorbells de la marque Ring sans détour, voire avec un certain cynisme : il s'agit de pouvoir éviter son voisin, de ne pas avoir à interagir avec le livreur, et d'aller jusqu'à déléguer à sa sonnette la responsabilité d'un échange vocal avec ceux-ci[602]. On retrouve ici toute l'ambivalence de la notion d'immunité numérique du domicile détaillée dans la partie « Le domicile : des limites à la fois plus poreuses et plus fortes », p. 349.

[601] Il s'agit de l'attitude qui m'a le plus couramment été rapportée par les enquêtés, à l'exception près du téléphone qui reste souvent un objet personnel. La seule exception est E17, qui préfère garder un œil sur l'activité de sa sœur y compris sur son ordinateur de bureau. De la même façon qu'il était le seul des enquêtés à déclarer ne pas changer de comportement qu'il soit chez lui ou à l'extérieur, cette façon d'agir particulière est sans doute liée au passé d'une partie de sa famille ayant vécu sous un régime dictatorial.

[602] A. GEBHART, « How to use the automatic responses on Ring Doorbells », *CNET*, 29 juillet 2021 (en ligne : https://www.cnet.com/home/smart-home/how-to-use-the-automatic-responses-on-ring-doorbells/ ; consulté le 9 août 2021)

CONCLUSION PARTIELLE

En conclusion, l'enceinte connectée et ses périphériques domotiques sont bien sûr des objets techniques, mais ils sont avant tout des dispositifs sociaux à l'autonomie grandissante. La majorité des fonctions des objets de l'IoT domestique ne sont pas nouvelles, ni techniquement surprenantes. Leur intégration réticulaire horizontale (entre objets au sein du logis) et verticale (vers les serveurs de leurs fabricants) bouscule certes les processus immunitaires qui étaient jusqu'ici à l'œuvre autour de l'espace domestique. Mais l'essentiel de l'innovation tient à leur pilotage par un objet capable de conversation et d'une relative autonomie décisionnelle qui s'intègre désormais en tant que tel, et non comme simple médium, à nos sociabilités domestiques.

CONCLUSION

« Gadget, subst. masc. A. - Petit objet qui plaît plus par sa nouveauté et son originalité que par son utilité. (…) B. - P. ext. Solution miracle. »
Trésor de la langue Française informatisé, 1994

UN GADGET SANS PERENNITE ?

Il peut sembler étonnant de terminer la réflexion que nous avons menée jusque-là autour de l'enceinte connectée, de ses effets et de ses implications sur un terme qui la renvoie à la dimension la plus triviale, celle du gadget. L'enceinte connectée peut finalement apparaître comme un simple petit objet qui plairait avant tout par sa nouveauté, pas forcément utile, tout en étant parfois aussi présenté comme une solution miracle par certaines personnes ou par leurs fabricants. Toutes les acceptions du terme s'y appliquent. En tout état de cause, le fait de parler de gadget est tout sauf anodin pour les personnes interrogées. Il a été utilisé dans douze entretiens par treize enquêtés différents. Mais surtout, il a été utilisé spontanément par douze de ces enquêtés, alors qu'il était absent du guide d'entretien. Sur environ 10 000 formes uniques de mots, il est au 460e rang en termes de fréquence, avec 35 occurrences. Si l'on ne retient maintenant dans cette liste que les concepts et qu'on excepte les termes présents dans le guide d'entretien, « gadget » n'est devancé que par « humain » (53 occurrences) et « liberté » (46 occurrences).

Que les enquêtés l'utilisent ou non, l'enceinte est généralement ramenée à ce statut de gadget, dans toute la polysémie de ce terme. D'une part, il s'agit de mettre en avant ses multiples fonctionnalités, sa dimension presque magique qui permet à un monde de références jusque-là science-fictionnelles de faire irruption dans l'espace domestique et d'enchanter le quotidien. D'autre part, il s'agit aussi de ramener l'objet à son caractère dispensable et amusant, tant pour pointer ses limitations encore importantes, en particulier dans le contexte français, mais aussi pour s'accommoder de son étrangeté, voire pour mettre à distance des craintes, qui

subsistent dans le discours même des plus technophiles, en en faisant un dispositif véniel. Un enquêté potentiel dont la compagne manifestait de l'intérêt pour le rayon des enceintes connectées dans le centre commercial du Millénaire a rapidement balayé le sujet de l'enceinte connectée (et ma requête d'entretien) : « c'est la bêtise humaine », une babiole pour amuser ses enfants. La plupart des enquêtés-utilisateurs insistent quant à eux très souvent sur le jeu avec l'enceinte, qu'il s'agisse de lui demander des blagues, de deviner des capitales ou de créer des scénarios plus ou moins complexes selon le nombre d'objets connectés.

Si l'enceinte connectée en tant que telle ne me semble pas devoir rester durablement l'objet central de l'IoT domestique, il s'agit néanmoins d'un point de focalisation temporaire nous éclairant sur des trajectoires techniques et des problématiques sociales à plus long terme.

L'adjonction dans l'enceinte connectée d'un logiciel de dialogue, de capteurs, d'effecteurs, et d'une certaine capacité décisionnelle fondée sur le profilage de ses utilisateurs nous fait passer un nouveau cap de l'ère numérique. Les fonctions conversationnelles sont la principale technologie de rupture de l'enceinte connectée, mais l'innovation consiste également dans le design qui l'associe aux autres fonctions citées. Cette innovation n'est donc pas seulement ou pas foncièrement technique, mais avant tout sociale et singulièrement spatiale. Même si le dispositif de l'enceinte connectée ne devait pas subsister longtemps sous sa forme actuelle, il est le premier à nous accoutumer massivement à intégrer des machines dans nos relations sociales non pas comme moyen de communication avec d'autres humains, mais comme des interlocuteurs quotidiens. Quoiqu'ils soient encore loin d'être autonomes, ces dispositifs ne sont pas seulement des outils, plus tout à fait de simples actants, mais bien de véritables agents en devenir à qui déléguer une part toujours plus grande de la gestion de nos espaces et de nos spatialités du quotidien. Ils préfigurent de nouvelles proxémies domestiques et de nouveaux modes de communication entre habitants d'un logis en faisant de l'assistant vocal un interlocuteur possible, à même de porter la voix des habitants et de prendre en charge les transferts d'information inter-individuelles et le pilotage d'effecteurs toujours plus nombreux.

Au-delà de ses fonctions propres, l'enceinte connectée est un hub, une porte d'entrée vers des périphériques dont le nombre va croissant et qui constituent l'IoT domestique. Ainsi connecté, le logis devenu *smart home* n'est plus un volume d'espace dont on prend soin et dans lequel on dispose d'outils à manipuler, mais un système machinique de plus en plus automatisé dont on pilote les paramètres et les fonctionnalités selon des designs et des spécifications qui nous échappent en large partie. De ce point de vue, ce nouvel âge de la technologie domotique

contribue à l'artificialisation croissante des espaces habités, et accompagne la trajectoire identifiée par Peter Sloterdijk dont l'horizon est de construire les lieux d'habitat sur le modèle des stations spatiales : des lieux au volume d'air fermé, sous *monitoring* constant d'une station de base qui leur est extérieure, et qui sont à la fois extrêmement équipés et automatisés. Certaines des fonctionnalités de ces habitats machinisés devraient avoir de puissants effets spatiaux, en particulier les systèmes associant serrures connectées et webcam, qui changent fondamentalement le rôle de la porte et du seuil du logis.

À court terme, l'enceinte connectée est en fait autant le symbole de l'avènement de la domotique connectée que le symptôme de la limitation actuelle du potentiel offert par l'augmentation des espaces domestiques. La nécessité de l'enceinte telle qu'elle existe aujourd'hui nait de trois limitations dans la domotique connectée :

- Le pilotage de la domotique requiert la présence d'un réseau de télécommunication pour relier capteurs et effecteurs de l'IoT. En somme, il faut une antenne et un routeur par logement, voire par pièce ;
- L'éclatement des protocoles de communication dans l'IoT et des profils utilisateurs. Par rapport aux systèmes domotiques préexistants, les enceintes connectées permettent un premier moment d'adaptation autour des produits de quelques grandes entreprises et la connexion à leurs bases de données utilisateurs déjà très fournies ;
- L'absence d'une norme pour l'installation de capacités domotiques par défaut dans l'habitat, comme les normes qui imposent aujourd'hui la connexion des logements au réseau électrique, un certain nombre de prises par pièce, etc.

De ce point de vue, et malgré son caractère apparemment innovant, l'enceinte connectée est en réalité le signe d'une augmentation numérique encore très rudimentaire de nos espaces de vie. Pour reprendre la comparaison habituelle avec la téléphonie mobile, l'enceinte connectée est à la domotique connectée ce qu'était le téléphone fixe à la télécommunication. Pour l'utilisateur contemporain du *smartphone*, il paraît complètement désuet d'avoir été attaché (littéralement) à une ligne de cuivre, de n'avoir pu communiquer que du son et aucun autre média, de façon obligatoirement synchrone, et même, dans les premiers temps, d'avoir dépendu d'opérateurs humains pour la mise en relation avec son interlocuteur[603]. Pour autant, l'arrivée du téléphone

[603] De la même façon que de nombreux opérateurs humains sont encore aujourd'hui nécessaires pour corriger les modèles des logiciels de TALN.

fixe dans chaque foyer a été la première étape de l'individualisation des capacités de télécommunication, et le prélude à la situation actuelle dans laquelle nous pouvons communiquer vocalement et visuellement avec la quasi-totalité de nos contemporains à l'échelle du monde en n'ayant qu'à sortir un objet de quelques dizaines de grammes de nos poches.

Ainsi, à plus long terme, c'est tout l'espace habité qui pourrait être impliqué dans les dynamiques actuellement observables dans l'espace domestique. Notre profil numérique comme habitant, la manière dont nous habitons nos logis augmentés, pourrait permettre la constitution d'un nouvel ensemble de clés dans les trousseaux de nos habitèles. De la même manière que les interfaces de nos réseaux sociaux ou les publicités qui nous sont soumises sont personnalisées selon notre profil comme consommateur, les lieux connectés et machinisés où nous nous rendons pourraient finir par être à leur tour physiquement uniformisés selon notre profil comme habitant. Une chambre d'hôtel pourrait préconfigurer selon mes goûts l'éclairage de la pièce ou les services de *streaming* vidéo proposés par le téléviseur. Une voiture autonome pourrait régler son chauffage à la température de confort inférée à partir de mon réglage habituel à domicile – voire selon la manière dont je me serai vêtu ce matin-là.

LE VERTIGE SPATIAL DE L'ERE NUMERIQUE

Nous l'avons vu, le numérique n'abolit pas l'espace topographique, il l'augmente au contraire de spatialités nouvelles qui le transforment et le réorganisent. L'avènement de la domotique connectée est le grand processus de numérisation du Monde actuellement. Après avoir outillé les espaces publics et accompagné nos pratiques nomades, le numérique s'étend désormais à l'augmentation de l'espace domestique.

Si l'on considère ce développement du point de vue des acteurs économiques, il y a un véritable *spatial fix* en cours initié par certaines des entreprises les plus puissantes aujourd'hui, au premier rang desquelles Alphabet/Google et Amazon. Leur modèle d'affaires fondé sur le capitalisme de surveillance trouve dans l'espace domestique de nouveaux débouchés. Si l'on se place du côté des individus, la domotique connectée consiste en la mise en relation du foyer et du « vaste monde » auquel ouvrent les médiations numériques. Il ne s'agit plus seulement d'y recevoir de l'information diffusée de l'extérieur, comme avec la télévision et même quelque peu encore avec Internet : l'espace domestique en tant que tel produit désormais des données qui ne sont plus encloses en ses murs, et il est également agi de l'extérieur. Ce vertige spatial

des individus fait écho à celui de la discipline géographique face à l'émergence de la « société d'information » à la fin du XXe siècle, en un moment où ses concepts et outils traditionnellement tournés vers la matérialité et le territoire ont dû être adaptés à la réalité nouvelle d'un Monde où les échanges immatériels et réticulaires se sont imposés comme des forces déterminantes dans la production de l'espace et des spatialités[604]. De la même manière, la domotique connectée met les individus face à une forme d'isotropisation des espaces domestiques du point de vue de la captation et de la circulation des données (voir « Internet et la « fin de l'espace » », p. 72), alors que le logis pouvait encore jusqu'ici faire figure d'espace du privé, du particulier, de rupture avec l'espace public et le monde.

Ainsi, les perceptions et discours très négatifs à propos des enceintes connectées vues comme des « mouchards dans le salon » sont révélateurs d'un sentiment d'écrasement de l'espace domestique, d'échelle micro, par des acteurs du numérique opérant, eux, à l'échelle mondiale. La question de la défense de la vie privée est centrale dans le discours d'opposition aux enceintes et à la domotique connectée. Elle est présentée comme le principal enjeu exposé dans cette mise en relation dissymétrique entre l'espace des individus et les moyens des géants du numérique. Au terme de cette thèse, il semble que la focalisation autour de la notion de vie privée dans la conversation sur la domotique connectée tient au moins autant à la volonté des individus de protéger leurs données personnelles qu'elle est convoquée comme étant le vocable symbolique permettant en réalité de signifier l'attachement à (et la crainte de perdre) ce qui fait domicile, ce qui marque la singularité du logis comme espace.

L'opposition aux enceintes connectées au nom de la protection de la vie privée, qui est à prendre au sérieux au premier degré contre les tenants d'un *privacy paradox*, est donc au second degré et au moins autant une façon de verbaliser un vertige face à la disproportion des échelles des pratiques mises en interspatialité par le numérique domestique. En témoigne un des résultats les plus intéressants de cette thèse, à savoir que des opposants virulents aux enceintes connectées peuvent être des utilisateurs assidus de leur *smartphone*. Si cette attitude peut sembler contradictoire au premier degré, elle ne l'est pas quand on considère la question d'un point de vue spatial. Le *smartphone* nous suit partout, et c'est justement pour cela qu'il n'est pas aussi mal perçu que l'enceinte connectée du point de vue de la protection de la vie privée alors même que son potentiel en termes de surveillance et d'exploitation du « surplus

[604] Il s'est agi d'un moment de transformation épistémologique majeur au cours duquel « la géographie, [a été] amenée à reconsidérer ses schémas d'analyse scalaires et temporels face à l'intrusion de plus en plus [p. 436] massive et influente des techniques d'information et de communication » *in* E. EVENO, « Pour une géographie de la Société de l'Information », *op. cit.*, p. 435-436

comportemental » des individus est beaucoup plus grand. L'enceinte, elle, est fixée au domicile. Quoique moins « dangereuse » techniquement, elle rend beaucoup plus visible cette captation des traces de nos pratiques quotidiennes. En outre, elle refait puissamment surgir une conscience de l'espace de nos pratiques en augmentant numériquement un géotype psychiquement très structurant et plus que symbolique : le logis.

L'AVENIR DU LOGIS ET DE L'HABITER AUGMENTE

En permettant l'irruption d'une *voix* et d'*oreilles* dans nos intérieurs, l'enceinte connectée a puissamment contribué à un retour réflexif sur l'espace domestique, jusqu'ici assez négligé par les sciences sociales et par la géographie[605]. Au-delà de ce qui est parfois perçu comme une prédation des pratiques censément privées que les murs des logis dérobaient jusqu'ici aux regards et aux oreilles indiscrètes, l'IoT et la domotique redonnent également de l'importance au géotype éminemment topographique qu'est le domicile, entérinant là encore l'idée que le numérique n'abolit pas l'espace. De ce point de vue, la domotique connectée participe aussi à des processus qui lui préexistaient, comme la tendance au repli domestique observée dans les années 1980 déjà[606]. Là encore, elle vient pour ainsi dire augmenter numériquement ce repli domestique, en donnant aux individus toujours plus d'outils (et de prétextes) pour personnaliser et aménager leur intérieur, ainsi que pour s'éviter les contraintes de la sortie de chez soi, fusse pour des activités aussi triviales que de faire des courses ou de vérifier sa boite aux lettres.

Un autre résultat de cette thèse est donc de voir que, paradoxalement, les espaces domestiques se trouvent aussi revivifiés à la fois comme espaces topographiques et comme lieux emblématiques du privé… par des dispositifs réticulaires qui contribuent à les rendre transparents au Monde. Les matériels et logiciels de l'IoT domestique mettent en évidence dans le domaine numérique l'activité immunitaire de repli domestique qu'ils supportent autant qu'ils en sont le produit. Partant, il importe de dépasser les discours de premier degré s'arrêtant au caractère intrusif des enceintes et de la domotique connectées, ou à l'inconséquence de leurs utilisateurs, pour s'interroger sur les moyens d'accompagner cette activité immunitaire nouvelle. La régulation est ici fondamentale, tant pour informer les utilisateurs sur les possibilités qui leur

[605] Il faut tout de même admettre que, entre le début et la fin de ce travail de recherche, la pandémie de covid-19 et les confinements à domicile associés auront extraordinairement stimulé la réflexion collective sur l'espace domestique.
[606] J.-C. KAUFMANN, *La chaleur du foyer. Analyse du repli domestique*, *op. cit.*

sont offertes en la matière que pour contraindre les fabricants à accompagner ces attentes légitimes.

*

En nous faisant prendre conscience de la fragilité immunitaire du domicile, les nouveaux outils de la domotique connectée nous amènent à un virage intéressant dans la pensée de l'habiter contemporain, qui est à dissocier du seul logis. Pour reprendre Michel Lussault : « S'il importe donc de conserver une place éminente à la résidence, il convient de ne pas rabattre sur elle toute l'analyse. L'habitat est en vérité un objet bien plus protéiforme et complexe : l'espace socialement construit de l'existence humaine, généralement centrée sur le logis (…) Chaque individu arrange son habitat qui cristallise même l'identité personnelle (…). Cette identité est donc intrinsèquement spatiale »[607]. De fait, l'enceinte connectée et ses périphériques participent au regain d'intérêt contemporain pour le géotype territorial et privé le plus classique qui soit, et ce recentrement se fait à travers des outils paradoxalement fondés avant tout sur les spatialités, l'immatérialité et la réticularité. En questionnant l'augmentation numérique de l'habitat, la domotique connectée nous invite finalement à renouveler notre lecture de ce qu'est l'habitation du Monde.

[607] M. LUSSAULT, *L'homme spatial*, *op. cit.*, p. 349

ANNEXES

QUESTIONNAIRE POUR LES UTILISATEURS D'ENCEINTES CONNECTEES

Vous êtes libre de ne pas répondre à toute question qui vous gêne.

Sentez-vous libre de développer votre point de vue au-delà du seul cadre de la question, ou de me questionner sur le sens des questions. Il s'agit d'une conversation, mes questions sont secondaires par rapport à votre avis.

