La protection automatisée des données à caractère personnel et la vérification automatisée d'actes juridiques

Nino Tskhovrebashvili

▶ **To cite this version:**

Nino Tskhovrebashvili. La protection automatisée des données à caractère personnel et la vérification automatisée d'actes juridiques. Intelligence artificielle [cs.AI]. Université Panthéon-Sorbonne - Paris I, 2022. Français. NNT : 2022PA01E014 . tel-03852208

HAL Id: tel-03852208
https://theses.hal.science/tel-03852208

Submitted on 14 Nov 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

UNIVERSITÉ PARIS 1
PANTHÉON SORBONNE

THESE

Pour obtenir le grade de

DOCTEUR DE L'UNIVERSITE PARIS 1 PANTHEON SORBONNE
Spécialité : informatique

Présentée par :
Nino Tskhovrebashvili

Titre :

La protection des données à caractère personnel et la vérification automatisée d'actes juridiques

Thèse soutenue publiquement le 24/02/2022
Devant le jury composé de :

M. David NACCACHE		Directeur de These
Mme.	Benedicte LE GRAND	Exeminateur
M.	Revaz KAKUBAVA	Exeminateur
Mme.	Lily PETRIASHVILI	Rapporteur
M.	Ioseb KARTVELISHVILI	Rapporteur

Vouloir nous brûle et pouvoir nous détruit ; mais savoir laisse notre faible organisation dans un perpétuel état de calme.

Honoré de Balzac

J'adresse mes remerciements à mon directeur de thèse, Monsieur David Naccache, Professeur à l'ENS Paris, membre du DI-ENS, qui a toujours été présent à mes côtés pour m'orienter. Il m'a permis d'approfondir mes travaux et développer mes idées. Je lui suis reconnaissante pour son suivi pédagogique, pour son accompagnement scientifique et pour ses qualités humaines. Son intelligence et sa réputation m'ont toujours poussée vers plus de responsabilité et m'ont enthousiasmée pour réaliser des projets importants.

J'adresse mes remerciements à Monsieur Camille Salinesi, Professeur des Universités à l'Université Paris 1 Panthéon Sorbonne, pour son attention envers mes travaux, pour ses conseils avisés.

J'adresse mes remerciements à Mme Bénédicte Le Grand, Professeur des universités (Informatique) et Directrice de laboratoire CRI, pour son écoute et son attention qui ont été prépondérantes pour la réussite de cette thèse.

Je voudrais remercier chaleureusement Mme Selmin Nurcan, Maître de Conférences et Directrice du Master programme *Systèmes d'Information et de Connaissance (SIC) & Management of Information and Knowledge Systems (MIKS)* de m'avoir fait confiance tout au long de ces années. Ses remarques et sa gentillesse m'ont permis d'atteindre les objectifs de l'enseignement dans le cadre du doctorat.

Je remercie Mmes Sophie Tournon, Ketevan Tsiklauri, Marie Otiashvili Arnaud, Shorena Astavishvili, Gocha Chitaishvili, Temur Maisuradze, Solomon Nergadze, et David Plipilashvili pour leur aide durant ces travaux.

Je remercie également Mme Manuele Kirsch Pinheiro, maître de conférences et M. Fabrice Boissier, M. Stefane Mélo pour leur soutien et leur gentillesse. J'adresse de sincères remerciements à Mme Nino Tshukhishvili, secrétaire parlementaire de l'association des jeunes juristes, pour son accueil chaleureux et ses recommandations.

Je remercie chaleureusement les étudiants français et géorgiens ainsi que l'équipe de l'université de Robakidze pour leur participation dans mes recherches durant ces années. Je souhaite remercier également toute l'équipe du CRI de l'Université Paris 1 Panthéon-Sorbonne et les différentes personnes qui m'ont permis, par leurs conseils, de pousser un peu plus haut mon raisonnement.

Je remercie l'association « Droni » et mes amies Nino et lela pour leur soutien et encouragements.

Je remercie enfin les membres de ma famille qui ont toujours été à mes côtés pendant cette thèse et qui m'ont toujours encouragée. Je remercie grandement ma fille, Gabriella, qui me donne l'envie de grandir et réussir dans la vie.