USAGES DES ASSISTANTS DOMESTIQUES

- Depuis quand possédez-vous une enceinte connectée ?
- Qu'est-ce qui a motivé son acquisition ?
  - Pourquoi le choix de cette marque ?
- Quels sont les usages les plus courants que vous faites de votre enceinte connectée ?
- Où sont situées la ou les enceintes connectées dans votre domicile ?
  - En mettriez-vous une dans votre chambre ?
- À votre connaissance, quels sont les autres appareils connectés dans votre domicile ?
- Quels appareils sont connectés à votre enceinte connectée ?
- Quelles applications et services web sont connectés à votre enceinte connectée ?
- Votre enceinte connectée vous a-t-elle parfois surpris, en bien ou en mal ?
- Utilisez-vous d'autres assistants personnels sur vos autres appareils, comme Siri ou Cortana ?
- Au compte Google / Amazon / Apple de quelle personne est liée votre enceinte connectée ?

- Pourquoi ce choix ?

- Comment les autres personnes de votre foyer utilisent-elles l'enceinte connectée ?

- Avez-vous parfois des conflits autour de l'utilisation de l'enceinte connectée ?

- Êtes-vous familier de l'application smartphone pilotant votre enceinte connectée ?

- Me montreriez-vous comment vous l'utilisez ?

AUTRES DISPOSITIFS DOMOTIQUES

LINKY

Connaissez-vous Linky ? En êtes-vous équipé ? Que pensez-vous de ce dispositif ?

Préférez-vous qu'un agent ERDF (ou autre) se rende chez vous pour relever le compteur ?

SERRURES CONNECTEES

Connaissez-vous les serrures connectées Amazon Key, August Access (non disponibles en France) ou de marque Somfy ?

Que pensez-vous de ce dispositif ?

Accepteriez-vous de l'utiliser ? À quelles conditions ?

VIDEOSURVEILLANCE DU DOMICILE

Connaissez-vous les caméras à reconnaissance faciale (ex : marque Netatmo) reconnaissant les membres de la famille quand ils rentrent au domicile ?

Que pensez-vous de ce dispositif ?

VOTRE NOTION DE LA VIE PRIVEE

LA VIE PRIVEE EN GENERAL

Comment définiriez-vous la notion de vie privée ?

Si les données personnelles n'ont pas été évoquées : Comment définiriez-vous les données personnelles ?

DONNEES PERSONNELLES ET ENCEINTES CONNECTEES

Trouvez-vous que votre enceinte vous connaît bien ? De mieux en mieux ?

Savez-vous que les données personnelles collectées par votre enceinte sont traitées sur les serveurs de Google / Amazon / Apple ?

Préféreriez-vous que les données personnelles collectées par votre enceinte restent chez vous ?

DONNEES PERSONNELLES ET ENTREPRISES

- Plus généralement, voyez-vous un ou des problèmes à ce que vos données personnelles, y compris celles que vous produisez chez vous, soient connues et traitées :
  - Par des entreprises privées à qui vous les donnez directement (ex : formulaires d'inscription, sondage téléphonique) ?
  - Par des entreprises privées à qui vous les donnez indirectement (ex : cartes de fidélité, revente de vos données de navigation pour le ciblage publicitaire) ?
- Chez quelles grandes entreprises du type Google, Microsoft, Facebook ou Apple avez-vous un compte ?
- Trouvez-vous que cette entreprise vous connaît bien ? (ex : recherches pertinentes, publicités ciblées…)
- Est-ce que cela vous gêne ?

DONNEES PERSONNELLES ET ÉTAT

- Voyez-vous un ou des problèmes à ce que vos données personnelles, y compris celles que vous produisez chez vous, soient connues et traitées par les services publics ?
- Connaissez-vous Edward Snowden ?

VOUS ET LA VIE PRIVEE

De manière plus générale, considérez-vous plus intime votre géolocalisation physique ou votre historique de navigation en ligne (téléphone/tablette/ordinateur/télévision) ?

Faites-vous une différence entre les personnes susceptibles d'avoir accès à des données personnelles vous concernant ? Ex : famille/ami, employeur, entreprises, FAI, banquier, services publics…

Connaissez-vous une anecdote vous concernant, vous ou un proche, où vous estimez que la vie privée de cette personne a été compromise ? (au travail, en famille, par rapport à l'assurance...)

QUESTIONNAIRE POUR LES NON-UTILISATEURS D'ENCEINTES CONNECTEES

Vous êtes libre de ne pas répondre à toute question qui vous gêne.

Sentez-vous libre de développer votre point de vue au-delà du seul cadre de la question, ou de me questionner sur le sens des questions. Il s'agit d'une conversation, mes questions sont secondaires par rapport à votre avis.

(NON-)USAGES DES ASSISTANTS PERSONNELS / DOMESTIQUES

- Avez-vous déjà interagi avec un assistant personnel de type Google Assistant, Siri ou Cortana ?
  - En utilisez-vous régulièrement ?
- Envisageriez-vous de posséder une enceinte connectée de type Google Home, Apple HomePod ou Amazon Alexa ?
- Envisageriez-vous d'utiliser une enceinte connectée ? L'avez-vous déjà fait ?
  - Si oui, dans quel cadre ? Quel a été votre sentiment par rapport à cette expérience ?
  - Si réticence, par quoi est-elle motivée ?
  - Si réticence, vous pousserait-elle jusqu'à ne pas vous rendre chez un ou une proche équipé-e de tels appareils, et notamment d'enceintes connectées ?
- Si vous deviez vous équiper d'une enceinte connectée, où la mettriez-vous dans votre domicile ? Pourquoi ?
- Faites-vous une différence entre les différents modèles et différentes marques d'enceintes connectées ?
- Disposez-vous d'autres objets dits connectés ? Et plus particulièrement domotiques ? (ex : montre de sport, ampoules Philips Hue, télévision, alarme de domicile…)
  - Sont-ils reliés à Internet ?
  - À un compte en ligne chez un prestataire ?
  - À un serveur local personnel ?

ÉQUIPEMENT NUMERIQUE DU FOYER (CREDOC)

État des lieux des équipements du foyer. Comparaison possible avec les rapports de référence du CREDOC (envisager aussi de reprendre leurs catégories socio-démographiques, pour faciliter les comparaisons).

- Disposez-vous, personnellement, d'un téléphone mobile ?
- D'un smartphone ?
- D'une tablette ?
- Pour quelle raison principale n'avez-vous pas de smartphone ? (Une seule réponse)
  - Vous ne connaissez pas ces appareils ou vous trouvez qu'ils sont trop compliqués à utiliser ...
  - Vous ne souhaitez pas vous en servir, pour des problèmes de confidentialité et de protection des données
  - Vous trouvez ça trop cher
  - Vous ne trouvez pas ça utile, vous n'en avez pas besoin
  - Autre raison
  - Ne sait pas
- Comment qualifieriez-vous votre propre compétence pour utiliser… ?

Très compétent Assez compétent Pas très compétent Pas du tout compétent Ne se prononce pas

Un ordinateur

Une tablette

Un smartphone

AUTRES DISPOSITIFS DOMOTIQUES

LINKY

- Connaissez-vous Linky ? En êtes-vous équipé ? Que pensez-vous de ce dispositif ?
- Préférez-vous qu'un agent ERDF (ou autre) se rende chez vous pour relever le compteur ?

SERRURES CONNECTEES

- Connaissez-vous les serrures connectées Amazon Key, August Access (non disponibles en France) ou de marque Somfy ?
- Que pensez-vous de ce dispositif ?
- Accepteriez-vous de l'utiliser ? À quelles conditions ?

VIDEOSURVEILLANCE DU DOMICILE

- Connaissez-vous les caméras à reconnaissance faciale (ex : marque Netatmo) reconnaissant les membres de la famille quand ils rentrent au domicile ?
- Que pensez-vous de ce dispositif ?

NAVIGATION SUR INTERNET

- À l'aide de quels dispositifs vous connectez-vous à Internet ?
- Quel navigateur utilisez-vous sur votre ordinateur ? Sur votre smartphone ? Sur votre tablette ?
- Quels sont les services que vous utilisez principalement sur Internet :
  - Moteur de recherche.
  - Courriel.
    - Autres communications : Skype, Apple Facetime, Discord...
  - Identification par un compte tiers (ex : via le compte Google).
  - Multimédia : musique (Spotify, Apple Store…), vidéo (YouTube, Netflix…).
  - Rencontres : Tinder, Grindr...
  - Autres.

VOTRE NOTION DE LA VIE PRIVEE

LA VIE PRIVEE EN GENERAL

Comment définiriez-vous la notion de vie privée ?

Si les données personnelles n’ont pas été évoquées : Comment définiriez-vous les données personnelles ?

DONNEES PERSONNELLES ET ENCEINTES CONNECTEES

Trouvez-vous que votre enceinte vous connaît bien ? De mieux en mieux ?

Savez-vous que les données personnelles collectées par votre enceinte sont traitées sur les serveurs de Google / Amazon / Apple ?

Préféreriez-vous que les données personnelles collectées par votre enceinte restent chez vous ?

DONNEES PERSONNELLES ET ENTREPRISES

- Plus généralement, voyez-vous un ou des problèmes à ce que vos données personnelles, y compris celles que vous produisez chez vous, soient connues et traitées :
  - Par des entreprises privées à qui vous les donnez directement (ex : formulaires d’inscription, sondage téléphonique) ?
  - Par des entreprises privées à qui vous les donnez indirectement (ex : cartes de fidélité, revente de vos données de navigation pour le ciblage publicitaire) ?
- Chez quelles grandes entreprises du type Google, Microsoft, Facebook ou Apple avez-vous un compte ?
- Trouvez-vous que cette entreprise vous connaît bien ? (ex : recherches pertinentes, publicités ciblées…)
- Est-ce que cela vous gêne ?

DONNEES PERSONNELLES ET ÉTAT

- Voyez-vous un ou des problèmes à ce que vos données personnelles, y compris celles que vous produisez chez vous, soient connues et traitées par les services publics ?
- Connaissez-vous Edward Snowden ?

VOUS ET LA VIE PRIVEE

- De manière plus générale, considérez-vous plus intime votre géolocalisation physique ou votre historique de navigation en ligne (téléphone/tablette/ordinateur/télévision) ?

- Faites-vous une différence entre les personnes susceptibles d'avoir accès à des données personnelles vous concernant ? Ex : famille/ami, employeur, entreprises, FAI, banquier, services publics…

- Connaissez-vous une anecdote vous concernant, vous ou un proche, où vous estimez que la vie privée de cette personne a été compromise ? (au travail, en famille, par rapport à l'assurance…)

  - Si utilisateur de Grindr : avez-vous entendu parler de la vente de données par Grindr à des entreprises tierces, dont la presse a parlé début 2018 ?

ÉCHELLE DE VALEURS

Ce qui relève de l'espace privé-intime ou de l'espace public-partageable selon vous, avec possibilité de faire une différence pour chaque question selon les acteurs (ex : OK pour mon médecin, mais non pour mon employeur).

- Prénom et nom

Privé / intime Public / partageable

- Numéro de téléphone.

Privé / intime Public / partageable

  - Par exemple, préférez-vous recevoir une publicité par texto, recevoir un appel de démarchage, ou plutôt une lettre ou un mail ?

- Carnet d'adresses (numéros etc. de vos proches)

Privé / intime Public / partageable

  - Utilisez-vous WhatsApp, Hangout, ou une application du style ? Savez-vous que ces données sont stockées et analysées par Google, Facebook etc. ?

- Ordinateur personnel

Privé / intime Public / partageable

- Adresse postale

Privé / intime Public / partageable

- Vos comptes sur les réseaux sociaux

Privé / intime Public / partageable

- Les sites Internet que vous visitez / historique de navigation

Privé / intime Public / partageable

- Votre géolocalisation

Privé / intime Public / partageable

- Votre historique de navigation

Privé / intime Public / partageable

- Affiliation politique ou syndicale

Privé / intime Public / partageable

- Orientation sexuelle

Privé / intime Public / partageable

- Métadonnées téléphoniques ou autres

Privé / intime Public / partageable

- Contenus des SMS, courriels

Privé / intime Public / partageable

- Listes des applications installées

Privé / intime Public / partageable

- Pseudonymes

Privé / intime Public / partageable

- Salaire

Privé / intime Public / partageable

- Vous pouvez répondre par oui, non, NSP, et n'hésitez pas à expliquer une situation ou votre position en détails si vous le jugez utile. « Avez-vous déjà…? (question CREDOC)
    - Refusé d'être géo localisé en ouvrant une page internet ou dans une application ?
    - Renoncé à installer une application, afin de protéger vos données personnelles (votre carnet d'adresses, vos photos, votre agenda...) ?
    - Éteint votre téléphone mobile pour éviter d'être tracé ?
    - Pris des dispositions pour ne pas laisser de traces sur internet, par exemple en supprimant des cookies ou en naviguant en mode privé ?
    - Renoncé à un achat parce que vous n'aviez pas suffisamment confiance au moment du paiement ?
    - Souscrit à un service de sécurisation de paiement en ligne, par exemple avec un procédé qui évite de communiquer votre numéro de carte habituelle ?
    - Renoncé à publier, ou supprimé, un message sur un réseau social pour protéger votre vie privée ?
    - Arrêté votre navigation sur internet à cause de l'insuffisante sécurité d'une page internet (avertissement du navigateur, absence du https ou de l'icône cadenas dans la barre d'adresse) ? »

Questions JFP :

- Craignez-vous que des propos que vous avez tenus par le passé sur Internet ou dans une publication vous nuise aujourd'hui ou dans le futur ?
- Faites-vous une différence entre les différentes marques (d'enceintes connectées, de smartphones…) du point de vue de la vie privée ?

SOI DANS L'ESPACE PUBLIC (= HORS DE CHEZ SOI)

Avez-vous une différence de ressenti quand vous êtes chez vous et dans l'espace public ? Si oui, comment la qualifieriez-vous ?

Au travail, qu'est-ce que cela vous fait si quelqu'un voit ce que vous faites sur votre téléphone ? Sur votre écran d'ordinateur ? Autre ?

Même question pour l'espace public (dans un parc, dans les transports…) ? Ex : lire par-dessus votre épaule.

Pensez-vous que nous soyons contrôlés, surveillés dans l'espace public ? Dans quelle mesure, à quel moment, par qui… ? (si une réponse unique type « la police », essayer de voir ce qui vient en suggérant d'autres acteurs, type bornes CB ou Navigo, Google Maps...)

Quelle est votre position par rapport à ces éventuelles formes de surveillance ? (réponse plutôt générale sur son bien-fondé)

Quel est votre ressenti par rapport à ces éventuelles formes de surveillance ? (si l'interviewé reste trop général)

Pensez-vous que votre téléphone notamment, mais aussi l'utilisation de cartes de crédit et autres cartes de transport, divulgue des informations à propos de vos déplacements, achats, etc. ?

Pensez-vous que ces informations sont révélatrices à l'égard de votre identité, de votre personnalité ?

Cela vous gêne-t-il ?

Que pensez-vous de ce que l'on appelle vidéoprotection ou vidéo-surveillance ?

Que pensez-vous des nouvelles techniques de vidéosurveillance embarquée, comme les lunettes connectées avec reconnaissance faciale déjà utilisée par certaines unités de police chinoises ?

DONNEES SOCIO-DEMOGRAPHIQUES (TYPE CREDOC)

- Sexe
  - Homme
  - Femme
  - Autre
- Âge
  - 18-24 ans
  - 25-39 ans
  - 40-59 ans

- 60-69 ans
- 70 ans et plus

• Nombre de personnes dans le logement :

- 1
- 2
- 3
- 4
- 5+

• Diplôme

- Aucun
- BEPC
- Bac
- Licence / Master / Doctorat

• Profession :

- Indépendant
- Cadre supérieur
- Profession intermédiaire
- Employé
- Ouvrier
- Au foyer
- Retraité
- Élève / étudiant.

• Niveau de vie :

• Lieu de résidence :

- 2 000- hab.

- 20 000- hab.
- 100 000- hab.
- 100 000+ hab.
- Paris et agglo parisienne

- Dernière question : accepteriez-vous qu'on se revoie dans quelques mois pour savoir comment votre perception des choses a évolué ?

Niveau de vie médian des différents groupes de niveau de vie

	En € par unité de consommation	En € par foyer
Bas revenus	805	1 200
Classe moyenne inférieure	1 300	1 800
Classe moyenne supérieure	1 803	2 800
Hauts revenus	2 887	4 800

Source : CREDOC, Enquête « Conditions de vie et Aspirations», juin 2017.

PRESENTATION DES ENQUETES PRINCIPAUX

E1 / 17-04-2018

E1 est un homme de 26 ans. Diplômé d'un master, il est attaché d'administration d'État à Paris et appartient à la classe moyenne supérieure. Très technophile, il n'en reste pas moins plutôt critique des dérives dans l'utilisation des données personnelles dans le secteur numérique, et peut être décrit comme un pragmatique. Sensibilité de gauche marquée. Il s'agit d'un ami à moi dont l'entretien de test du guide a été versé aux entretiens principaux.

E2 / 27-04-2018

E2 est une femme de 29 ans. Diplômée d'un master, elle est alors dans une phase d'alternance entre divers emplois de bureau à Paris et appartient à la classe moyenne inférieure. Assez distante vis-à-vis du numérique, elle n'en utilise pas moins quotidiennement smartphone et ordinateur. Elle est assez gênée pourtant dans son rapport à l'utilisation des données personnelles, et formalise sa pensée plutôt au cours de l'entretien. C'est une pragmatique. Sensibilité de gauche marquée. Il s'agit d'une amie à moi dont l'entretien de test du guide a été versé aux entretiens principaux.

E3 et E4 / 18-07-2018

E3 et E4 sont un homme de 32 ans et une femme de 31 ans interrogés en couple, parents d'une fille d'un an. Il est ingénieur informaticien, elle est titulaire d'une licence professionnelle et travaille dans les ressources humaines. Ils vivent et travaillent en proche banlieue parisienne, et ont de hauts revenus. Ils sont tous deux très technophiles et utilisateurs d'une Amazon Echo Dot et de domotique connectée. Sensibilité de centre-droit. E3 a été recruté sur le forum d'informatique du site hardware.fr

E5 / 06-08-2018

E5 est un homme de 34 ans vivant à Paris. Il est informaticien en SSII, titulaire d'un master, et travaille en proche banlieue parisienne. Il est le cas-type de technophile critique, étant même président d'un fournisseur d'accès à Internet associatif au moment de l'entretien, et évidemment opposé aux enceintes et à la domotique connectée. Sensibilité de gauche marquée. Il a été recruté lors des événements de la Quadrature du Net.