Abstract

The automation of information exchange links individuals and companies via an increasing number of legal acts/texts. These acts/texts specify the economic obligations of the parties as well as the operational constraints governing the performance of many services. When a consumer signs a contract with an Internet Service Provider (ISP), the contracting parties bind each other. On the one hand, the consumer undertakes to pay the subscription fees. The ISP undertakes, for its part, to provide a service with specific characteristics. Typically, the ISP will commit to a level of personal data protection, quality of service or many other contractual obligations.

To date, the balance of power between consumers and digital service provider's leans strongly in favor of the providers: in the event of non-payment, the consumer will be penalized by cutting off his Internet connection, whereas in the event of disrespect for his contractual obligations, it will be difficult to sanction the supplier.

A precise legislative framework relating to the protection of personal data has existed since the first European data protection directive of 1995. A new directive was proposed in 2012 in order to give citizens back control of their personal data. More recently, in 2018, the General Data Protection Regulation (GDPR) came into force.

France was one of the first countries to legislate on the collection and processing of personal data. In 2020, the CNIL carried out more than 247 checks and received more than 13,585 complaints from users. The commission had 9,677,000 million visits to its website and 20,452 electronic requests on "Need help". These figures reflect a great concern related to the deletion of data on sites, the confidentiality of personal data and the surveillance of citizens.

It is important to note that all the checks carried out by the CNIL are carried out in an "artisanal" manner, by human experts. Collection and transmission of data are carried out at high speed around the world. On the one hand, technology has evolved, but on the other hand this has raised the issue of privacy. For companies, the collection and processing of data is a strategic matter that must be dealt with on the one hand by laws and on the other by personal ethics.

Considering the above it is important to find answers to the following questions: what is privacy, and where is the line between personal data and commercial and security interests?

Keywords: Data protection; Social networks; Encryption; GDRP; General Data Protection Regulation; Digital culture; E commerce; Right to be forgotten, DESI, Algorithms and Data Verification.

Résumé

L'automatisation des échanges d'information lie individus et entreprises via un nombre croissant d'actes/textes juridiques. Ces actes/textes spécifient les obligations économiques des parties ainsi que les contraintes opérationnelles régissant l'exécution de nombreux services.

Lorsqu'un consommateur signe un contrat avec un fournisseur d'accès Internet (FAI), les parties contractantes s'engagent mutuellement. D'une part, le consommateur s'engage à payer les frais d'abonnement. Le FAI s'engage, quant à lui, à assurer un service ayant des caractéristiques précises. Typiquement, le FAI s'engagera sur un niveau de protection des données personnelles, de qualité de service ou sur bien d'autres obligations d'ordre contractuel.

A ce jour, le rapport de force entre consommateurs et fournisseurs de services numériques penche fortement en faveur des fournisseurs : en cas d'impayés, le consommateur sera sanctionné par la coupure de sa liaison Internet, alors qu'en cas d'irrespect de ses obligations contractuelles, il sera difficile de sanctionner le fournisseur.

Un cadre législatif précis relatif à la protection des données personnelles existe depuis la première directive européenne relative à la protection des données de 1995. Une nouvelle directive a été proposée en 2012 afin de redonner aux citoyens le contrôle de leurs données personnelles. Plus récemment, en 2018, le Règlement général sur la protection des données (RGPD) est entré en application.

La France fut l'un des premiers pays à légiférer sur la collecte et le traitement des données personnelles. La CNIL a réalisé en 2020 plus de 247 contrôles et reçu plus 13 585 plaintes de la part des usagers. La commission comptabilisait 9 677 000 millions de visites sur son site web et 20 452 requêtes par voie électronique sur « Besoin d'aide ». Ces chiffres reflètent une grande préoccupation liée à la suppression des données sur des sites, à la confidentialité des données à caractère personnel et à la surveillance des citoyens.

Il est important de noter que tous les contrôles effectués par la CNIL sont effectués de manière « artisanale », par des experts humains.

Récolte et transmission des données s'effectuent à grande vitesse à travers le monde. D'une part, la technologie a évolué, mais d'autre part cela a posé le problème de la protection de la vie privée. Pour les entreprises, la collecte et le traitement de données sont une affaire stratégique qui doit être traitée d'une part par les lois et d'autre part par l'éthique personnelle.

La variété des réponses que ce sujet suscite pose la question : en quoi consiste le respect de la vie privée, et où se trouve la frontière entre les données personnelles et les intérêt commerciaux et sécuritaires ?

Mots clés : Protection des données ; Réseaux sociaux; chiffrement, RGPD ; Règlement général sur la protection des données ; culture numérique ; Commerce électronique; Droit à l'oubli, DESI, Algorithmes de Vérification

SOMMAIRE

CHAPITRE 1

Introduction

Ces dernières années, des données à caractère personnel concernant chacun d'entre nous sont collectées, traitées et diffusées activement et de manière massive. Très souvent, nous négligeons nous-mêmes ces données personnelles et, par conséquent, la protection de notre vie privée devient de plus en plus complexe.

Selon une définition générale, les données à caractère personnel recouvrent tous les types d'informations qui se rapportent à une personne physique permettant de distinguer celle-ci, directement ou indirectement, d'un ensemble de personnes. Il peut s'agir d'un numéro d'identification physique/sociale ou d'un enregistrement audio/vidéo.

Les progrès de la technologie ont, d'une part, joué un rôle positif dans l'industrie et, d'autre part, augmenté le risque de confidentialité. Au fil des années, plusieurs pays européens ont adopté différentes lois au niveau national et ont uni leurs forces dans le cadre du Groupe 29. Le 23 mai de 2018 est la date de l'adoption du Règlement général sur la Protection des Données, RGPD, qui constitue un cadre solide et cohérent dans l'Union. Or, malgré le bon fonctionnement des organisations de défense des droits de l'homme, il reste beaucoup à faire dans le domaine de la protection des données à caractère personnel

1.1 Contribution de la thèse

Dans le cadre de notre thèse, nous avons étudié les expériences de différents pays au niveau législatif et gouvernemental. Nous avons organisé des recherches en milieu académique, en France et en Géorgie, sur le sujet de la protection des données et de la vie privée, et nous avons entre autres étudié différents sites internet publics géorgiens. Les résultats collectés nous donnent la possibilité de voir les attitudes concernant la protection de la vie privée au prisme de nationalités, et donc de cultures, différentes.

Nous avons de plus constaté qu'une certaine organisation recueille les données disponibles sur des pages Web via un algorithme spécial et les publie sur sa page Web sous une forme plus facile d'accès. En indiquant les données d'identification d'une personne dans les options de recherche, il nous a été possible d'obtenir une information complète liée à la personne en question. Dans ce manuscrit, nous avons élaboré des recommandations qui peuvent éviter les manipulations sur les sites internet qui seraient préjudiciable à nos données ainsi que le non-respect des données à caractère personnel.

1.2. Structure de la thèse

Notre thèse se compose :

- de l'introduction,
- des objectifs,
- des recherches menées auprès de différentes institutions,
- de l'analyse des données et des recommandations.

Elle contient les chapitres suivants :

1. **Introduction**
2. **Mécanismes et cadre législatif de la protection de la vie privée au niveau européen et international**
3. **Protection alternative des données à caractère personnel**
4. **Aspect économique et social**
5. **Protection des données, réseaux sociaux et moteurs de recherches**
6. **Institutions financières et règles à respecter au niveau de la protection des données à caractère personnel**
7. **Commerce et obligation de protection des données à caractère personnel**
8. **Contrat de vente et risques de protection de la vie privée**
9. **Niveau de la protection de la vie privée dans les pays non représentants de l'UE : ex. de la Géorgie**
10. **RGPD : Nouvelles règles appliquées**
11. **Vérification automatisée**
12. **Protocole de sécurité**
13. **Automatisation des documents : atouts et inconvénients**
    - **Résultats des recherches et recommandations**

14 **Bibliographie**

CHAPITRE 2

Données à caractère personnel et normes législatives

Dans ce chapitre, nous allons étudier le cadre législatif concernant les données à caractère personnel et les normes internationales concernant la vie privée. Nous montrerons la mission de la CNIL dans la préparation **des mesures législatives et réglementaires de la protection de la vie privée.**

2.1 Introduction

La loi Informatique et libertés de 1978 est une loi française adoptée à la suite de l'affaire SAFARI qui avait provoqué un scandale dans la société.

En 1974, le ministre de l'Intérieur avait décidé de créer un fichier automatisé nommé SAFARI, acronyme de « Système Automatisé pour Fichier Administrative et Répertoire des Individus ». Ce système prévoyait de créer une base de données de la population à partir du numéro de Sécurité sociale comme identifiant.