E6 et E7 / 08-09-2018

E6 et E7 sont un homme et une femme de 22 ans, en couple. Ils sont étudiants en sciences sociales à Lyon où ils vivent et travaillent à côté de leurs études, notamment comme babysitteuse pour E7. Ils ont de bas revenus. E6 est très technophile et possède une Google Home Mini, E7 se décrit comme plutôt technodistante mais utilise en fait couramment des outils et services numériques, dont l'enceinte connectée. Sensibilité de gauche ou de centre-gauche. Ils ont été recrutés sur renseignement d'une collègue.

E8 / 22-11-2018

E8 est un homme de 39 ans, en couple avec deux enfants. Il vit et travaille dans la région bordelaise comme ingénieur dans le domaine de l'alimentation, son foyer appartient à la classe moyenne supérieure. Il est très technophile et a largement domotisé sa maison. Il a d'ailleurs été rencontré en tant qu'administrateur du groupe Facebook « Les Alexiens », dédié à l'enceinte d'Amazon, dont il possède plusieurs exemplaires. L'entretien s'est déroulé en visioconférence. Sensibilité politique inconnue, vraisemblablement de centre-droit.

E9 / 18-12-2018

E9 est un homme de 50 ans, en couple puis séparé entre les deux moments d'entretien. Il vit d'abord en grande banlieue parisienne, puis a déménagée vers Montpellier. Il est chômeur de la maintenance informatique, et a repris une formation en université. Il ne m'a pas communiqué ses revenus, mais on peut supposer qu'il appartient à la classe moyenne inférieure. Il est assez technophile, mais virulent contre les GAFAM et la surveillance de masse, quoiqu'il soit confiant dans la démocratie et pas si inquiet de la collecte par des entreprises. Il a été recruté sur le parking d'une zone commerciale de Cergy-Pontoise après que je l'ai vu s'intéresser à l'îlot dédié aux enceintes connectées dans la petite FNAC locale. Il a refusé l'enregistrement pour les deux phases d'entretien, d'abord en face-à-face à l'oral, puis par téléphone. Sensibilité politique inconnue, vraisemblablement de gauche.

E10 / 19-12-2018

E10 est une femme d'environ 35 ans, en couple, vivant en région parisienne. Elle ne m'a pas communiqué d'autres informations sociodémographiques, sinon ses origines africaines. Elle est plutôt pragmatique, partagée entre l'idée que la domotique connectée est un gadget et en même temps bien pratique. C'est une pragmatique. Elle a été rencontrée à la FNAC de Châtelet à Paris autour du rayon des enceintes connectées.

E11 / 21-12-2018

E11 est une femme d'un peu moins de 40 ans. Elle vit et travaille en région lyonnaise Elle estime avoir « trop de trucs connectés en ce moment », mais est également dithyrambique à propos de Spotify et de ses algorithmes de recommandation. C'est donc une pragmatique, voire une enthousiaste, qui déclare vouloir « être au milieu » entre « naïveté » et « paranoïa ». Sensibilité politique centriste (sans « avis politique particulier »). Rencontrée à la FNAC de Lyon Part-Dieu où elle venait acheter une Google Home pour ses parents à l'occasion des fêtes de fin d'année. Ses parents vivent assez loin de Lyon, dans le Jura (je lui ai laissé mes coordonnées au cas où ils seraient intéressés par un entretien, elle ne m'a pas recontacté).

E12 et E13 / 22-12-2018

E12 et E13 sont deux hommes d'une quarantaine d'année. Je les ai rencontrés à Lyon autour du rayon des enceintes connectées du Boulanger de Cordeliers. Ils sont à Lyon pour le week-end. Peu gênés par les enjeux de vie privée du numérique commercial, ils sont très technophiles et semblent travailler dans l'informatique et/ou avoir une culture technique forte, évoquant même l'entreprise Snips dont la notoriété est restée cantonnée aux connaisseurs.

E14 et E15 / 21-02-2019

E14 et E15 sont deux hommes de 35 et 36 ans vivant en couple. Ils vivent et travaillent en proche banlieue parisienne, comme consultant informatique en SSII et comme analyste financier, avec de hauts revenus. Très technophiles, ils possèdent une enceinte HomePod et sont les plus équipés des enquêtés avec plusieurs dizaines de périphériques connectés.

E16 / 10-03-2019

E16 est un homme de 30 ans. Il vit dans le périurbain lyonnais. Paraplégique, il a conservé une certaine motricité dans les bras mais ne peut plus travailler après un accident. Il était opticien et titulaire d'un BTS. Ses revenus personnels ne sont pas élevés, mais il vit dans la maison de son père qui a de hauts revenus. Il possède une Google Home Mini offerte par son frère. Il était déjà technophile avant son accident, mais l'utilisation d'une enceinte connectée est dans son cas liée à son handicap moteur. E16 est un ami à moi. Sensibilité politique de centre-gauche.

E17 / 19-03-2019

E17 est un homme dans la fourchette d'âge 40-59 ans. Il vit et travaille dans une grande métropole française, dans une grande enseigne vendant entre autres choses des enceintes

connectées. Il est titulaire d'une maitrise, et travaillait auparavant dans le journalisme. Il est à la fois enthousiaste vis-à-vis des possibilités offertes par les nouvelles technologies, et en même temps très critique par rapport à la manière dont elles sont mises en œuvre aujourd'hui (lors de notre premier contact, il se refusait par exemple encore à posséder un *smartphone*). Je l'ai rencontré sur son lieu de travail. Sensibilité politique apparente de centre-gauche.

E18 et E19 / 03-07-2019

E18 et E19 sont un homme et une femme en couple de 62 ans. Ils vivent à Lyon, où ils travaillaient avant la retraite respectivement comme ingénieur électrique et médecin. Ils ont de hauts revenus. Ils sont plutôt réticents quant à l'utilisation qui est faite des technologies numériques, quoiqu'ils les utilisent tout de même. Ils possèdent des *smartphones* et E18 me fait même la démonstration spontanée de l'utilisation de Google Assistant. Ce sont des pragmatiques tendant vers une posture critique. Ils ne possèdent pas d'enceinte connectée, mais l'entretien s'est déroulé à leur domicile. Ils ont été recrutés dans un atelier de type Café Vie Privée à Lyon. Sensibilité politique de centre-gauche.

E20 / 11-07-2019

E20 est une femme de 30 ans. Elle vit et travaille en région lyonnaise dans le service financier d'une grande entreprise, elle appartient à la classe moyenne supérieure et a le titre d'ingénieure. Rencontrée au cours d'un atelier de type Café Vie Privée à Lyon, elle est plutôt critique et cherche justement à mettre en œuvre pratiquement ses convictions théoriques, après avoir été longtemps plutôt pragmatique.

E21 / 06-03-2019

E21 est une femme en couple de 52 ans. Elle vit et travaille à Lyon comme coach sportive. Elle est titulaire d'une licence. Elle est une enthousiaste déclarée, voire militante, et une utilisatrice se décrivant avancée d'une enceinte Echo d'Amazon. Elle dispose également de nombreux périphériques domotiques, en particulier des luminaires connectés, mais également de l'*everywear*. Elle a été recrutée comme parente d'un ami et rencontrée dans un premier temps dans une réunion politique de droite.

FICHE SYNTHETIQUE SUR LES LABELS EXISTANTS DANS LE CADRE DU TRAVAIL POUR LE GROUPE ISOC/IOT

Texte de la fiche soumise par Jean-François Perrat sur l'espace de travail collaboratif du groupe ISOC/IOT en février 2019.

Synthèse labels existants

- Personne référente pour ce document : Jean-François Perrat (ENS de Lyon, Franciliens.net).
- Tour d'horizon de diverses solutions existantes pour la labellisation des objets connectés, dans une optique de sécurité informatique et de protection de la vie privée des utilisateurs.

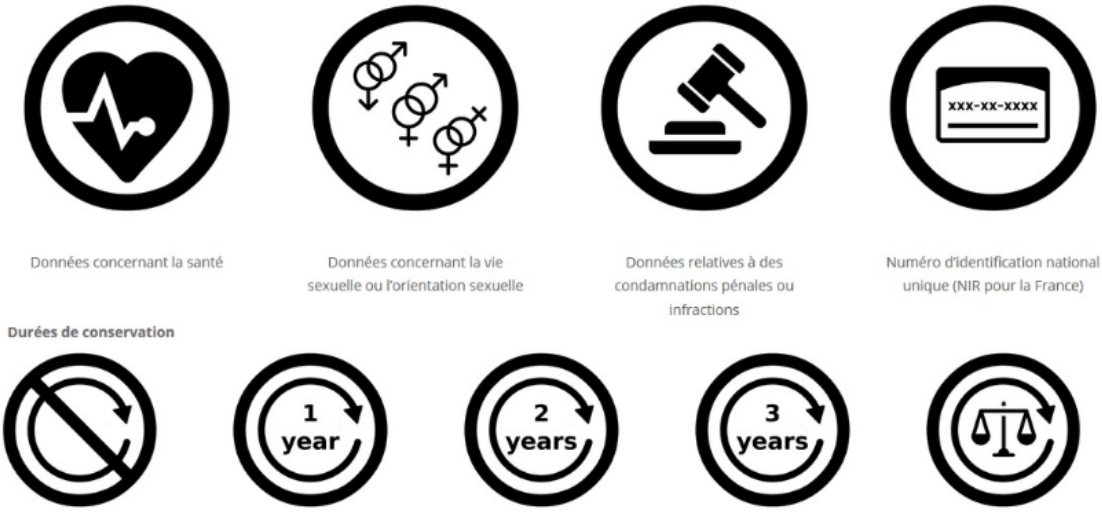
Table des matières

1. Association *Privacy Tech* (France)

1.1. Travaux intéressants pour le groupe de travail IoT

- Un projet de « certification tierce partie » très proche de l'idée du label. Il semble pour l'instant en relatif sommeil. Voir : https://www.privacytech.fr/certification-privacy-tech/.
- Un livre blanc pour lequel ils voudraient réunir tous types d'acteurs intéressés pour promouvoir une nouvelle gouvernance des données : https://www.privacytech.fr/livre-blanc/
- Une **gamme de logos traduisant graphiquement quelles données personnelles seront utilisées par un service** (identité, coordonnées bancaires…).
  - Ils sont plutôt bien faits et en licence CC-BY-ND. Ils s'inspirent justement des équivalents graphiques pour les licences Creative Commons.
  - C'est le projet qu'ils ont l'air de promouvoir le plus. Voir : https://www.privacytech.fr/privacy-icons/
  - Catégories retenues :
    - Nature des données collectées
    - Durées de conservation
    - Gestion des tiers (destinataires) & Politique de sécurité
    - Usages des données collectées
    - Flux transfrontaliers
    - Modification et viralité de la politique de confidentialité

- Plus gros défaut identifié : même si les logos sont plutôt clairs et bien faits, ils sont tout de même nombreux et pas forcément compréhensibles au premier coup d'œil pour une personne non-avertie.



1.2. Éléments divers sur Privacy Tech

- Découverts lors de l'intervention de Alessandro FIORENTINO (vice-président de l'association, au moins à l'époque) le 16 mars 2018 dans une conférence sur le RGPD donnée par le journal *L'Opinion*.
- Caractérisation de l'association :
  - Semble plutôt une association professionnelle dans une logique B2B, cf les types de membres possibles.
  - Semble très liée à l'AFCDP.
  - D'après leur charte, ils cherchent à promouvoir « l'excellence française dans le domaine de la protection des données et de la vie privée » grâce à des « biens communs » tant juridiques que techniques et à « la montée en puissance d'une communauté d'innovateurs et de formateurs pour accompagner les entreprises et les administrations qui souhaitent assigner à leurs services un haut niveau de protection des données personnelles ».
- Activité de l'association :
  - Au niveau des publications, seulement un texte de mémoire, *Le réveil de la vie privée* par Alessandro FIORENTINO. Voir : http://www.privacytech.fr/fiorentino-le-reveil-de-la-vie-privee-afcdp2016.pdf.
  - Leur Twitter créé en décembre 2016 n'a que 230 abonnés et 209 tweets en tout. Leurs derniers tweets et RT datent néanmoins de début janvier 2019 *(à date de février 2019)*.

- Ils participent jusqu'à récemment à des événements de natures assez diverses :
  - Avec le soutien apparent de Paula Fortezza, ils auraient déjà présenté leurs travaux en mars 2018 à l'assemblée nationale, puis en juin à la Commission européenne (tweet).
  - Présentations en salons professionnels.
  - Ou encore un hackathon axé *legal tech* réunissant juristes et start-up.
- Site web de l'association : https://www.privacytech.fr
  - Assez étonnant, avec une vidéo de présentation qui met en scène leur logo en 3D sur un fond musical de film d'action.
  - Site plutôt bien fait dans l'ensemble, par ailleurs, dégageant une impression de sérieux.

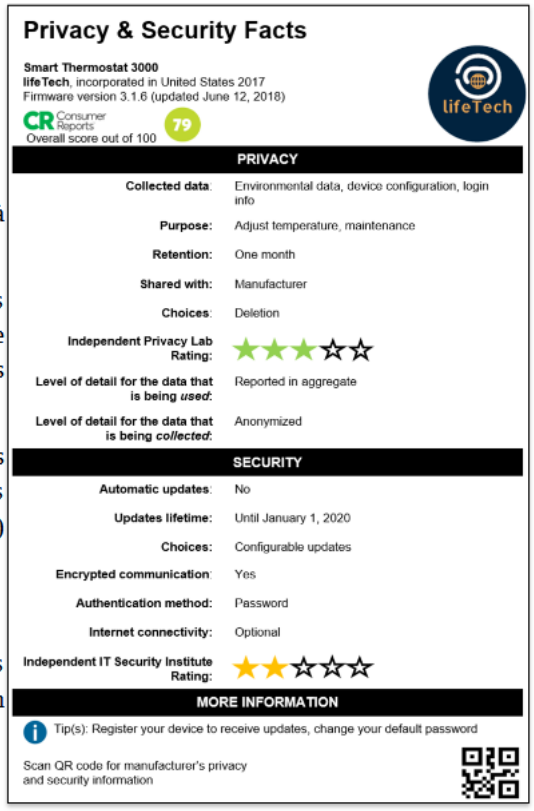
    Semble évidemment conforme au RGPD, utilise Matomo comme outil de statistiques.

2. Shorenstein Center (université d'Harvard)

Le Shorenstein Center on Media, Politics and Public Policy est un groupe de recherche visant à mettre en lien universitaires, industriels, et associations de consommateurs dans le but de promouvoir de bonnes pratiques dans la philosophie des Privacy Enhancing Technologies (PETs) / *privacy by design*.

Leur travail est assez concret, ils proposent notamment diverses formes de labellisation inspirantes.

2.1. Privacy and Security Nutrition Label for Smart Devices



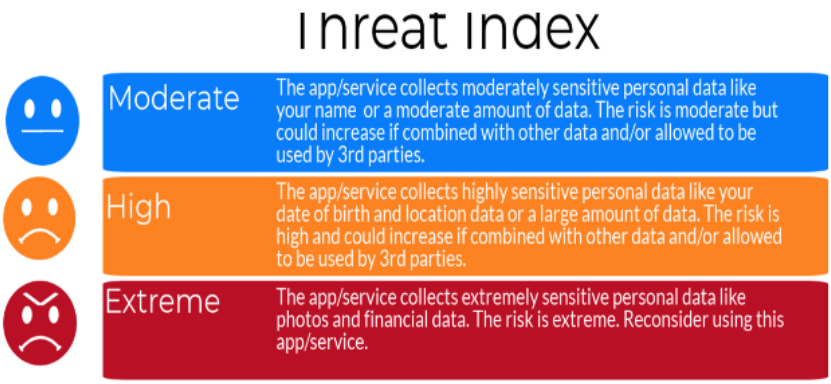
- **La solution la plus séduisante :**
  - implication des industriels,
  - grande clarté, évoque des étiquettes déjà connues des utilisateurs,
  - modularité : il est possible de ne pas reprendre tous les champs proposés comme d'en intégrer de nouveaux selon les besoins identifiés en groupe de travail,
  - promeut indirectement des bonnes pratiques déjà repérées (ex : ne pas collecter plus de données que nécessaire) afin d'éviter de charger la liste.
- Points de fragilité éventuelle :
  - Fragilité identifiée par les auteurs : les personnes enquêtées lors de l'élaboration

du label étaient assez résignées quant aux problèmes de sécurité / vie privée. Le label leur servait finalement au moins autant à avoir des informations techniques sur l'objet qu'à évaluer les risques liées à l'utilisation de l'objet.

- Sans standardisation de la liste des champs « données collectées » ou « finalités », il reste possible de botter en touche sur ces items (par exemple, en mettant « informations générales », sans préciser s'il s'agit seulement du nom et du prénom, mais aussi du numéro de téléphone, de l'adresse, etc.).
  - Le label ne peut donc être repris tel quel, un travail de standardisation doit le prolonger.
- L'étiquette est potentiellement complexe à lire pour une personne non-avertie.
  - Solution : faire apparaître plus clairement un score synthétique global (qu'on retrouve dans le score sur 5 étoiles au champ « Independant Privacy Lab Rating »), par exemple en haut d'étiquette et avec une police plus remarquable.
- Même si les concepteurs de produits peuvent / devraient fournir eux-mêmes les informations, une vérification par une autorité indépendante pourrait être nécessaire pour assurer la validité du label.
  - Ou alors, il faut que le label soit véritablement contractuel pour qu'un éventuel plaignant puisse s'en saisir en cas de non-conformité.

- Référence scientifique : EMAMI-NAEINI Pardis, Henry DIXON, Yuvraj AGARWAL et Lorrie Faith CRANOR, « Exploring How Privacy and Security Factor into IoT Device Purchase Behavior », dans *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*, Glasgow, Scotland Uk, ACM Press, 2019, p. 1-12 (en ligne : http://dl.acm.org/citation.cfm?doid=3290605.3300764, consulté le 7 juin 2019).
  - On y apprend notamment que leur label a été testé sur un panel de 24 consommateurs possédant au moins un objet connecté. Ces consommateurs ont participé à l'établissement des points à mettre en avant, au graphisme, etc.
  - Ils ont également interrogé 200 personnes via un sondage sur la plateforme Amazon Mechanical Turk.

2.2. Threat Index: helping users assess personal data risk



- Solution plus « agressive » : mise en garde des utilisateurs contre des risques potentiels.
  - Semble plutôt être un label à établir / attribuer à un service plutôt qu'un référentiel co-construit avec les fournisseurs du service.
    - En somme, une manière d'attribuer des mauvais points avant tout.
    - Pas d'implication du secteur.
  - Il n'existe pas de catégorie « vertueuse » sur le traitement des données personnelles, le risque est, au mieux, « modéré ».
    - Cette philosophie a du sens : fournir une donnée expose toujours au risque qu'elle soit divulguée ou dévoyée.
      - Mais ce n'est pas incitatif pour les entreprises.
- Seul mérite : une grande simplicité / lisibilité.
- De manière générale, une solution comme le Nutriscore dans l'alimentaire me semble plus approprié et plus incitatif.