Devant le mécontentement provoqué par cette idée surnommée « La chasse aux Français », le Premier ministre de l'époque fut obligé de le retirer et de créer la commission « Informatique et Liberté » chargée de préciser l'utilisation des moyens informatiques.

L'objet de cette commission était de dénoncer les abus de l'informatique via l'institution d'une autorité administrative centralisée. D'après le rapport du conseiller d'Etat Bernard Tricot, l'Etat s'engageait à renforcer les moyens pour contrôler les activités humaines en utilisant l'informatique dans le sens technique en appréciant la liberté de l'homme.

Dans le même temps, ailleurs en Europe, des lois semblables relatives à l'informatique étaient adoptées. En République fédérale d'Allemagne, une telle loi est entrée en application en 1978, et en Belgique, un projet de loi sur la vie privée fut déposé au Sénat dès 1976.

La loi Informatique et liberté a été modifiée par un décret de 1991. Cette modification reconnaît les fichiers des Renseignements généraux en permettant la collecte, la conservation et le traitement d'informations relatives aux personnes majeures, qui font apparaître des signes particuliers ainsi que les activités politiques, philosophiques, religieuses ou syndicales.

La loi a encore été modifiée en 2004, pour transposer la directive sur la protection des données. Les données à caractère personnel ne doivent plus être soumises à un traitement automatisé si elles ne remplissent pas les exigences posées par ces principes : proportionnalité, transparence et finalité. En 2005, la loi modifiée est complétée par un décret élargissant le domaine des données personnelles.

Au niveau international, vers 1970, le Conseil de l'Europe a conclu que les articles de la CEDH comportaient un grand nombre de lacunes dans la portée de la notion de vie privée, l'accent était surtout mis sur les menaces concernant la vie privée. Ces initiatives ont encouragé le Conseil de l'Europe à préparer un traité international, première réglementation commune en ce domaine. Le Conseil de l'Europe a rédigé la convention [78] sur la protection des Données qui s'applique aux membres du conseil, dont des Etats membres de l'UE. Cette convention déclare qu'elle « garantit à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant. Les données personnelles doivent être « obtenues et traitées **loyalement et licitement** » et doivent être « enregistrées pour des finalités déterminées et légitimes et ne doivent pas être utilisées de manière incompatible avec ces finalités»[77].

Un autre point significatif est que les données doivent être « conservées sous une forme permettant l'identification des personnes concernées pendant **une durée n'excédant pas celle nécessaire aux finalités** pour lesquelles elles sont enregistrées [77] ».

Des réglementations strictes sont prévues pour le traitement des données particulièrement sensibles. Les données « révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle » doivent être traitées en lien avec le droit interne et des garanties appropriées. Tout abus de traitement peut être passible de condamnations pénales.

La Cour européenne a joué un rôle important dans la formalisation de cette convention. La Cour établit que la « vie privée » peut également comprendre des aspects de la vie professionnelle ainsi que des comportements en public, dans le passé ou non.

La Commission européenne a rédigé une proposition de directive pour harmoniser les législations dans les États membres relative à la protection des données. La proposition de la Commission était une condition indispensable pour le développement ultérieur des données et la création des garanties appropriées.

La commission a rendu la directive 95/46/CE22 [91] qui accordait aux États membres un délai de trois ans pour sa transposition dans leur législation. Cette directive poursuivait un double objectif :

- Elle contenait l'obligation de garantir la protection des libertés et des droits fondamentaux, en particulier pour leur vie privée, à l'égard du traitement des données à caractère personnel
- Elle contenait également l'obligation de ne pas restreindre la libre circulation des données à caractère personnel entre États membres pour des raisons liées à la protection précitée.

Un aspect intéressant de la directive réside dans la réglementation en matière de transfert de données avec les pays tiers. La directive s'applique en premier lieu au traitement de données à caractère personnel effectué « dans le cadre des activités d'un établissement » sur le territoire de l'État membre de l'UE (Article 4, paragraphe 1, point a) [91]. **D'après les principes de la directive, les données à caractère personnel peuvent être transférées uniquement aux pays tiers qui possèdent un niveau de protection adéquat.** Sans cela, le transfert n'est autorisé que dans certaines situations. Internet posait de nouveaux défis, surtout en ce qui concerne le positionnement des sites web, des moteurs de recherche, des réseaux sociaux mais également pour les données au sein d'entreprises multinationales et de la sous-traitance des services. Cette directive a été transposée par tous les membres dans leur législation nationale.