COMMUNIQUE DE PRESSE ET 22 RECOMMANDATIONS FINALS DU GROUPE ISOC/IOT

Paris, le 5 mars 2020 – Le nombre d'objets connectés pourrait osciller entre 30 milliards (Gartner) et 80 milliards (iDate) cette année. Pourtant, tous ne respectent pas les règles de protection de la sécurité et de la vie privée de leurs utilisateurs. Internet Society et Internet Society France ont constitué il y a un an le premier groupe de travail multi-acteurs français et dévoilent aujourd'hui 22 recommandations pour renforcer la confiance des utilisateurs.

Que ce soit des télévisions, des balances, des montres ou des téléviseurs, les objets connectés ont envahi le quotidien de nombreux Français : 38% en possèdent au moins un en 2019, contre 27% en 2017 et 17% en 2016[1]. La présence en masse d'objets reliés à Internet multiplie les cyber-risques. A juste titre, les Français s'en inquiètent : les trois quarts (76%) d'entre eux conviennent que les objets connectés présentent un risque pour le respect de la vie privée ou la protection des données personnelles [2].

Fabricants, éditeurs, société civile, pour la première fois réunis

De ce constat est né en janvier 2019, à l'initiative de l'Internet Society et de l'Internet Society France, un groupe de travail composé d'experts issus de la société civile, de la communauté technique et académique, des acteurs publics, d'entreprises et d'organisations professionnelles. L'objectif : renforcer la sécurité et la protection des données personnelles des objets connectés.

« La mission d'Internet Society est de mettre en relation des partenaires dans un cadre multipartite pour initier la discussion. Une approche qui renforce l'acceptabilité des normes par l'ensemble des acteurs. La création de ce groupe de travail sur la sécurité des objets connectés était naturelle. »
Constance Bommelaer de Leusse, vice-présidente des relations institutionnelles de l'Internet Society et co-présidente du groupe de travail

Les membres du groupe de travail sur les objets connectés : Afnic, ARCEP, Agence du Numérique, ANSSI, Conseil national du numérique, CINOV-IT, Internet Society, Internet Society France, MEDEF, Nokia, Systematic Paris-Région, UNAF, ainsi que des experts et universitaires invités.

Le groupe a choisi de s'intéresser à la situation en France, en s'inspirant des bonnes pratiques observées autant en Europe que dans le reste du monde et en prenant appui sur le travail d'initiatives similaires mises en place par l'Internet Society au Sénégal et au Canada.

22 recommandations pour une plus grande fiabilité des objets connectés

L'Internet Society présente 22 recommandations (en détail page suivante) qui sont le fruit des travaux du groupe, réparties dans 4 domaines : sécurité, transparence, protection de la vie privée et des données personnelles et enfin résilience, interopérabilité et durabilité.

« Nous encourageons vivement les industriels de l'Internet des Objets à prendre en compte ces recommandations pour rendre les objets connectés plus sûrs, mais aussi pour leur garantir une longue durée de vie. »
Lucien Castex, secrétaire général de l'Internet Society France et co-président du groupe de travail

Les 22 recommandations

Sécurité

INTÉGRER UNE NOTICE DE SÉCURITÉ UTILISATEUR (changer fréquemment le mot de passe, limiter l'accès de l'objet connecté aux autres appareils électroniques, procéder aux mises à jour de sécurité…)

CRÉER UN LABEL DE SÉCURITÉ DÉLIVRÉ OU AUTO-ÉVALUÉ pour toute mise sur le marché d'un objet connecté

UTILISER EXCLUSIVEMENT DES MOTS DE PASSE ROBUSTES à l'exclusion des mots de passe par défaut

GARANTIR LA SÉCURITÉ DES COMMUNICATIONS par le renforcement du chiffrement

ASSURER L'INTÉGRITÉ PHYSIQUE DE L'UTILISATEUR

Transparence

RENFORCER LA MAÎTRISE DES UTILISATEURS DES OBJETS CONNECTÉS en créant un droit à l'explicabilité et à la protection de l'attention

INCITER LES FABRICANTS À S'INTERROGER sur l'adéquation des fonctionnalités installées et la finalité de l'objet connecté

INFORMER CLAIREMENT L'UTILISATEUR afin de lui permettre un choix libre et éclairé

PERMETTRE À L'UTILISATEUR DE DÉSACTIVER à tout moment l'appareil

METTRE À DISPOSITION, AU PROFIT DE CHAQUE UTILISATEUR, UNE INFORMATION CLAIRE et facilement accessible par la standardisation d'une série de pictogrammes

Protection de la vie privée et des données personnelles

METTRE EN PLACE UNE ÉVALUATION D'IMPACT SYSTÉMATIQUE SUR LA VIE PRIVÉE au stade de la conception de tout objet connecté

LANCER UNE MISSION D'ÉTUDE ET D'ÉVALUATION DE LA COMPATIBILITÉ DES GRANDS PRINCIPES DU RGPD avec l'Internet des objets

ÉTABLIR UN RÉGIME SPÉCIFIQUE DE RESPONSABILITÉ CIVILE pour les objets connectés

ASSURER EN TOUTE TRANSPARENCE L'INFORMATION ET LA PROTECTION DES DONNÉES à caractère personnel des utilisateurs

PORTER UNE ATTENTION TOUTE PARTICULIÈRE À LA PROTECTION DES DROITS DES MINEURS. Pour toute vente d'objet connecté destiné aux enfants, intégrer une notice de sécurité adaptée (explications en des termes simples, dessins…)

AVOIR UNE APPROCHE INTERNATIONALE DE LA PROTECTION de la vie privée et des données à caractère personnel

METTRE EN OEUVRE UNE POLITIQUE DE DIVULGATION DES VULNÉRABILITÉS qui garantisse la protection du lanceur d'alerte.

Résilience, interopérabilité et durabilité

MINIMISER L'IMPACT ENVIRONNEMENTAL des objets connectés

PROPOSER DES MISES À JOUR qui tiennent compte de la durée de vie des objets connectés.

INTÉGRER LA GESTION ET LA SUPERVISION DES VULNÉRABILITÉS dès la conception.

GARANTIR UNE SÉCURITÉ DE BOUT EN BOUT ET UNE FIABILITÉ de l'objet connecté avec l'assurance d'une interopérabilité effective.

PRÉVOIR ET INFORMER L'UTILISATEUR QUANT AUX POSSIBILITÉS DE RECYCLAGE de l'objet dans le respect d'un principe de gratuité ou de reprise par le fabricant.

BIBLIOGRAPHIE

OUVRAGES ET CHAPITRES D'OUVRAGES

ABLER R., « The telephone and the evolution of the American metropolitan system », dans IDS Pool, *The social impact of the telephone*, Cambridge (États-Unis), MIT Press, 1977, p. 318-341.

ACAS Renaud, Eric BARQUISSAU, Yves-Marie BOULVERT, Éric DOSQUET, Frédéric DOSQUET, Jérémy PIROTTE et Olivier EZRATTY, *Objets connectés : La nouvelle révolution numérique*, Saint-Herblain (France), ENI, 2015.

ACQUISTI Alessandro et Jens GROSSKLAGS, « Privacy attitudes and privacy behavior - Losses, Gains, and Hyperbolic Discounting », dans J. Camp et R. Lewis, *The Economics of Information Security*, Alphen aan den Rijn (Pays-Bas), Kluwer Academic, 2004.

AÏM Olivier, *Les théories de la surveillance - Du panoptique aux Surveillance Studies*, Paris (France), Armand Colin, coll. « Collection U », 2020.

AÏM Olivier, « Introduction », dans *Les théories de la surveillance - Du panoptique aux Surveillance Studies*, Paris (France), Armand Colin, coll. « Collection U », 2020, p. 7-14.

BAKIS Henry, *I.B.M: une multinationale régionale*, Grenoble (France), Presses universitaires de Grenoble, 1977.

BEAUDE Boris, « De quoi Wikipédia est-elle le lieu ? », dans Lionel Barbe, Louise Merzeau et Valérie Schafer (éd.), *Wikipédia, objet scientifique non identifié*, Nanterre, Presses universitaires de Paris Nanterre, coll. « Sciences humaines et sociales », 2015, p. 41-54.

BEAUDE Boris, *Les fins d'Internet*, Limoges (France), FYP (Limoges), coll. « Stimulo », 2014. ISSN 2265-7754.

BEAUDE Boris, *Internet: changer l'espace, changer la société - Les logiques contemporaines de synchorisation*, Limoges (France), Fyp éditions, coll. « Société de la connaissance », 2012.

BESSE Jean-Marc, *Habiter: un monde à mon image*, Paris (France), Flammarion, 2013.

BIERI Martin et Félicien VALLET, *À votre écoute - Exploration des enjeux éthiques, techniques et juridiques des assistants vocaux*, Paris (France), CNIL, 2020.

BORTZMEYER Stéphane, *Cyberstructure - L'Internet, un espace politique*, Caen (France), C&F éditions, coll. « Société numérique », 2018.

BOULLIER Dominique, « La portabilité des réseaux d'appartenance. Pour une théorie de l'habitèle », dans Émilie Bajolet, Jean-Marc Rennes et Marie-Flore Mattéi (éd.), *Quatre ans de recherche urbaine 2001-2004. Volume I : Action concertée incitative Ville. Ministère de la Recherche*, Tours (France), Presses universitaires François-Rabelais, coll. « Perspectives Villes et Territoires », 2013, p. 34-67.

BOULLIER Dominique, *L'urbanité numérique. Essai sur la troisième ville en 2100*, Paris (France), L'Harmattan, 1999.

BROWN Barry, *Studying the internet experience*, Bristol (Royaume-Uni), HP Laboratories, coll. « Publishing Systems and Solutions Laboratory », 2001.

CASILLI Antonio A., *En attendant les robots : enquête sur le travail du clic*, Edition augmentée de l'essai « Le travail à inégales distances »., Paris (France), Points, coll. « Points Essais 925 », 2021.

CASTELLS Manuel, *The rise of the network society*, 1999e éd., Oxford (Royaume-Uni), Blackwell, coll. « Information Age Series », 1996.

CAUQUELIN Anne, *Le site et le paysage*, 3e éd., Paris (France), Presses universitaires de France, coll. « Quadrige », 2012.

CHATTELIER Régis, Geooffrey DELCROIX, Estelle HARY, Camille GIRARD-CHANUDET, Pauline FAGET, Marie LEROUX et Stéphanie CHAPELLE, *La forme des choix*, Paris (France), CNIL, coll. « Cahiers Innovation et Prospective », 2019. ISSN : 2263-888.

DAMASIO Alain, *Les furtifs*, Clamart (France), La Volte, 2019.

DENIS Nathanael, Sophie CHABRIDON et Maryline LAURENT, « Bringing Privacy, Security and Performance to the Internet of Things Through Usage Control and Blockchains », dans Michael Friedewald, Stephan Krenn, Ina Schiering et Stefan Schiffner (éd.), *Privacy and Identity Management. Between Data Protection and Security*, [événement en ligne], Springer International Publishing, coll. « IFIP Advances in Information and Communication Technology », 2022, vol. 644, p. 57-72.

DESCOLA Philippe, *Par-delà nature et culture*, Paris (France), NRF : Gallimard, coll. « Bibliothèque des sciences humaines », 2005.

DOBBS Richard, Corinne SAWERS, Fraser THOMPSON, James MANYIKA, Jonathan WOETZEL, Peter CHILD, Sorcha MCKENNA et Angela SPATHAROU, *Overcoming obesity : An initial economic analysis*, McKinsey Global Institute, 2014.

DODGE Martin et Rob KITCHIN, *Mapping cyberspace*, Londres (Royaume-Uni), New-York (États-Unis), Routledge, 2001.

DODGE Martin et Rob KITCHIN, *Atlas of Cyberspace*, 1re éd., Harlow (Royaume-Uni), Addison-Wesley, 2001.

DRULHE Louise, *Atlas critique d'Internet - Spatialisation d'un objet complexe en vue d'en comprendre les enjeux socio-politiques*, Paris (France), 2015.

DUBY Georges, « Préface », dans Georges Duby et Philippe Ariès (éd.), *Histoire de la vie privée - Tome 1 - De l'Empire romain à l'an mil*, Paris (France), Seuil, coll. « L'univers historique », 1985.

DUPUY Gabriel, *La fracture numérique*, Paris (France), Ellipses, 2007.

DUPUY Gabriel, *Internet : géographie d'un réseau*, Paris (France), Ellipses, coll. « Carrefours », 2002, 1 vol.

DUPUY Gabriel, *L'informatisation des villes*, Paris (France), Presses universitaires de France, 1992.

FALIGOT Roger, « Du projet Safari au contrôle biométrique : Big Brother est parmi nous », dans *Histoire secrète de la Ve République*, Paris (France), La Découverte, coll. « Poche / Essais », 2007, p. 278-288. Cairn.info.

FEENBERG Andrew, « Building a Global Network: The WBSI Experience », dans Linda M. Harasim, *Global Networks : Computers and International Communication*, Cambridge (États-Unis), MIT Press, 1993, p. 185-197.

FRIEDMAN Thomas L, *The world is flat: a brief history of the twenty-first century*, New York (États-Unis), Farrar, Straus and Giroux, 2005.

GARCIA-MORCHON Oscar, Sandeep KUMAR et Mohit SETHI, *Internet of Things (IoT) Security: State of the Art and Challenges*, Internet Engineering Task Force, 2019.

GIBSON William, *Neuromancer*, New York (États-Unis), Ace Books, 1994.

GOTLIEB Calvin C., « Privacy: A Concept Whose Time Has Come And Gone », dans David Lyon et Elia Zuriek (éd.), *Computers, Surveillance, and Privacy*, sans lieu, 1996.

GREENFIELD Adam, *Every[ware]: la révolution de l'ubimedia*, Cyril Fiévet (trad.), Limoges (France), FYP Éditions, coll. « Innovation », 2007.

HARTZOG Woodrow, *Privacy's Blueprint: The Battle to Control the Design of New Technologies*, Cambridge (États-Unis), Harvard University Press, 2018. Google-Books-ID: cy1QDwAAQBAJ.

HARVEY David, *The Condition of Postmodernity - An Enquiry into the Origins of Cultural Changes*, Cambridge (États-Unis) et Oxford (Royaume-Uni), Blackwell, 1990.

HERCBERG Serge, *Propositions pour un nouvel élan de la politique nutritionnelle française de santé publique dans le cadre de la Stratégie Nationale de Santé - 1ère partie : Mesures concernant la Préventions nutritionnelle*, Paris (France), Ministère des Affaires Sociales et de la Santé, 2013.

HES R. et John BORKING, *Privacy-Enhancing Technologies: The Path to Anonymity*, La Haye (Pays-Bas), Registratiekamer, coll. « Achtergrondstudies en Verkenningen (Background Studies and Investigations) », 2000. ISBN 90 74087 12 4.

HESS A., « Reconsidering the Rhizome: A Textual Analysis of Web Search Engines as Gatekeepers of the Internet », dans Amanda Spink et Michael Zimmer (éd.), *Web Search: Multidisciplinary Perspectives*, Berlin & Heidelberg (Allemagne), Springer, coll. « Information Science and Knowledge Management », 2008, p. 35-50.

IACUB Marcela, *Par le trou de la serrure: histoire de la pudeur publique (XIXe-XXIe siècle)*, Paris (France), Fayard, coll. « Histoire de la pensée », 2008.

ISAACS E. et J. TANG, « Studying video-based collaboration in context: from small workgroups to large organisations », dans K. Finn, A. Sellen et S. Willbur, *Video Mediated Communication*, Mahwah (Etats-Unis), Lawrence Erlbaum Associates, 1997.

JABRAEIL JAMALI Mohammad Ali, Bahareh BAHRAMI, Arash HEIDARI, Parisa ALLAHVERDIZADEH et Farhad NOROUZI, « Some Cases of Smart Use of the IoT », dans Mohammad Ali Jabraeil Jamali, Bahareh Bahrami, Arash Heidari, Parisa Allahverdizadeh et Farhad Norouzi (éd.), *Towards the Internet of Things: Architectures, Security, and Applications*, Cham, Springer International Publishing, coll. « EAI/Springer Innovations in Communication and Computing », 2019, p. 85-129.

KAUFMANN Jean-Claude, *La chaleur du foyer. Analyse du repli domestique*, Paris (France), Klincksieck, 1988.

KITCHIN Rob et Martin DODGE, *Code/space: software and everyday life*, Cambridge (États-Unis), MIT Press, 2014.

LAURENT Marylène et Nesrine KAANICHE, *Personnalisation de services : quelles technologies pour la préservation de la vie privée ?*, Paris (France), Chaire Valeurs et Politiques des Information Personnelles, 2019.

LEGLEYE Stéphane et Annaïck ROLLAND, *Une personne sur six n'utilise pas Internet, plus d'un usager sur trois manque de compétences numériques de base*, Montrouge (France), INSEE, coll. « Insee Première », 2019.

LUSSAULT Michel, *L'avènement du Monde: essai sur l'habitation humaine de la Terre*, Paris (France), Seuil, coll. « La Couleur des idées », 2013.

LUSSAULT Michel, *L'homme spatial: la construction sociale de l'espace humain*, Paris (France), Seuil, coll. « La Couleur des idées », 2007.

LUSSAULT Michel, « Chapitre 1 - Action(s) ! », dans *Logiques de l'espace, esprit des lieux - Géographies à Cerisy*, sans lieu, 2000, p. 3-36.

LYON David, « Surveillance capitalism, surveillance culture and data politics », dans Didier Bigo, Engin Isin et Evelyn Ruppert, *Data Politics - Worlds, Subjects, Rights*, Londres (Royaume-Uni), Routledge, 2019, p. 64-77.

MASUTTI Christophe, *Affaires privées: aux sources du capitalisme de surveillance*, Caen (France), C&F éditions, coll. « Société numérique », 2020.

MCLUHAN Marshall et Quentin FIORE, *The Medium is the Massage*, Jerome Agel (éd.), Londres (Royaume-Uni), The Penguin Press, 1967.

MERLE Roger et André VITU, *Traité de droit criminel. Tome 1 - Problèmes généraux de la science criminelle, droit pénal général*, 7e éd., Paris (France), Cujas, 1997.

MICHEAU Frédéric, *Les Français et les objets connectés - Sondage OpinionWay pour ISOC France*, Paris (France), Internet Society France / OpnionWay, 2018.

MITCHELL William J., *City of bits: space, place, and the infobahn*, 6e éd., Cambridge (États-Unis), MIT Press, 1999.

MOLES Abraham André et Elisabeth ROHMER-MOLES, *Psychosociologie de l'espace*, Paris (France), l'Harmattan, coll. « Villes et entreprises », 1998.