Outre la directive 95/46/CE, d'autres réglementations sont apparues dans ce domaine. Les dispositions de la directive ont été examinées et complétées dans le domaine des communications électroniques dans la directive 2002/58/CE [92].

La Commission européenne a relancé une consultation publique en 2009 sur la question de la manière dont le cadre juridique nécessitait d'être adapté pour la protection des données à caractère personnel dans l'UE. Cette consultation, clôturée en décembre 2009, peut être consultée sur le site web de la Commission [65]. De l'avis général de ces consultations, la protection des données personnelles doit englober tous les domaines et tous les secteurs : privé et public. Elle doit garantir le droit à la protection à toute personne, sans aucune discrimination, dans la mesure de leur compétence. Les règles des entreprises contraignantes sont mentionnées comme un moyen d'assurer une protection adéquate.

« Le groupe de travail a déjà établi que les transferts internationaux de données à caractère personnel à partir de l'UE effectués entre filiales d'un même groupe peuvent avoir lieu sur la base des règles d'entreprise contraignantes. [93]» Les règles d'entreprises contraignantes décrivent la manière dont les personnes concernées sont informées du transfert et du traitement de leurs données personnelles.

- Toute personne a le droit d'obtenir une copie de toutes les données traitées la concernant, sans contrainte, à des intervalles raisonnables, et sans délais ou frais excessifs,
- Toute personne concernée a le droit d'obtenir la rectification, l'effacement ou le verrouillage de données, notamment au motif que les données sont incomplètes ou inexactes,
- Toute personne concernée a le droit de s'opposer, sur simple demande et sans frais.

2.2 Cadre législatif international relatif à la protection de la vie privée

Le cadre législatif concernant les données à caractère personnel est conséquent :

- Charte des droits fondamentaux de l'Union européenne : articles 7 et 8
- Article 7, Respect de la vie privée et familiale

Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications.

Article 8, Protection des données à caractère personnel :

✓ Toute personne a droit à la protection des données à caractère personnel la concernant.

✓ Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi [24].

- Directive 95/46/ CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. [91]
- Directive 2002/58/CE du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques [92]
- Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE. Cette directive concerne les droits des utilisateurs au regard des réseaux et services de communications électroniques.
- RECOMMANDATION N° R (87) 15 : la présente recommandation s'applique à la collecte, à l'enregistrement des données à caractère personnel, à l'utilisation et à la communication à des

fins de police. Chaque Etat membre devrait disposer d'une autorité de contrôle indépendante de la police, chargée de veiller aux principes énoncés de cette recommandation.

La collecte de données à caractère personnel à des fins de police devrait se limiter à ce qui est nécessaire à la prévention d'un danger concret ou à la répression d'une infraction pénale déterminée. Toute exception à cette disposition devrait faire l'objet d'une législation nationale spécifique [71]. Dans la mesure du possible, l'enregistrement de données à caractère personnel à des fins de police ne devrait concerner que des données exactes et se limiter aux données nécessaires pour permettre aux organes de police d'accomplir leurs tâches légales dans le cadre du droit interne et des obligations découlant du droit international. La personne concernée devrait pouvoir obtenir l'accès à un fichier de police à des intervalles raisonnables et sans délais excessifs conformément aux modalités prévues par le droit interne.

- **Convention 108** pour la protection des personnes à l'égard du traitement automatisé des données. Cette convention lutte contre l'usage abusif du traitement automatisé des données à caractère personnel.

- **La 30ème Conférence Internationale** des Commissaires à la Protection des Données et de la Vie Privée a adopté une Résolution sur l'urgence de protéger la vie privée dans un monde sans frontière. La résolution donnait mandat à l'Autorité Espagnole de Protection des Données, en tant qu'hôte de la 31ème Conférence internationale, pour créer un groupe de travail afin de rédiger une Proposition Conjointe pour l'établissement de Normes Internationales sur la Vie Privée et la Protection des Données Personnelles. [71]

- **OCDE, L'Organisation de coopération et de développement économiques,** affirme que le traitement automatique et les flux transfrontières de données à caractère personnel créent de nouvelles formes de relations entre les pays et exige l'instauration de règles et pratiques compatibles. Toute personne physique devrait avoir le droit :

    - ✓ d'obtenir du maître d'un fichier, ou par d'autres voies, confirmation du fait que le maître du fichier détient ou non des données la concernant [154]

    - ✓ Les pays membres devraient prendre en considération les conséquences pour d'autres pays membres d'un traitement effectué.