MUSSO Pierre, « IV. La numérisation du système des télécoms », dans *Les télécommunications*, Paris (France), La Découverte, coll. « Repères », 2008, p. 60-73.

MUSSO Pierre, *Critique des réseaux*, Paris (France), Presses universitaires de France, coll. « La politique éclatée », 2003.

NEGROPONTE Nicholas, *Being Digital*, New York (ÉUA), Knopf, 1995. Google-Books-ID: wL66CILxDLkC.

NIEL Xavier et Dominique ROUX, « Des évolutions permanentes », dans *Les 100 mots de l'Internet*, Paris (France), Presses Universitaires de France, coll. « Que sais-je ? », 2012, vol. 3, p. 113-120. ISSN : 0768-0066.

NISSENBAUM Helen Fay, *Privacy in context: technology, policy, and the integrity of social life*, Stanford (États-Unis), Stanford Law Books, 2010.

NOVA Nicolas, *Smartphones: une enquête anthropologique*, Genève (Suisse), MétisPresses, 2020.

PROST Antoine, « Frontières et espaces du privé », dans Georges Duby et Philippe Ariès (éd.), *Histoire de la vie privée - Tome 5 - De la première guerre mondiale à nos jours*, Paris (France), Seuil, coll. « L'univers historique », 1987.

REY Bénédicte, *La vie privée à l'ère du numérique*, Cachan (France), Lavoisier - Hermes Science, coll. « Traitement de l'information », 2012.

RIGAUX François, « L'individu, sujet ou objet de la société de l'information », dans Pierre Tabatoni, *La protection de la vie privée dans la société d'information*, sans lieu, Presses Universitaires de France, coll. « Cahiers des sciences morales et politiques », 2002, p. 122-137.

SCHWANEN Tim, « Information Technology and Mobility », dans *International Encyclopedia of Geography*, sans lieu, John Wiley & Sons, Ltd, 2022, p. 1-4.

SCHWANEN Tim, « Information Technology and Mobility », dans *International Encyclopedia of Geography*, sans lieu, American Cancer Society, 2017.

SENNETT Richard, *Les tyrannies de l'intimité*, Antoine Berman et Rebecca Folkman (trad.), Paris (France), Seuil, 1995.

SIMONNOT Brigitte et Gabriel GALLEZOT (éd.), *L'entonnoir: Google sous la loupe des sciences de l'information et de la communication*, Caen (France), C&F éditions, 2009.

SLOTERDIJK Peter, *Écumes - Sphérologie plurielle*, Olivier Mannoni (trad.), Paris (France), Hachette Littératures, coll. « Pluriel », 2006.

SLOTERDIJK Peter, *Bulles*, Olivier Mannoni (trad.), Paris (France), Pauvert, coll. « Sphères, microsphérologie 1 », 2002.

SNOWDEN Edward J., *Permanent record*, Londres (Royaume-Uni), Macmillan, 2019.

SOLOVE Daniel J., *Understanding privacy*, Cambridge (États-Unis), Harvard University Press, 2008.

SOLOVE Daniel J., *« I've Got Nothing to Hide » and Other Misunderstandings of Privacy*, Rochester (États-Unis), Social Science Research Network, 2007.

SZAKOLCZAI Janos Mark, « 'What have you caught?': Nannycams and hidden cameras as normalised surveillance of the intimate », dans *The Technologisation of the Social*, 1re éd., Londres (Royaume-Uni), Routledge, 2021.

THORNGREN Bertil, *Telecommunications and Regional Development in Sweden*, National Swedish Board for Technical Development, 1977.

TISSERON Serge, *L'Intimité surexposée*, Paris (France), Ramsay, 2001.

TUBARO Paola et Antonio A. CASILLI, « Human Listeners and Virtual Assistants: Privacy and Labor Arbitrage in the Production of Smart Technologies », dans Mark E. Graham et Fabian Ferrari, *Digital Work in the Planetary Market*, Cambridge (États-Unis) et Londres (Royaume-Uni), MIT Press, 2022, p. 175-190.

TURNER Fred, *Aux sources de l'utopie numérique: de la contre-culture à la cyberculture, Stewart Brand, un homme d'influence*, Laurent Vannini (trad.), 2e éd., Caen (France), C&F éditions, 2021.

TUROW Joseph, *The Voice Catchers: How Marketers Listen In to Exploit Your Feelings, Your Privacy, and Your Wallet*, New Haven, Yale University Press, 2021.

VIDAL Philippe et Henry BAKIS, « De la négation du territoire au géocyberespace : vers une approche intégrée de la relation entre espace et TIC », dans Claire Brossaud et Bernard Reber (éd.), *Humanités numériques 1 : nouvelles technologies cognitives et épistémologie*, Paris (France), Hermes - Lavoisier, coll. « Cognition et traitement de l'information », 2007, vol. 1, p. 101-116.

VIRILIO Paul, *La bombe informatique*, Paris (France), Galilée, 1998.

VIRILIO Paul, *L'espace critique*, Paris (France), C. Bourgois, 1984.

WESTIN Alan F., *Privacy and Freedom*, New York (ÉUA), Atheneum, 1967.

ZUBOFF Shoshana, *The Age of Surveillance Capitalism*, New York (États-Unis), PublicAffairs, 2019.

RAPPORTS ET LITTERATURE INSTITUTIONNELLE

La régulation de l'Arcep au service des territoires connectés - Tome 2, Paris (France), Arcep, 2021.

Baromètre du numérique 2021 - Enquête sur la diffusion des technologies de l'information et de la communication dans la société française, Paris (France), CRÉDOC, 2021.

Assistants vocaux et enceintes connectées: l'impact de la voix sur l'offre et les usages culturels et médias, Paris (France), Hadopi & CSA, 2019.

Smart Home Market - Analysis by Size, Growth, Trend and Forecast to 2024, Pune (Inde), Markets and Markets, 2019.

Word of the Year 2018 - Shortlist, Londres (Royaume-Uni), Oxford Languages, 2018.

Paths to Our Digital Future, Internet Society, coll. « Global Internet Report », 2017.

THÈSES ET MÉMOIRES

ALATKAR Sayati Anil, *Detecting Smart Home Activity Through Network Traffic Signatures*, mémoire de master, New York (ÉUA), State University of New York, 2020.

APPELBAUM Jacob R., *Communication in a world of pervasive surveillance: Sources and methods: Counter-strategies against pervasive surveillance architecture*, thèse de doctorat en mathématiques et informatique, Eindhoven (Pays-Bas), Technische Universiteit Eindhoven, 2022.

BRETOU Sandrine, *De la mythologie basque à une construction identitaire militante : éthique de l'engagement au prisme de l'imaginaire collectif*, thèse de doctorat en sociologie, Montpellier (France), Montpellier 3, 2009.

CORNEC Jérémy, *Imaginaires de la dystopie et du posthumain dans les séries d'anticipation science-fictionnelles contemporaines (2009-2019)*, thèse de doctorat en langue et littérature anglophone, Brest (France), Université de Bretagne occidentale - Brest, 2021.

COURMONT Antoine, *Politiques des données urbaines : ce que l'open data fait au gouvernement urbain*, thèse de doctorat en science politique, Paris (France), Institut d'études politiques de Paris, 2016.

DANIELI Aude, *La « mise en société » du compteur communicant : innovations, usages et controverses dans les mondes sociaux du compteur d'électricité Linky en France*, thèse de doctorat en sociologie, Marne-la-Vallée (France), Paris Est, 2018.

DUFEAL Marina, *Les sites web, marqueurs et vecteurs de dynamiques spatiales et économiques dans l'espace méditerranéen français*, thèse de doctorat en géographie, Avignon (France), université d'Avignon et des Pays du Vaucluse, 2004.

GRAVELAIS Isabelle, *La protection juridictionnelle de l'inviolabilité du domicile*, thèse de doctorat en droit public, Dijon (France), université de Bourgogne, 2013.

NOVA Nicolas, *Figures mobiles: une anthropologie du smartphone*, thèse de doctorat en sociologie, Genève (Suisse), université de Genève, 2018.

OLLIVON Franck, *La prison chevillée au corps. Pour une approche géographique du placement sous surveillance électronique.*, Thèse de doctorat en géographie, Lyon (France), Université Lumière - Lyon II, 2018.

PERRAT Jean-François, *Peler l'oignon. Étude géographique des services cachés du réseau Tor*, mémoire de master 2 en géographie, Lyon (France), École normale supérieure de Lyon, 2016.

SARDIER Thibaut, *Du quartier topographique au quartier topologique : Comment smartphone et réseaux sociaux redéfinissent la notion de proximité.*, mémoire de master 2, Lyon (France), ENS de Lyon, 2014.

TREGUER Félix, *Pouvoir et résistance dans l'espace public : une contre-histoire d'Internet (XVe -XXIe siècle)*, thèse de doctorat en histoire, Paris (France), EHESS, 2017.

ARTICLES SCIENTIFIQUES

ACQUISTI Alessandro, Idris ADJERID, Rebecca BALEBAKO, Laura BRANDIMARTE, Lorrie Faith CRANOR, Saranga KOMANDURI, Pedro Giovanni LEON, Norman SADEH, Florian SCHAUB, Manya SLEEPER, Yang WANG et Shomir WILSON, « Nudges for Privacy and Security: Understanding and Assisting Users », *ACM Computing Surveys*, vol. 50, nº 3, 8 août 2017, p. 44:1-44:41 (en ligne : https://doi.org/10.1145/3054926 ; consulté le 7 juin 2022).

ALBER Alex, « Voir le son : réflexions sur le traitement des entretiens enregistrés dans le logiciel Sonal », *Socio-logos . Revue de l'association française de sociologie*, nº 5, 13 avril 2010 (DOI : 10.4000/socio-logos.2482).

ALOMBERT Anne et Émilien CRISTIA, « L'espace urbain à l'épreuve de la révolution numérique : nouvelles technologies urbaines et intelligence collective », *ISTE Open Science*, vol. 6, nº 3, coll. « Technologie et innovation », 7 mai 2021 (DOI : 10.21494/ISTE.OP.2021.0657 consulté le 15 mars 2023).

Anonyme, « Questions à Michel Foucault sur la géographie », *Hérodote - Revue de géographie et de géopolitique*, nº 1, 1976, p. 71-85 (en ligne : https://gallica.bnf.fr/ark:/12148/bpt6k5621035h/f80.vertical).

AUSTIN Lisa et David LIE, « Data Trusts and the Governance of Smart Environments: Lessons from the Failure of Sidewalk Labs' Urban Data Trust », *Surveillance & Society*, vol. 19, nº 2, 25 juin 2021, p. 255-261 (en ligne : https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/14409).

BAKIS Henry, « Le « géocyberespace » revisité », *Netcom*, vol. 21, nº 3-4, 16 décembre 2007, p. 285-296 (en ligne : http://netcom.revues.org/2220 ; consulté le 15 novembre 2016).

BAKIS Henry, « Télécommunication et organisation spatiale des entreprises », *Revue Géographique de l'Est*, vol. 25, nº 1, 1985, p. 33-46 (en ligne : https://www.persee.fr/doc/rgest_0035-3213_1985_num_25_1_1566 ; consulté le 28 septembre 2018).

BAKIS Henry, « Éléments pour une géographie des télécommunications », *Annales de géographie*, vol. 89, nº 496, 1980, p. 657-688 (en ligne : https://www.persee.fr/doc/geo_0003-4010_1980_num_89_496_19992 ; consulté le 2 octobre 2018).

BAKIS Henry et Emmanuel EVENO, « Les géographes et la société de l'information. Des effets pervers d'un champ réputé a-géographique », *Géocarrefour*, vol. 75, nº 1, 2000, p. 7-9 (en ligne : http://www.persee.fr/doc/geoca_1627-4873_2000_num_75_1_2448).

BARR Nathaniel, Gordon PENNYCOOK, Jennifer A. STOLZ et Jonathan A. FUGELSANG, « The brain in your pocket: Evidence that Smartphones are used to supplant thinking », *Computers in Human Behavior*, vol. 48, 1er juillet 2015, p. 473-480 (en ligne : https://www.sciencedirect.com/science/article/pii/S0747563215001272 ; consulté le 6 décembre 2022).

BEAUDE Boris et Nicolas NOVA, « Topographies réticulaires », *Réseaux*, nº 195, 24 mars 2016, p. 53-83 (en ligne : http://www.cairn.info/resume.php?ID_ARTICLE=RES_195_0053 ; consulté le 22 septembre 2016).

BENHAMOU Bernard, « L'internet des objets », *Esprit*, nº 3, 2009, p. 137-150 (en ligne : https://www.cairn.info/revue-esprit-2009-3-page-137.htm).

BERNARDIN Stève et Gilles JEANNOT, « La ville intelligente sans les villes ? », *Réseaux*, vol. 218, nº 6, La Découverte, 28 novembre 2019, p. 9-37 (en ligne : https://www.cairn.info/revue-reseaux-2019-6-page-9.htm ; consulté le 3 mai 2022).

BOULLIER Dominique, « Habitele: mobile technologies reshaping urban life », *URBE*, vol. 6, nº 1, avril 2014, p. 13-16 (en ligne : https://www.boullier.bzh/articles/boullier-dominique-habitele-mobile-technologies-reshaping-urban-life/ ; consulté le 29 septembre 2020).

BOULLIER Dominique, « Objets communicants, avez-vous donc une âme ? Enjeux anthropologiques », *Les Cahiers du numérique*, vol. 3, nº 4, Lavoisier, 2002, p. 45-60 (en ligne : https://www.cairn.info/revue-les-cahiers-du-numerique-2002-4-page-45.htm ; consulté le 22 juin 2022).

BURKELL Jacquelyn, Alexandre FORTIER, Lorraine (Lola) Yeung Cheryl WONG et Jennifer Lynn SIMPSON, « Facebook: public space, or private space? », *Information, Communication & Society*, vol. 17, nº 8, 14 septembre 2014, p. 974-985 (en ligne : http://www.tandfonline.com/doi/citedby/10.1080/1369118X.2013.870591 ; consulté le 23 janvier 2018).

BUTLEN Max et Joaquim DOLZ, « La logique des compétences : regards critiques », *Le francais aujourd'hui*, vol. 191, nº 4, Armand Colin, 23 décembre 2015, p. 3-14 (en ligne : https://www.cairn.info/revue-le-francais-aujourd-hui-2015-4-page-3.htm).

CARDULLO Paolo et Rob KITCHIN, « Being a 'citizen' in the smart city: up and down the scaffold of smart citizen participation in Dublin, Ireland », *GeoJournal*, vol. 84, nº 1, 1er février 2019, p. 1-13 (en ligne : https://doi.org/10.1007/s10708-018-9845-8).

DEPECKER Loïc, « Que diriez-vous d' « ordinateur » ? », *Bibnum. Textes fondateurs de la science*, FMSH - Fondation Maison des sciences de l'homme, 1er juin 2015 (en ligne : http://journals.openedition.org/bibnum/534 ; consulté le 27 mars 2021).

DESBOIS Henri, « La carte et le territoire à l'ère numérique », *Socio. La nouvelle revue des sciences sociales*, nº 4, 25 avril 2015, p. 39-60 (en ligne : https://socio.revues.org/1262 ; consulté le 20 février 2017).

DUBOIS Pierre, Paulo ALBUQUERQUE, Olivier ALLAIS, Céline BONNET, Patrice BERTAIL, Pierre COMBRIS, Saadi LAHLOU, Natalie RIGAL, Bernard RUFFIEUX et Pierre CHANDON, « Effects of front-of-pack labels on the nutritional quality of supermarket food purchases: evidence from a large-scale randomized controlled trial », *Journal of the Academy of Marketing Science*, vol. 49, nº 1, 1er janvier 2021, p. 119-138 (en ligne : https://doi.org/10.1007/s11747-020-00723-5 ; consulté le 17 juillet 2022).

DUFEAL Marina, « L'inscription spatiale de l'insularité: la Corse séparée de la France – sur le Web, Abstract », *Annales de géographie*, vol. 5, nº 645, 2005, p. 496-509 (en ligne : https://www.cairn.info/revue-annales-de-geographie-2005-5-page-496.html ; consulté le 29 juin 2018).

DUFEAL Marina et Loïc GRASLAND, « La planification des réseaux à l'épreuve de la matérialité des TIC et de l'hétérogénéité des territoires », *Flux*, nº 54, 2003, p. 49-69 (en ligne : http://www.cairn.info/article.php?ID_ARTICLE=FLUX_054_0049 ; consulté le 2 octobre 2018).

DUPUY Gabriel, « Fracture et dépendance : l'enfer des réseaux? », *Flux*, vol. 83, nº 1, Métropolis, 1er mars 2011, p. 6-23 (en ligne : https://www.cairn.info/revue-flux1-2011-1-page-6.htm).

EVENO Emmanuel, « La Ville intelligente : objet au cœur de nombreuses controverses », *Quaderni. Communication, technologies, pouvoir*, nº 96, Les éditions de la Maison des sciences de l'Homme, 15 mai 2018, p. 29-41 (en ligne : http://journals.openedition.org/quaderni/1174 ; consulté le 12 février 2021).

EVENO Emmanuel, « Le paradigme territorial de la Société de l'Information », *NETCOM : Réseaux, communication et territoires / Networks and communication studies*, vol. 18, nº 1, Persée - Portail des revues scientifiques en SHS, 2004, p. 89-132 (en ligne : https://www.persee.fr/doc/netco_0987-6014_2004_num_18_1_1601 ; consulté le 16 février 2023).

EVENO Emmanuel, « Pour une géographie de la Société de l'Information », *NETCOM : Réseaux, communication et territoires / Networks and communication studies*, vol. 11, nº 2, Persée - Portail des revues scientifiques en SHS, 1997, p. 431-457 (en ligne : https://www.persee.fr/doc/netco_0987-6014_1997_num_11_2_1369).

FRAWLEY Ryan, « Logging and Analysis of Internet of Things (IoT) Device Network Traffic and Power Consumption », *Master's Theses*, 1er juin 2018 (DOI : 10.15368/theses.2018.60 consulté le 19 novembre 2020).

GEORGE Éric, « Les usages militants d'Internet », *Communication. Information médias théories pratiques*, vol. 22, nº 2, Editions Nota bene, 15 octobre 2003, p. 99-124 (en ligne : https://journals.openedition.org/communication/4655 ; consulté le 1er septembre 2021).

HALPERIN Jean-Louis, « Protection de la vie privée et privacy : deux traditions juridiques différentes ? », *Nouveaux cahiers du conseil constitutionnel*, nº 48, juin 2015, p. 59-68 (en ligne : https://www.conseil-constitutionnel.fr/node/1308/pdf).

HOANG Nguyen Phong, Arian Akhavan NIAKI, Jakub DALEK, Jeffrey KNOCKEL, Pellaeon LIN, Bill MARCZAK, Masashi CRETE-NISHIHATA, Phillipa GILL et Michalis POLYCHRONAKIS, « How Great is the Great Firewall? Measuring China's DNS Censorship », *arXiv*, 3 juin 2021 (en ligne : http://arxiv.org/abs/2106.02167 ; consulté le 13 juillet 2021). ArXiv: 2106.02167.

HUANG Danny Yuxing, Noah APTHORPE, Frank LI, Gunes ACAR et Nick FEAMSTER, « IoT Inspector: Crowdsourcing Labeled Network Traffic from Smart Home Devices at Scale », *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 4, nº 2, 15 juin 2020, p. 46:1-46:21 (en ligne : https://doi.org/10.1145/3397333 ; consulté le 18 novembre 2020).

HUSTINX Peter, « Privacy by design: delivering the promises », *Identity in the Information Society*, vol. 3, nº 2, 1er août 2010, p. 253-255 (en ligne : https://doi.org/10.1007/s12394-010-0061-z ; consulté le 18 juillet 2022).

JEANNOT Gilles et Victor MAGHIN, « La ville intelligente, de l'administration à la gouvernance », *Réseaux*, vol. 218, nº 6, La Découverte, 28 novembre 2019, p. 105-142 (en ligne : https://www.cairn.info/revue-reseaux-2019-6-page-105.htm ; consulté le 7 octobre 2021).

JOLIVEAU Thierry, « Le géoweb, un nouveau défi pour les bases de données géographiques », *L'Espace géographique*, vol. 40, nº 2, 12 juillet 2011, p. 154-163 (en ligne : http://www.cairn.info/resume.php?ID_ARTICLE=EG_402_0154 ; consulté le 29 septembre 2016).

DE JONG Martin, Simon JOSS, Daan SCHRAVEN, Changjie ZHAN et Margot WEIJNEN, « Sustainable–smart–resilient–low carbon–eco–knowledge cities; making sense of a multitude of concepts promoting sustainable urbanization », *Journal of Cleaner Production*, vol. 109, coll. « Special Issue: Toward a Regenerative Sustainability Paradigm for the Built Environment: from vision to reality », 16 décembre 2015, p. 25-38 (en ligne : https://www.sciencedirect.com/science/article/pii/S0959652615001080 ; consulté le 3 mai 2022).

KLAUSER Francisco, « Splintering Spheres of Security: Peter Sloterdijk and the Contemporary Fortress City », *Environment and Planning D: Society and Space*, vol. 28, nº 2, avril 2010, p. 326-340 (en ligne : http://journals.sagepub.com/doi/10.1068/d14608).

KLAUSER Francisco, Till PAASCHE et Ola SÖDERSTRÖM, « Michel Foucault and the Smart City: Power Dynamics Inherent in Contemporary Governing through Code », *Environment and Planning D: Society and Space*, vol. 32, nº 5, SAGE Publications Ltd STM, 1er octobre 2014, p. 869-885 (en ligne : https://doi.org/10.1068/d13041p).

KOKOLAKIS Spyros, « Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon », *Computers & Security*, vol. 64, 1er janvier 2017, p. 122-134 (en ligne : https://www.sciencedirect.com/science/article/pii/S0167404815001017).

LABARBE Jules, « De l'oral à l'écrit dans la Grèce archaïque », *Bulletins de l'Académie Royale de Belgique*, vol. 67, nº 1, Persée - Portail des revues scientifiques en SHS, 1981, p. 30-66 (en ligne : https://www.persee.fr/doc/barb_0001-4133_1981_num_67_1_55494 ; consulté le 6 décembre 2022).

LASSERRE Frédéric, « Internet : La fin de la géographie ? », *Cybergeo : European Journal of Geography*, 31 octobre 2000 (en ligne : https://cybergeo.revues.org/4467 ; consulté le 5 janvier 2017).

LEVY Michel Louis, « Le statisticien face aux tabous », *Sociétal*, nº 37, 2002, p. 35-38 (en ligne : http://archives.institut-entreprise.fr/sites/default/files/article_de_revue/docs/documents_internes/societal-37-9-levy-reperesettendances.pdf).

LIMONIER Kevin, « Vers un « Runet souverain » ? Perspectives et limites de la stratégie russe de contrôle de l'Internet », *EchoGéo*, nº 56, Pôle de recherche pour l'organisation et la diffusion de l'information géographique (CNRS UMR 8586), 25 mai 2021 (DOI : 10.4000/echogeo.21804 consulté le 17 juillet 2021).

MCDONALD Aleecia M et Lorrie Faith CRANOR, « The Cost of Reading Privacy Policies », *I/S : A Journal of Law and Policy for the Information Society*, vol. 4, nº 3, 2008, p. 543-568 (en ligne : https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf?sequence=1&isAllowed=y).

MEIRIEU Philippe, « La télécommande et l'infantile », *Médium*, vol. 2, nº 1, Association Médium, 2005, p. 44-59 (en ligne : https://www.cairn.info/revue-medium-2005-1-page-44.htm ; consulté le 6 décembre 2022).

MELL Laurent, « Une dialectique de la pudeur : les pratiques de mise en visibilité de soi sur Facebook », *tic&société*, vol. 10, nº 2-3, ARTIC, 30 avril 2017 (DOI : 10.4000/ticetsociete.2088).

MERICSKAY Boris, Matthieu NOUCHER et Stéphane ROCHE, « Usages des traces numériques en géographie : potentiels heuristiques et enjeux de recherche », *L'Information géographique*, vol. 82, nº 2, 9 juillet 2018, p. 39-61 (en ligne : http://www.cairn.info/revue-l-information-geographique-2018-2-page-39.htm ; consulté le 5 octobre 2018).

MOREL Michel et Tania BÄNZIGER, « Le rôle de l'intonation dans la communication vocale des émotions : test par la synthèse », *Cahiers de l'Institut de Linguistique de Louvain*, vol. 30, nº 1-3, Peeters, 2004, p. 207-232 (en ligne : https://hal.archives-ouvertes.fr/hal-00100347 ; consulté le 22 décembre 2022).

MUSSO Pierre, « Territoires numériques », *Médium*, nº 15, 2008, p. 25-38 (en ligne : http://www.cairn.info/revue-medium-2008-2-p-25.html ; consulté le 21 juin 2018).

NIMMER Melville B, « The Right of Publicity », *Law and Contemporary Problems*, 1953, p. 21 (en ligne : https://scholarship.law.duke.edu/cgi/viewcontent.cgi?referer=https://en.wikipedia.org/&httpsredir=1&article=2595&context=lcp).

NPOCHINTO MOUMENI I. et F. MOUREY, « Intérêt en EHPAD du robot émotionnel Pepper dans les troubles neurocomportementaux de la maladie d'Alzheimer », *NPG Neurologie - Psychiatrie - Gériatrie*, vol. 21, nº 121, 1er février 2021, p. 11-18 (en ligne : https://www.sciencedirect.com/science/article/pii/S1627483020301598).

OBAR Jonathan A. et Anne OELDORF-HIRSCH, « The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services », *Information, Communication & Society*, vol. 23, nº 1, Routledge, 2 janvier 2020, p. 128-147 (en ligne : https://doi.org/10.1080/1369118X.2018.1486870 ; consulté le 9 juin 2022).

OFFNER Jean-Marc, « La smart city pour voir et concevoir autrement la ville contemporaine », *Quaderni. Communication, technologies, pouvoir*, nº 96, Les éditions de la Maison des sciences de l'Homme, 15 mai 2018, p. 17-27 (en ligne : https://journals.openedition.org/quaderni/1172#tocto1n3 ; consulté le 14 février 2022).

OIRY Ewan et Lise VERLAET, « Éditorial - Une maison intelligente pour quoi faire ? Les enjeux des technologies de l'information et de la communication au service de l'habiter », *Communication & management*, vol. 17, nº 1, ESKA, 2020, p. 3-4 (en ligne : https://www.cairn.info/revue-communication-et-management-2020-1-page-3.htm ; consulté le 18 avril 2022).

PEEL Kyle et Eliot TRETTER, « Waterfront Toronto: Privacy or Piracy? », *Global Urban Research at the University of Calgary Working Paper*, 12 juin 2019 (DOI : 10.31235/osf.io/xgz2s).

PERRAT Jean-François, « Un "deep/dark web" ? Les métaphores de la profondeur et de l'ombre sur le réseau Tor », *Netcom. Réseaux, communication et territoires*, vol. 32, nº 1-2, 2018 (en ligne : https://journals.openedition.org/netcom/3134).

PREECE Jenny, Diane MALONEY-KRICHMAR et Chadia ABRAS, « History of online communities », *Encyclopedia of community*, vol. 3, nº 1023-1027, 2003, p. 86.

PROSSER William, « Privacy », *California Law Review*, nº 48, 1960, p. 383-389.

REGAN Priscilla M., Gerald FITZGERALD et Peter BALINT, « Generational views of information privacy? », *Innovation: The European Journal of Social Science Research*, vol. 26, nº 1-2, mars 2013, p. 81-99 (en ligne : http://www.tandfonline.com/doi/abs/10.1080/13511610.2013.747650 ; consulté le 7 juillet 2021).

RIEDER Bernhard, Òscar COROMINA et Ariadna MATAMOROS-FERNÁNDEZ, « Mapping YouTube: A quantitative exploration of a platformed media system », *First Monday*, vol. 25, nº 8, 3 août 2020 (DOI : http://dx.doi.org/10.5210/fm.v25i8.10667 consulté le 24 mai 2021).

RIOS Ruben, Jose A. ONIEVA, Rodrigo ROMAN et Javier LOPEZ, « Personal IoT Privacy Control at the Edge », *IEEE Security & Privacy*, vol. 20, janvier 2022, p. 23-32 (en ligne : https://www.computer.org/csdl/magazine/sp/2022/01/09516686/1watX9oWPe0 ; consulté le 23 mars 2022).

SENEVIRATNE Suranga, Yining HU, Tham NGUYEN, Guohao LAN, Sara KHALIFA, Kanchana THILAKARATHNA, Mahbub HASSAN et Aruna SENEVIRATNE, « A Survey of Wearable Devices and Challenges », *IEEE Communications Surveys Tutorials*, vol. 19, nº 4, 2017, p. 2573-2620.

SEYMOUR Tom, Dean FRANTSVOG et Satheesh KUMAR, « History Of Search Engines », *International Journal of Management & Information Systems*, vol. 15, nº 4, 12 septembre 2011, p. 47-58 (en ligne : https://www.clutejournals.com).

SHEEHAN Kim Bartel, « Toward a Typology of Internet Users and Online Privacy Concerns », *The Information Society*, vol. 18, nº 1, 2002, p. 21-32 (en ligne : https://www.academia.edu/312464/Toward_a_Typology_of_Internet_Users_and_Online_Privacy_Concerns ; consulté le 2 juillet 2021).

SHI Weisong, Jie CAO, Quan ZHANG, Youhuizi LI et Lanyu XU, « Edge Computing: Vision and Challenges », *IEEE Internet of Things Journal*, vol. 3, nº 5, octobre 2016, p. 637-646.

SMYRNAIOS Nikos, « L'effet GAFAM : stratégies et logiques de l'oligopole de l'internet », *Communication & Langages*, vol. 2, nº 188, NecPlus, 2016, p. 61-83 (en ligne : https://www.cairn.info/journal-communication-et-langages1-2016-2-page-61.htm).

SOLOVE Daniel J., « A Taxonomy of Privacy », *University of Pennsylvania Law Review*, vol. 154, nº 3, janvier 2006, p. 477-560 (en ligne : https://papers.ssrn.com/abstract=667622 ; consulté le 21 juin 2017).

STASZAK Jean-François, « L'espace domestique : pour une géographie de l'intérieur », *Annales de géographie*, vol. 110, nº 620, 2001, p. 339 (en ligne : https://archive-ouverte.unige.ch/unige:76456 ; consulté le 29 décembre 2022).

STOCK Mathis, « L'hypothèse de l'habiter poly-topique : pratiquer les lieux géographiques dans les sociétés à individus mobiles. », *EspacesTemps.net*, Association Espaces Temps.net, 1er février 2006 (en ligne : http://www.espacestemps.net/document1853.html).

TISSERON Serge, « Intimité et extimité », *Communications*, vol. 1, nº 88, Le Seuil, 2011, p. 83-91 (en ligne : https://www.cairn.info/revue-communications-2011-1-page-83.htm ; consulté le 18 juin 2021).

VELGHE Pieter, « «Lire la Chine». Internet des Objets, surveillance et gestion sociale en RPC. », *Perspectives chinoises*, vol. 2019, nº 2019-1, Centre d'Études Français sur la Chine contemporaine, 2019, p. 91-96.

VYTH Ellis L., Ingrid HM STEENHUIS, Annet JC ROODENBURG, Johannes BRUG et Jacob C. SEIDELL, « Front-of-pack nutrition label stimulates healthier product development: a quantitative analysis », *International Journal of Behavioral Nutrition and Physical Activity*, vol. 7, nº 1, 8 septembre 2010, p. 65 (en ligne : https://doi.org/10.1186/1479-5868-7-65 ; consulté le 17 juillet 2022).

WARREN Samuel et Louis BRANDEIS, « The Right to Privacy », *Harvard Law Review*, vol. 4, nº 5, 15 décembre 1890.

WEST Emily, « Amazon: Surveillance as a Service », *Surveillance & Society*, vol. 17, nº 1/2, 31 mars 2019, p. 27-33 (en ligne : https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/13008 ; consulté le 26 juillet 2021).

ZAZA Ornella, « La mesure de l'humain », *Les Cahiers de la recherche architecturale urbaine et paysagère*, nº 3, Ministère de la culture, 26 décembre 2018 (DOI : 10.4000/craup.1153).

ACTES DE COLLOQUE ET COMMUNICATIONS SCIENTIFIQUES

AL BARAKEH Z, S. ALKORK, A. S. KARAR, S. SAID et T. BEYROUTHY, « Pepper Humanoid Robot as a Service Robot: a Customer Approach », Paris (France), 2019, p. 1-4.

BENOUAKTA Sofia, Santasri KOLEY, Florin Doru HUTU et Yvan DUROC, « Conception d'une antenne hélice pour fil textile RFID UHF extensible », dans *Actes JNM 2019*, Caen (France), 2019, p. 865-868.

BERND Julia, Ruba ABU-SALMA, Junghyun CHOY et Alisa FRIK, « Balancing Power Dynamics in Smart Homes: Nannies' Perspectives on How Cameras Reflect and Affect Relationships », sans lieu, 2022, p. 687-706 (en ligne : https://www.usenix.org/conference/soups2022/presentation/bernd ; consulté le 10 août 2022).

BOULLIER Dominique, « Rendre le numérique habitable : l'habitèle », dans Yann Calbérac, Olivier Lazzarotti, Jacques Lévy et Michel Lussault (éd.), *Les colloques de Cerisy*, Paris (France), Hermann, 2019, p. 151-174 (en ligne : https://drive.google.com/file/d/1TCcu8tzQwgzc3Afh_jdN7RY8QBL-Yy6a/view ; consulté le 29 septembre 2020).

BOUNAZEF Djida et Nathalie CRUTZEN, « Les citoyens et stratégies communales à l'ère de la smart city : Echanges et interactions entre sourds ? », Bruxelles (Belgique), 2019 (en ligne : https://orbi.uliege.be/handle/2268/237154).

CARRASCAL Juan Pablo, Christopher RIEDERER, Vijay ERRAMILLI, Mauro CHERUBINI et Rodrigo DE OLIVEIRA, « Your browsing behavior for a Big Mac : economics of personal information online », dans *Proceedings of the 22nd international conference on World Wide Web*, New York (ÉUA), Association for Computing Machinery, coll. « WWW '13 », 2013, p. 189-200 (en ligne : https://doi.org/10.1145/2488388.2488406 ; consulté le 2 juin 2022).

CHENG Peng, Ibrahim Ethem BAGCI, Jeff YAN et Utz ROEDIG, « Smart Speaker privacy control - acoustic tagging for Personal Voice Assistants », San Francisco (États-Unis), IEEE, 2019 (en ligne : https://cora.ucc.ie/handle/10468/8396 ; consulté le 17 novembre 2021). Accepted: 2019-08-27T11:31:24Z.

DESFONTAINES Damien et Balázs PEJO, « SoK: Differential Privacies », dans *Proceedings on Privacy Enhancing Technologies*, sans lieu, 2020, vol. 2, p. 288-313 (en ligne : http://arxiv.org/abs/1906.01337 ; consulté le 26 juillet 2022). ArXiv:1906.01337 [cs].

DINGLEDINE Roger, Nick MATHEWSON et Paul SYVERSON, « Tor: The Second-Generation Onion Router », dans *Proceedings of the 13th USENIX Security Symposium*, San Diego (États-Unis), The USENIX Association, 2004, p. 303-320 (en ligne : https://www.usenix.org/legacy/events/sec04/tech/dingledine.html).

FENG Yuanyuan, Yaxing YAO et Norman SADEH, « A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things », dans *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, New York (ÉUA), Association for Computing Machinery, coll. « CHI '21 », 2021, p. 1-16 (en ligne : https://doi.org/10.1145/3411764.3445148 ; consulté le 27 juillet 2022).

GÜRSES Seda, Carmela TRONCOSO et Claudia DIAZ, « Engineering Privacy by Design Reloaded », Amsterdam (Pays-Bas), 2015, p. 21 (en ligne : http://witdom.eu/content/engineering-privacy-design-reloaded ; consulté le 1er février 2018).

JONES Brian D., « The Georgia Tech Aware Home - Supporting Research, Partnerships, Students, and Beyond », Atlanta (États-Unis), 28 mai 2019 (en ligne : https://awarehome.gatech.edu/sites/default/files/documents/AwareHome_slides.pdf ; consulté le 24 avril 2022).

KRÖGER Jacob Leon, Philip RASCHKE et Towhidur Rahman BHUIYAN, « Privacy implications of accelerometer data: a review of possible inferences », dans *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy - ICCSP '19*, Kuala Lumpur (Malaisie), ACM Press, 2019, p. 81-87 (en ligne : http://dl.acm.org/citation.cfm?doid=3309074.3309076 ; consulté le 22 mai 2021).

PRESSE

AFP, « La famille Zuckerberg a un nouveau "majordome virtuel", Jarvis », *RTBF*, 20 décembre 2016 (en ligne : https://www.rtbf.be/article/la-famille-zuckerberg-a-un-nouveau-majordome-virtuel-jarvis-9485677 ; consulté le 28 décembre 2022).

AGEZ Florian, « Test Amazon Echo Input : le galet qui greffe Alexa à votre installation sonore », *Les Numériques*, 16 avril 2019 (en ligne : https://www.lesnumeriques.com/assistant-domotique/amazon-echo-input-p50627/test.html ; consulté le 19 mars 2022).