- L'ONU participe dès le début au mouvement de défense de droit de l'homme.

« Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes [156]».

2.3 La CNIL et ses missions dans la protection des données à caractère personnel

Par la loi du 6 janvier 1978 « Informatique et Liberté », en France a été créée la Commission Nationale de l'informatique et des libertés ou CNIL. La commission a pour mission de veiller à ce que « l'informatique ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».

La CNIL remplit les fonctions de conseil ainsi que de contrôle et de sanction. Elle collabore avec ses homologues européens et internationaux. Les membres de la CNIL se réunissent en séances plénières une fois par semaine. Une partie des séances est consacrée à l'examen de projet de loi soumis à la CNIL par le gouvernement. Les 17 membres de CNIL sont élus soit par l'assemblée soit par les juridictions auxquelles ils appartiennent. La CNIL compte 199 agents recrutés par le président de l'organisation, son budget relève du budget de l'État et ses décisions peuvent faire l'objet de recours de la juridiction.

Une des missions de la CNIL est de contrôler et d'informer. L'organisation peut accéder à tous les locaux professionnels, demander tout document nécessaire et d'en prendre copie, accéder aux programmes informatiques et aux données. Elle répond aux demandes des particuliers ainsi que des professionnels. La CNIL participe à divers colloques et conférences et fédère un collectif d'organismes qui mènent des actions en faveur de l'éducation au Numérique. D'après un sondage effectué en 2015, 68% des personnes connaissent l'organisation. En 2021, plus de 9 677 000 personnes visitent son site [44]. Ces chiffres montrent l'intérêt et l'inquiétude des citoyens envers l'abus de la vie privée.

La CNIL **protège les droits des citoyens.** Toute personne peut s'adresser à la CNIL. Toute personne peut prendre connaissance de l'intégralité des données la concernant. Elle exerce pour les citoyens qui le souhaitent l'accès aux fichiers intéressant la sûreté de l'Etat, la défense, la sécurité. La CNIL possède un système de recueil de plaintes en ligne concernant les problèmes d'internet, carte bancaires, commerce… La CNIL propose au gouvernement des mesures législatives ou réglementaires sur la protection de la vie privée. Le gouvernement consulte la CNIL avant de transmettre au Parlement tout projet de la loi relatif à la protection des données.

Plusieurs institutions nationales sont construites sur un modèle collégial, tandis que certaines sont dirigées par un président, qui porte le titre de commissaire. Pour plus d'indépendance, dans certains différents pays, des membres sont nommés par une autorité différente. C'est le cas pour la CNIL française, dont les autorités de nomination sont les deux chambres du Parlement. Dans certains pays, les membres des autorités de protections des données sont nommés par le monarque (la reine, par ex.), sur proposition du ministre, ou par le président de la République sur proposition du premier ministre (Exemple : Pays-Bas et Hongrie).

En France, chaque chambre et leur président sont une autorité de nomination parmi d'autres. Dans les autres pays européens, le parlement joue parfois un rôle primordial tandis que dans certains pays, son rôle est totalement absent. L'interdiction d'une carrière politique en parallèle au mandat à la tête d'une autorité de PDP est incluse dans une interdiction générale. Comme défini, la fonction de président de la commission est incompatible avec toute activité professionnelle.

2.4 Conclusion

L'internet pose de nouvelles questions, surtout au sujet de la position des sites web, des moteurs de recherche, des réseaux sociaux et également pour des données au sein d'entreprises multinationales et la sous-traitance des services. Les données « révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé » ne doivent être traitées qu'avec les garanties appropriées. » La CNIL est l'institution chargée de veiller à ce que l'informatique ne porte atteinte ni aux droits de l'homme, ni à la vie privée.

CHAPITRE 3

Protection alternative des données

Avec la globalisation, le nombre de transferts de données hors de l'Europe ne cesse de croître. Le transfert de données hors de l'Union européenne n'est possible qu'à condition d'assurer un niveau de protection des données approprié.