AGEZ Florian et Valentine DE BRYE, « Test Amazon Echo Show 10 : le smart display qui nous fait tourner la tête », *Les Numériques*, 8 mai 2021 (en ligne :

https://www.lesnumeriques.com/assistant-domotique/amazon-echo-show-10-p60107/test.html ; consulté le 3 septembre 2021).

AMADEO Ron, « Google Home can now tell users apart just by their voice », *Ars Technica*, 20 avril 2017 (en ligne : https://arstechnica.com/gadgets/2017/04/google-home-gets-support-for-multiple-users/ ; consulté le 22 août 2022).

Anonyme, « Domotique : le protocole Matter a sa version finale », *Next INpact*, rubrique « #LeBrief », 4 octobre 2022 (en ligne : https://www.nextinpact.com/lebrief/70089/domotique-protocole-matter-a-sa-version-finale ; consulté le 4 octobre 2022).

Anonyme, « Amazon veut racheter iRobot, pour 1,7 milliard de dollars », *Next INpact*, rubrique « #LeBrief », 8 août 2022 (en ligne : https://www.nextinpact.com/lebrief/69771/amazon-veut-racheter-irobot-pour-17-milliard-dollars ; consulté le 28 août 2022).

Anonyme, « Sonos lance sa nouvelle barre de son Ray et son propre assistant vocal », *Next INpact*, rubrique « #LeBrief », 13 mai 2022 (en ligne : https://www.nextinpact.com/lebrief/69170/sonos-lance-sa-nouvelle-barre-son-ray-et-son-propre-assistant-vocal ; consulté le 16 mai 2022).

Anonyme, « Reflets s'invite par hasard dans les voitures de police ukrainiennes », *Reflets.info - Journal d'investigation en ligne et d'information-hacking*, 2 mars 2022 (en ligne : https://reflets.info/articles/reflets-s-invite-par-hasard-dans-les-voitures-de-police-ukrainiennes ; consulté le 2 mars 2022).

Anonyme, « SFR lance la 5G à Nice, avec de nouveaux forfaits », *Next INpact*, rubrique « Le Brief », 20 novembre 2020 (en ligne : https://www.nextinpact.com/lebrief/44743/sfr-lance-5g-a-nice-avec-nouveaux-forfaits ; consulté le 1er septembre 2021).

Anonyme, « Des employés Ring ont tenté d'accéder aux vidéos des caméras », *Next INpact*, rubrique « LeBrief », 9 janvier 2020 (en ligne : https://www.nextinpact.com/lebrief/41088/10844-des-employes-ring-ont-tente-d-acceder-aux-videos-des-cameras ; consulté le 27 juillet 2021).

Anonyme, « Sonos rachète Snips, qui développe un assistant numérique respectueux de la vie privée », *Next INpact*, rubrique « #LeBrief », sans date (en ligne : https://www.nextinpact.com/lebrief/40641/10397-sonos-rachete-snips--qui-developpe-un-assistant-numerique-respectueux-de-la-vie-privee# ; consulté le 3 janvier 2023).

ARCE Charlotte, « 5 tendances cocooning aussi cool que le hygge », *Le Huffington Post*, rubrique « LIFE », 11 février 2017 (en ligne : https://www.huffingtonpost.fr/2017/02/11/5-tendances-cocooning-aussi-cool-que-le-hygge_a_21659274/ ; consulté le 21 septembre 2021).

BECHADE Corentin, « C'est toujours le bazar dans la domotique et ça ne va pas s'améliorer de sitôt », *Numerama*, 16 août 2021 (en ligne : https://www.numerama.com/tech/732843-cest-toujours-le-bazar-dans-la-domotique-et-ca-ne-va-pas-sameliorer-de-sitot.html ; consulté le 17 août 2021).

BERRAUD Gilles, « Ces puces intelligentes qu'on porte sur nous », *Le Nouvelliste*, 31 janvier 2015, p. 4 (en ligne : https://www.theark.ch/media/document/0/conferencetechnoarkhabitronique_nf_31.01.2015.pdf).

BOUCHER Philippe, « "Safari" ou la chasse aux Français », *Le Monde*, rubrique « Justice », 21 mars 1974, p. 9.

BRIDGES Lauren, « Amazon's Ring is the largest civilian surveillance network the US has ever seen », *The Guardian*, rubrique « Opinion », 18 mai 2021 (en ligne : https://amp.theguardian.com/commentisfree/2021/may/18/amazon-ring-largest-civilian-surveillance-network-us ; consulté le 23 mai 2021).

BRIGNULL Harry, « Dark Patterns: inside the interfaces designed to trick you », *The Verge*, 29 août 2013 (en ligne : https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you ; consulté le 7 juin 2022).

CHAFFIN Zeliha, « Téléphonie : la 5G, vedette du Salon de Barcelone », *Le Monde*, 23 février 2019 (en ligne : https://www.lemonde.fr/economie/article/2019/02/23/telephonie-la-5g-vedette-du-salon-de-barcelone_5427273_3234.html).

CHEN Brian X. et Cade METZ, « Google's Duplex Uses A.I. to Mimic Humans (Sometimes) », *The New York Times*, rubrique « Technology », 22 mai 2019 (en ligne : https://www.nytimes.com/2019/05/22/technology/personaltech/ai-google-duplex.html ; consulté le 22 décembre 2022).

CIMPANU Catalin, « Alexa and Google Home devices leveraged to phish and eavesdrop on users, again », *ZDNet*, sans date (en ligne : https://www.zdnet.com/article/alexa-and-google-home-devices-leveraged-to-phish-and-eavesdrop-on-users-again/ ; consulté le 24 mai 2021).

CIOLFI Marie, « Test Amazon Echo Spot : quand Alexa tourne bien rond », *Les Numériques*, 16 septembre 2018 (en ligne : https://www.lesnumeriques.com/assistant-domotique/amazon-echo-spot-p41337/test.html ; consulté le 1er septembre 2021).

CIOLFI Marie et Valentine DE BRYE, « Amazon lance enfin en France son Echo Show », *Les Numériques*, 27 mars 2019 (en ligne : https://www.lesnumeriques.com/assistant-domotique/amazon-echo-show-2eme-generation-p51515/amazon-lance-enfin-en-france-son-echo-show-n85315.html ; consulté le 1er septembre 2021).

CODERE Jean-François, « Don d'ADN pour un burger », *La Presse*, rubrique « DOSSIER SPÉCIAL », 26 avril 2014 (en ligne : https://plus.lapresse.ca/screens/4c47-b330-5357ba5b-b386-2311ac1c6068|6HlR00chIHX~.html ; consulté le 2 juin 2022).

COROT Léna, « Ces start-up qui lèvent des millions pour leur service de livraison de courses à domicile », *L'Usine Digitale*, 4 juin 2021 (en ligne : https://www.usine-digitale.fr/editorial/ces-start-up-qui-levent-des-millions-pour-leur-service-de-livraison-de-courses-a-domicile.N1100004 ; consulté le 18 juin 2021).

DE BRYE Valentine, « Test Bouton connecté Concierge : un assistant dont l'utilité nous échappe », *Les Numériques*, rubrique « Maison connectée », 14 décembre 2018 (en ligne : https://www.lesnumeriques.com/objet-connecte/concierge-concierge-p29407/test.html ; consulté le 23 août 2021).

DINGMAN Shane, « With Toronto, Alphabet looks to revolutionize city-building », *The Globe and Mail*, 17 octobre 2017 (en ligne : https://www.theglobeandmail.com/report-on-business/with-toronto-alphabet-looks-to-revolutionize-city-building/article36634779/ ; consulté le 3 mai 2022).

FANSTEN Emmanuel, « Etat d'urgence : « Une inscription dans le droit commun qui annule toute contestation » », *Libération*, rubrique « Société », 9 juin 2017 (en ligne : https://www.liberation.fr/france/2017/06/09/etat-d-urgence-une-inscription-dans-le-droit-commun-qui-annule-toute-contestation_1575516/ ; consulté le 2 janvier 2023). Section: Société.

FOROOHAR Rana, « Year in a Word: Techlash », *Financial Times*, rubrique « Year in a Word », 16 décembre 2018 (en ligne : https://www.ft.com/content/76578fba-fca1-11e8-ac00-57a2a826423e ; consulté le 15 juin 2022).

GAVOIS Sébastien, « On vous explique les protocoles pour les objets connectés : Zigbee, Z-Wave, EnOcean, DIO… », *Next INpact*, 29 juin 2022 (en ligne : https://www.nextinpact.com/article/69505/on-vous-explique-protocoles-pour-objets-connectes-zigbee-z-wave-enocean-dio? ; consulté le 1er juillet 2022).

GAVOIS Sébastien, « Domotique : CHIP devient Matter, la Zigbee Alliance renommée Connectivity Standards Alliance », *Next INpact*, 12 mai 2021 (en ligne : https://www.inpact-hardware.com/article/2469/domotique-chip-devient-matter-zigbee-alliance-renommee-connectivity-standards-alliance ; consulté le 27 septembre 2021).

GEBHART Andrew, « How to use the automatic responses on Ring Doorbells », *CNET*, 29 juillet 2021 (en ligne : https://www.cnet.com/home/smart-home/how-to-use-the-automatic-responses-on-ring-doorbells/ ; consulté le 9 août 2021).

GEORGESCU DE HILLERIN Marie et Marie CIOLFI, « Sonos One, la première enceinte qui mixe Alexa et Google Assistant », *Les Numériques*, 5 octobre 2017 (en ligne : https://www.lesnumeriques.com/platine-musicale-serveur-audio/sonos-one-p41423/sonos-one-premiere-enceinte-qui-mixe-alexa-google-assistant-n67073.html ; consulté le 17 septembre 2021).

GUE C., « Simone, la voix des gares », *leparisien.fr*, rubrique « /economie/ », 24 janvier 2004 (en ligne : https://www.leparisien.fr/economie/simone-la-voix-des-gares-25-01-2004-2004707818.php ; consulté le 22 décembre 2022).

GUO Eileen, « A Roomba recorded a woman on the toilet. How did screenshots end up on Facebook? », *MIT Technology Review*, 19 décembre 2022 (en ligne : https://www.technologyreview.com/2022/12/19/1065306/roomba-irobot-robot-vacuums-artificial-intelligence-training-data-privacy/ ; consulté le 20 décembre 2022).

HADERO Haleluya, « Amazon keeps growing, and so does its cache of data on you », *Los Angeles Times*, rubrique « Business », 23 août 2022 (en ligne : https://www.latimes.com/business/story/2022-08-23/amazon-keeps-growing-and-so-does-its-cache-of-data-on-you ; consulté le 28 août 2022).

HARTMANS Avery, « Google unveiled a new “experiment” that will impersonate a human to make restaurant reservations for you over the phone », *Business Insider*, rubrique « Tech », 8 mai 2018 (en ligne : https://www.businessinsider.com/google-assistant-makes-phone-calls-schedules-appointments-reservations-google-duplex-google-io-2018-5 ; consulté le 22 décembre 2022).

LAUSSON Julien, « Après le NutriScore pour l’alimentation, voilà le CyberScore pour la sécurité des sites », *Numerama*, 25 novembre 2021 (en ligne : https://www.numerama.com/tech/758555-apres-le-nutriscore-pour-lalimentation-voila-le-cyberscore-pour-la-securite-des-sites.html ; consulté le 26 novembre 2021).

LAUSSON Julien, « Les caméras de Ring passent enfin au chiffrement de bout en bout (si on active l’option) », *Numerama - Cyberguerre*, 14 juillet 2021 (en ligne : https://cyberguerre.numerama.com/12711-les-cameras-de-ring-passent-enfin-au-chiffrement-de-bout-en-bout-si-on-active-loption.html ; consulté le 27 juillet 2021).

LAUSSON Julien, « Le terrible incendie chez OVH rappelle l’enjeu de la redondance pour les sites web », *Numerama*, rubrique « Tech », 10 mars 2021 (en ligne :

https://www.numerama.com/tech/695843-le-terrible-incendie-chez-ovh-rappelle-lenjeu-de-la-redondance-pour-les-sites-web.html ; consulté le 2 janvier 2023).

LAZARUS David, « Column: Amazon wants to use radar so Alexa can watch as you sleep », *Los Angeles Times*, rubrique « Business », 16 juillet 2021 (en ligne : https://www.latimes.com/business/story/2021-07-16/column-amazon-radar-sleep ; consulté le 4 octobre 2021).

LEGOUGE Matthieu, « Comment transformer votre enceinte en enceinte connectée grâce à Balena Sound et un Raspberry Pi ? », *Clubic.com*, rubrique « Bluetooth », 4 mai 2020 (en ligne : https://www.clubic.com/raspberry-pi/article-891655-1-raspberry-pi-transformer-enceintes-airplay-spotify.html ; consulté le 18 mars 2022).

LIN Liza, « A Smart Lamp That Watches Kids When They Study Is a Hit in China », *Wall Street Journal*, rubrique « Tech », 31 mai 2021 (en ligne : https://www.wsj.com/articles/a-smart-lamp-that-watches-kids-when-they-study-is-a-hit-in-china-11622466002 ; consulté le 29 décembre 2022).

MACDONALD Cheyenne, « "I never knew Alexa had such a potty mouth": South Park episode activates viewers' Alexa and Google Home devices, creating "erroneous alarms" and shopping lists for "hairy balls" », *Daily Mail Online*, DMG Media Limited, rubrique « Science », 14 septembre 2017 (en ligne : http://global.factiva.com/redir/default.aspx?P=sa&an=DAMONL0020170914ed9e0093x&cat=a&ep=ASE ; consulté le 31 août 2021).

MARTIN Taylor, « How to set up voice recognition on the Amazon Echo », *CNET*, 12 octobre 2017 (en ligne : https://www.cnet.com/home/smart-home/how-to-setup-voice-profiles-on-the-amazon-echo-alexa/ ; consulté le 22 août 2022).

MATHIS Sommer et Alexandra KANIK, « Why you'll be hearing a lot less about 'smart cities' », *City Monitor*, 18 février 2021 (en ligne : https://citymonitor.ai/government/why-youll-be-hearing-a-lot-less-about-smart-cities ; consulté le 16 mars 2021).

MORIN Jérôme, « Faute de décret d'application, un tiers des lois n'est pas promulgué », *BFM TV*, rubrique « Politique », 12 juin 2015 (en ligne : https://www.bfmtv.com/politique/parlement/faute-de-decret-d-application-un-tiers-des-lois-n-est-pas-promulgue_AN-201506120073.html ; consulté le 26 juillet 2022).

MOSCA Marco, « Snips : "nous voulons détruire Alexa" Entretien avec Rand Hindi, son fondateur », *Les Numériques*, 26 août 2018 (en ligne : https://www.lesnumeriques.com/assistant-domotique/rand-hindi-snips-veut-detruire-alexa-a3897.html ; consulté le 7 décembre 2018).

O'BRIEN Matt, « Amazon says it's considered face scanning in Ring doorbells - Canadian Business », *Canadian Business*, rubrique « News », 20 novembre 2019 (en ligne : https://archive.canadianbusiness.com/business-news/amazon-says-its-considered-face-scanning-in-ring-doorbells/ ; consulté le 18 mars 2022).

OUEST-FRANCE, « La baby-sitter maltraitait l'enfant : les parents posent des caméras pour la filmer », *Ouest-France*, rubrique « France », 1er août 2011 (en ligne : https://www.ouest-france.fr/europe/france/la-baby-sitter-maltraitait-lenfant-les-parents-posent-des-cameras-pour-la-filmer-72017 ; consulté le 29 août 2022). Section: France.

PAISTEL Coline, « Étudiants à Rennes. Dormez, vous êtes surveillés... », *Ouest-France*, 6 septembre 2017 (en ligne : https://www.ouest-france.fr/bretagne/rennes-35000/etudiants-rennes-dormez-vous-etes-surveilles-5227294).

PRIEST David, « Alexa is starting to ask questions. How should we respond? », *CNET*, sans date (en ligne : https://www.cnet.com/home/smart-home/alexa-is-starting-to-ask-questions-how-should-we-respond/ ; consulté le 8 septembre 2020).

RAHMIL David-Julien, « « Chuuut, Instagram nous écoute » : retour sur une théorie pas si complotiste que ça », *L'ADN*, rubrique « Tendances », 30 juin 2021 (en ligne : https://www.ladn.eu/media-mutants/reseaux-sociaux/pourquoi-impression-instagram-ecoute-conversations/ ; consulté le 1er juillet 2021).

REES Marc, « Cyberscore : vers un vote conforme de la proposition de loi au Sénat », *Next INpact*, 18 février 2022 (en ligne : https://www.nextinpact.com/article/49887/cyberscore-vers-vote-conforme-proposition-loi-au-senat ; consulté le 18 février 2022).

RONFAUT Lucie, « L'avortement est un enjeu de cybersécurité », *Numerama*, 15 mai 2022 (en ligne : https://www.numerama.com/politique/960951-lavortement-est-un-enjeu-de-cybersecurite.html ; consulté le 16 juin 2022).

RUBIN Ben Fox, « Ads for voice assistants are here and they're already terrible », *CNET News.com*, CNET Networks Inc., 21 avril 2017 (en ligne : http://global.factiva.com/redir/default.aspx?P=sa&an=CNEWSN0020170421ed4l00003&cat=a&ep=ASE ; consulté le 31 août 2021).

SERRAND Didier, « HD 2000 - Une "première" unique en Europe », *Réseau - Mensuel de l'innovation régionale*, décembre 1989, p. 1-2 (en ligne : https://www.espace-sciences.org/sites/espace-sciences.org/files/images/sciences-ouest/numeros/r_051_12_1989.pdf).

STEPHAN Laure, « « L'annonce de la taxe sur WhatsApp est l'étincelle » : colère contre de nouveaux prélèvements à Beyrouth », *Le Monde*, 18 octobre 2019 (en ligne : https://www.lemonde.fr/international/article/2019/10/18/tout-est-cher-au-liban-on-n-en-peut-plus-a-beyrouth-des-milliers-des-manifestants-contre-de-nouvelles-taxes_6016010_3210.html ; consulté le 17 septembre 2021).

TRUJILLO Elsa, « Sur ces sites français, refuser les cookies ne suffit pas à ne plus être tracé », *BFM TV*, rubrique « Vie numérique », 10 décembre 2019 (en ligne : https://www.bfmtv.com/tech/vie-numerique/sur-ces-sites-francais-refuser-les-cookies-ne-suffit-pas-a-ne-plus-etre-trace_AN-201912100036.html ; consulté le 14 juin 2022).

TURCAN Marie, « Monsieur Cuisine Connect : micro caché, Android non sécurisé... les dessous du robot cuiseur de Lidl », *Numerama*, 13 juin 2019 (en ligne : https://www.numerama.com/tech/525214-monsieur-cuisine-connect-micro-cache-android-non-securise-les-dessous-du-robot-cuisine-de-lidl.html ; consulté le 23 juillet 2022).

UNTERSINGER Martin, « La justice européenne invalide le très controversé Safe Harbor, un accord sur les données personnelles », *Le Monde.fr*, rubrique « Pixels », 6 octobre 2015 (en ligne : https://www.lemonde.fr/pixels/article/2015/10/06/la-justice-europeenne-invalide-le-tres-controverse-accord-safe-harbor-sur-les-donnees-personnelles_4783262_4408996.html ; consulté le 12 juillet 2022).

VIRILIO Paul, « Un monde surexposé - Fin de l'histoire, ou fin de la géographie ? », *Le Monde diplomatique*, 1er août 1997 (en ligne : https://www.monde-diplomatique.fr/1997/08/VIRILIO/4878 ; consulté le 23 mai 2019).

WOOLDRIDGE Adrian, « The coming tech-lash », *The Economist*, 18 novembre 2013 (en ligne : https://www.economist.com/news/2013/11/18/the-coming-tech-lash ; consulté le 16 juin 2022).

AUTRES (ARTICLES DE LOI, BLOGS, USUELS…)

Anonyme, « Loi n° 2022-309 du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public », dans *Code de la consommation*, 3 mars 2022 (en ligne : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045294275 ; consulté le 26 juillet 2022).

BORTZMEYER Stéphane, « RFC 9124: A Manifest Information Model for Firmware Updates in Internet of Things (IoT) Devices », sur *Blog de Stéphane Bortzmeyer*, 15 janvier 2022 (en ligne : https://www.bortzmeyer.org/9124.html ; consulté le 1er février 2022).

BORTZMEYER Stéphane, « RFC 8576: Internet of Things (IoT) Security: State of the Art and Challenges », sur *Blog de Stéphane Bortzmeyer*, avril 2019 (en ligne : https://www.bortzmeyer.org/8576.html ; consulté le 28 mars 2021).

BRELAND Ali, « How Amazon bullies, manipulates, and lies to reporters », sur *Mother Jones*, rubrique « Politics », 25 juin 2021 (en ligne : https://www.motherjones.com/politics/2021/06/amazon-journalists-pr-tactics/ ; consulté le 26 juin 2021).

CLINTON William J., « Administration of Export Controls on Encryption Products », dans *Executive Order*, nº 13026, 1996.

GAFFIOT Félix, « Ubi », dans *Dictionnaire latin français*, Paris (France), Hachette, 1934, p. 1620-1621 (en ligne : https://www.lexilogos.com/latin/gaffiot.php?q=ubique).

GAUDIAUT Tristan, « Les métropoles européennes avec le plus de caméras au km^2 », sur *Statista Infographies*, 23 juin 2021 (en ligne : https://fr.statista.com/infographie/25143/densite-de-cameras-de-videosurveillance-dans-les-grandes-villes-europeennes/ ; consulté le 25 juin 2021).

GHADIRY Amir, « Is My Google Home Spying On Me? », sur *SogetiLabs*, 5 avril 2017 (en ligne : https://labs.sogeti.com/google-home-spying/ ; consulté le 19 novembre 2020).

GUARIGLIA Matthew, « Amazon's Ring Is a Perfect Storm of Privacy Threats », sur *Electronic Frontier Foundation*, 8 août 2019 (en ligne : https://www.eff.org/deeplinks/2019/08/amazons-ring-perfect-storm-privacy-threats ; consulté le 12 septembre 2019).

IDC, « Répartition des expéditions de smartphones dans le monde par système d'exploitation entre 2013 et 2022 », sur *Statista*, décembre 2018 (en ligne : https://fr-statista-com.ezproxy.u-pec.fr/statistiques/570954/part-de-marche-mondiale-des-systeme-d-exploitation-de-smartphone-en-expeditions-d-unites--2020/ ; consulté le 22 août 2022).

JOLIVEAU Thierry, « Géomatique et géonumérisation », sur *Monde géonumérique*, 8 octobre 2007 (en ligne : https://mondegeonumerique.wordpress.com/geomatique-et-cie/geomatique-et-geonumerisation/ ; consulté le 8 octobre 2018).

KELLEY Jason et Matthew GUARIGLIA, « Amazon Ring Must End Its Dangerous Partnerships With Police », sur *Electronic Frontier Foundation*, 10 juin 2020 (en ligne : https://www.eff.org/fr/deeplinks/2020/06/amazon-ring-must-end-its-dangerous-partnerships-police ; consulté le 13 septembre 2021).

KINSELLA Bret, « Nearly 90 Million U.S. Adults Have Smart Speakers, Adoption Now Exceeds One-Third of Consumers », sur *Voicebot.ai*, rubrique « smart speaker », 28 avril 2020 (en ligne : https://voicebot.ai/2020/04/28/nearly-90-million-u-s-adults-have-smart-speakers-adoption-now-exceeds-one-third-of-consumers/ ; consulté le 11 mai 2020).

KRAUS Rachel, « Ring watched your kids trick or treat and then bragged about it », sur *Mashable*, 1er novembre 2019 (en ligne : https://mashable.com/article/ring-halloween-surveillance/ ; consulté le 24 mai 2021).

LA QUADRATURE DU NET, « Manifeste », sur *Technopolice*, sans date (en ligne : https://technopolice.fr/presentation/ ; consulté le 20 juin 2022).

LEVY Jacques, « Espace », dans Jacques Lévy et Michel Lussault (éd.), *Dictionnaire de la géographie et de l'espace des sociétés*, Paris (France), Belin, 2003 2013, p. 353-360.

LEVY Jacques, « Substance », dans Jacques Lévy et Michel Lussault (éd.), *Dictionnaire de la géographie et de l'espace des sociétés*, Paris (France), Belin, 2003, p. 880-881.

LUSSAULT Michel, « Spatialité », dans Jacques Lévy et Michel Lussault (éd.), *Dictionnaire de la géographie et de l'espace des sociétés*, Paris (France), Belin, 2003, p. 866-868.

LUSSAULT Michel, « Actant », dans Jacques Lévy et Michel Lussault (éd.), *Dictionnaire de la géographie et de l'espace des sociétés*, Paris (France), Belin, 2003, p. 38-39.

LUSSAULT Michel, « Agent », dans Jacques Lévy et Michel Lussault (éd.), *Dictionnaire de la géographie et de l'espace des sociétés*, Paris (France), Belin, 2003, p. 47-48.

LUSSAULT Michel, « Proxémie », dans Jacques Lévy et Michel Lussault (éd.), *Dictionnaire de la géographie et de l'espace des sociétés*, Paris (France), Belin, 2003, p. 750-751.

MAJAK R. Roger, « Revised U.S. Encryption Export Control Regulations », dans *RIN*, 2000.

MALANOV Alexey, « Smartphones sur écoute : mythe ou réalité ? », sur *Kapersky Daily*, 6 août 2019 (en ligne : https://www.kaspersky.fr/blog/smartphones-eavesdropping/12070/ ; consulté le 9 janvier 2023).

MANACH Jean-Marc, « Le «fichier des gens honnêtes», ce révélateur d'un mal français », sur *Slate.fr*, rubrique « France », 1er mars 2017 (en ligne : http://www.slate.fr/story/138356/saga-generalisation-fichier-des-gens-honnetes ; consulté le 27 mai 2021).

MARTIN Robert, « Immunité », dans *Dictionnaire du Moyen Français*, Nancy (France), ATILF - CNRS & Université de Lorraine, 2020 (en ligne : zeus.atilf.fr/scripts/dmfX.exe?LEM=immunit%E9;XMODE=STELLa;FERMER;;AFFICHAGE=0;MENU=menu_dmf;;ISIS=isis_dmf2020.txt;MENU=menu_recherche_dictionnaire;OUVRIR_MENU=1;ONGLET=dmf2020;OO1=2;OO2=1;OO3=-1;s=s13532b0c;LANGUE=FR; ; consulté le 1er juin 2021).

MONSEES David, « More information about our processes to safeguard speech data », sur *Google*, 11 juillet 2019 (en ligne : https://blog.google/products/assistant/more-information-about-our-processes-safeguard-speech-data/ ; consulté le 18 novembre 2020).

MORGENSTERN Maik, « Careless Whisper: Does Amazon Echo send data in silent mode? », sur *AV-TEST Internet of Things Security Testing Blog*, 8 juin 2017 (en ligne : https://www.iot-tests.org/2017/06/careless-whisper-does-amazon-echo-send-data-in-silent-mode/ ; consulté le 19 novembre 2020).

NAIR Sanjay, « Trust in Tech Is Wavering and Companies Must Act », sur *Edelman*, 8 avril 2019 (en ligne : https://www.edelman.com/research/2019-trust-tech-wavering-companies-must-act ; consulté le 23 mars 2022).

NIZON Michel, « L'ICO de Snips passée au crible des 3 critères de notre fiche d'analyse. », sur *Le Crowdfunding, ça vous chatouille ou ça vous gratouille ?*, rubrique « Analyse de start-up », 24 juin 2018 (en ligne : https://www.michelnizon.com/lico-de-snips-passee-au-crible-des-3-criteres-de-notre-fiche-danalyse/ ; consulté le 3 janvier 2023).

O'SHEA Sean, « Ann Cavoukian, former Ontario privacy commissioner, resigns from Sidewalk Labs », sur *Global News*, 21 octobre 2018 (en ligne : https://globalnews.ca/news/4579265/ann-cavoukian-resigns-sidewalk-labs/ ; consulté le 6 novembre 2018).

PLANCHER Alexandre, « Google va payer 15 milliards de dollars à Apple pour rester le moteur de recherche par défaut », sur *Siècle Digital*, 27 août 2021 (en ligne : https://siecledigital.fr/2021/08/27/google-va-payer-15-milliards-de-dollars-a-apple-pour-rester-le-moteur-de-recherche-par-defaut/ ; consulté le 16 septembre 2021).

RANKIN Kyle, « Your Phone Is Your Castle », sur *Purism*, rubrique « Librem 5 », 11 septembre 2020 (en ligne : https://puri.sm/posts/your-phone-is-your-castle/ ; consulté le 15 octobre 2020).

RUSSAKOVSKII Artem, « Google is permanently nerfing all Home Minis because mine spied on everything I said 24/7 [Update x2] », sur *Android Police*, rubrique « News », 10 octobre 2017 (en ligne : https://www.androidpolice.com/2017/10/10/google-nerfing-home-minis-mine-spied-everything-said-247/ ; consulté le 6 juillet 2021).

SCHWARTZ Eric Hal, « Alexa Can Now Adjust Your Smart Home Devices Without Needing to Ask Permission », sur *Voicebot.ai*, rubrique « Amazon alexa », 26 janvier 2021 (en ligne : http://voicebot.ai/2021/01/26/alexa-can-now-adjust-your-smart-home-devices-without-needing-to-ask-permission/ ; consulté le 26 juin 2021).

SERFATY-GARZON Perla, « Cocooning », dans Marion Segaud, Jacques Brun et Jean-Claude Driant (éd.), *Dictionnaire critique de l'habitat et du logement*, Paris (France), Armand Colin, 2003, p. 74-75 (en ligne : http://perlaserfaty.net/wp-content/uploads/2017/01/Cocooning-un-texte-de-Perla-Serfaty-Garzon.pdf).

SSALI Julie, « Infographic: Half the global population are now using the mobile internet », sur *GSMA Intelligence*, février 2020 (en ligne : https://data.gsmaintelligence.com/research/research/research-2020/infographic-half-the-global-population-are-now-using-the-mobile-internet ; consulté le 15 février 2022).

TURNER Michele, « 4 Google smart home updates that Matter », sur *Google*, 19 mai 2021 (en ligne : https://blog.google/products/google-nest/four-google-smart-home-updates-matter/ ; consulté le 11 septembre 2021).

VALLET Félicien, « Chéri(e), mon smartphone m'écoute ?! », 2 juillet 2021 (en ligne : https://linc.cnil.fr/fr/cherie-mon-smartphone-mecoute ; consulté le 30 août 2021).

« David Lyon retires from Queen's; remains P.I. of Big Data Surveillance », sur *The Surveillance Studies Centre*, 6 juillet 2021 (en ligne : https://www.sscqueens.org/news/david-lyon-retires-from-queens-remains-pi-of-big-data-surveillance ; consulté le 23 juillet 2021).

« Internet Society et Internet Society France présentent 22 recommandations pour un Internet des objets de confiance », sur *Internet Society France*, 5 mars 2020 (en ligne : https://www.isoc.fr/iot-22-recommandations/ ; consulté le 8 mai 2021).

« L'Internet Society fait progresser la sécurité des objets connectés », sur *Internet Society France*, rubrique « A la une », 8 janvier 2019 (en ligne : https://www.isoc.fr/lancement-groupe-iot/ ; consulté le 13 juillet 2022).

« Derrière les assistants vocaux, des humains vous entendent », sur *La Quadrature du Net*, rubrique « Données personnelles », 18 mai 2018 (en ligne : https://www.laquadrature.net/2018/05/18/temoin_cortana/ ; consulté le 9 février 2023).

« The Glass Room Experience », sur *La Gaîté Lyrique*, 2018 (en ligne : https://gaite-lyrique.net/evenement/the-glass-room-experience ; consulté le 5 septembre 2021).

« Une enquête d'Unisys révèle qu'une écrasante majorité de Français sont préoccupés par la collecte et l'utilisation de leurs données personnelles via Internet », sur *Unisys*, 20 juillet 2015 (en ligne : https://www.unisys.com/fr/news-release/fr-unisys-security-insights/ ; consulté le 27 septembre 2019).

« Voyeurisme », dans *Trésor de la Langue Française informatisé*, Nancy (France), CNRS & Université de Lorraine, 1994 (en ligne : https://www.cnrtl.fr/definition/voyeurisme ; consulté le 9 août 2022).

« La Paillasse », sur *La Paillasse*, sans date (en ligne : https://lapaillasse.org ; consulté le 5 septembre 2021).

« Closet », sans date (en ligne : https://www.merriam-webster.com/dictionary/closet ; consulté le 18 juin 2021).

« Cocon », dans *Dictionnaire de l'Académie française*, Paris (France), Centre national de ressources textuelles et lexicales, sans date (en ligne : https://www.cnrtl.fr/definition/academie9/cocon).

« About the Aware Home Research Initiative - Georgia Institute of Technology », sur *Aware Home Research Initiative*, sans date (en ligne : https://awarehome.gatech.edu/about-aware-home-research-initiative ; consulté le 24 avril 2022).

« Big Brother dans des lits connectés d'étudiants ? La réponse du concepteur, le retrait du Crous », sans date (en ligne : https://www.nextinpact.com/article/27165/105122-big-brother-dans-lits-connectes-detudiants-la-reponse-concepteur-retrait-crous ; consulté le 17 août 2022).

« Conseils pour respecter la vie privée d'autrui lorsque vous utilisez les produits Nest », sur *Aide Google Nest*, sans date (en ligne : https://support.google.com/googlenest/answer/9247517?hl=fr-LU ; consulté le 19 mars 2022).

TABLES DES ILLUSTRATIONS

FIGURES

TABLEAUX

PHOTOGRAPHIES

LISTE DES SIGLES ET ABREVIATIONS

API : *Application Programming Interface* (en français, interface de programmation d'application)

BATX : Baidu, Alibaba, Tencent et Xiaomi

CIA : Central Intelligence Agency

CIL : conseiller informatique et libertés

CNIL : commission nationale informatique et libertés

Crédoc : Centre de Recherche pour l'ÉtuDe et l'Observation des Conditions de vie

DPO : *data protection officers*

FAI : fournisseur d’accès à Internet

GAFAM : Google, Apple, Facebook, Amazon et Microsoft

I2P : *Invisible Internet Project*

IETF : Internet Engineering Task Force (voir SDO)

IoT : *Internet of Things* (en français, Internet des objets)

IRTF : Internet Research Task Force (voir SDO)

ISOC : Internet Society (voir SDO)

LINC : laboratoire d'innovation numérique de la CNIL

LQDN : la Quadrature du Net

MIT : Massachusets Institute of Technology

NSA : National Security Agency

PET : *Privacy-Enhancing Technology* (en français, technologies de protection de la vie privée)

RFID : *Radio Frequency Identification*

RGPD : règlement général sur la protection des données

SDO : *Standard Development Organizations* (en français, organisation de normalisation d'Internet)

SSID : *service set identifier* (en français, identifiant défini de service)

TALN : traitement automatisé du langage naturel

TCP/IP : *Transmission Control Protocol* / *Internet Protocol* (protocoles réseaux pour les échanges sur Internet)

TIC : technologies de l'information et de la communication

Tor : *The Onion Router* (en français, réseau de routage en oignon)

UHRS : *Universal Human Relevance System* (voir TALN)

URL : *Uniform Resource Locator* (en français, localisateur uniforme de ressource)

INDEX

INDEX DES AUTEURS

INDEX DES NOTIONS

D

E

G

H

I

L

M

INDEX DES ENTREPRISES, INSTITUTIONS ET PRODUITS

TABLE DES MATIERES

Table des matières

RESUME

FR : Les enceintes connectées et la myriade de périphériques de l'IoT qui peuvent leur être associés introduisent dans l'espace domestique de nombreux capteurs, à commencer par des microphones perfectionnés, mais aussi de plus en plus des caméras ou des détecteurs de mouvement. Connectées à Internet, elles sont opérées par des entreprises très puissantes comme Google ou Amazon, dont le modèle d'affaires consiste à exploiter les données produites par leurs utilisateurs afin de les profiler. Leur introduction au sein des espaces domestiques, historiquement construits comme les lieux par excellence du ressourcement et de l'intimité personnelle ou familiale, provoque des réactions de rejet marquées de la part de nombreux individus. L'expérience montre en effet que les pratiques de traçage sur Internet ont déjà mené à une forte érosion de la vie privée en ligne. L'extension de la numérisation du Monde aux espaces domestiques pourrait-elle mener à la fin du domicile en tant qu'espace perçu et conçu comme le lieu paroxystique du privé ?

Mots-clefs : vie privée, domotique, espace domestique, dématérialisation (informatique)

EN : Smart speakers and the myriad of IoT devices that can be associated with them introduce many sensors into the domestic space, starting with sophisticated microphones, but also increasingly cameras or motion detectors. Connected to the Internet, they are operated by powerful companies like Google or Amazon, whose business model consists of exploiting the data produced by their users in order to profile them. Their introduction into domestic spaces, historically constructed as the places of self care and personal or family intimacy, provokes marked reactions of rejection from many individuals. Experience shows that tracking practices on the Internet have already led to a strong erosion of privacy online. Could the extension of the digitization of the World to domestic spaces lead to the end of the home as a space perceived and conceived as the paroxysmal place of privacy?

Keywords : privacy, home automation, domestic space, digitalization (IT)