3.1 Introduction

Plusieurs entreprises multinationales rencontraient des problèmes au niveau des mécanismes de la protection des données et, en 2003, après leur demande, le G29 officialise les *Binding Corporate Rules* (BCR). En 2012, il introduit les BCR sous-traitants, à distinguer des BCR reconnues en 2003 qui s'intitulent, depuis, BCR responsable du traitement. D'après ce code de conduite interne, les entreprises définissent la politique de transfert des données personnelles hors UE. Il peut être considéré comme une alternative aux Clauses Contractuelles et *Safe Harbor*. Ses avantages sont la prévention des risques issus de transferts et surtout la conformité avec les principes de la directive européenne 95/46/CE. En adoptant la BCR, l'entreprise désigne une autorité européenne de Protection des Données, par exemple la CNIL, qui sera en charge de coopérer avec ses homologues du pays de transfert des données.

Les étapes pour faire un recours auprès de la BCR sont les suivantes [41] :

1. Réclamation du projet de BCR;
2. Désignation d'une autorité de chef de file ;
3. Etudes de la BCR par cette autorité ;
4. Etudes de la BCR par deux autres autorités ;
5. Accusé/Réception de la BCR par les autorités ;
6. Envoi des BCR finalisées à toutes les autorités européennes de Protection des Données ;
7. Demande d'autorisation de transfert auprès de chacune des autorités européennes ;
8. Autorisation de Transfert par ces autorités ;

Les personnes dont les données sont transférées par des groupes ayant des BCR peuvent avoir un droit d'accès, de rectification, d'effacement et de verrouillage des Données. Les consommateurs peuvent bénéficier du droit de Restrictions en cas de transfert ultérieurs en dehors du groupe et d'avoir un niveau élevé de sécurité de confidentialité.

Pour les pays hors de l'UE, le transfert de données personnelles peut avoir lieu si un « niveau de protection adéquat » est assuré par le pays importateur des données. A ce jour, peu de pays ont été reconnus assurant un « niveau de protection adéquat » par l'UE. Des dérogations ont été prévues dans la directive, qui autorise le transfert des données sans « protection adéquate ». Il s'agit de cas où les risques pour les personnes concernées sont faibles. Le G29 a précisé que ces dérogations devaient être appliquées de manière restrictive [96].

Le G29 précise que l'exécution d'un contrat entre la personne concernée et le responsable du traitement ne peut être invoquée comme dérogation que si le transfert est nécessaire à la finalité de l'exécution du contrat (Dérogation b) ou c) point 1 de l'article 26 de la directive, en annexe 1) [96]. Les BCR ne sont pas clairement mentionnées dans la directive européenne, mais la loi française mentionne des règles internes [136].

En France, la transposition de la directive a été tardive. L'Assemblée Nationale a validé cette loi en la qualifiant d'« indéniable mesure de souplesse pour les entreprises tout en garantissant le respect des droits et libertés fondamentales. »

Fig. 1 : *Liste des compagnies ayant déjà adopté les règles de la BCR, sous l'autorité de la CNIL [67]*

Nom Des Entreprises	**Autorité**
Airbus (Controller)	CNIL/FR
Atos (Controller and Processor)	CNIL/FR
AXA	CNIL/FR
Axa Private Equity	CNIL/FR
Bristol Myers Squibb	CNIL/FR
CMA-CGM	CNIL/FR
Corning (Controller)	CNIL/FR
ENGIE (ex GDF SUEZ; Controller)	CNIL/FR
General Electric (GE)	CNIL/FR
Hermès	CNIL/FR
HP Enterprise (Controller)	CNIL/FR
HP Inc. (ex Hewlett Packard; Controller)	CNIL/FR
International SOS	CNIL/FR
Legrand (Controller)	CNIL/FR
Linkbynet (Controller and Processor)	CNIL/FR
LVMH	CNIL/FR

Michelin	CNIL/FR
NOVARTIS	CNIL/FR
OVH	CNIL/FR
Safran	CNIL/FR
Salesforce (Processor)	CNIL/FR
Sanofi Aventis	CNIL/FR
Schneider Electric	CNIL/FR
Société Générale	CNIL/FR
Sopra HR Software (ex HR Access; Controller and Processor)	CNIL/FR
Total	CNIL/FR

Chaque entreprise a le choix et le droit de faire des BCR. Elle peut définir une « éthique interne » et leur champ d'application sur toutes les filiales du groupe au-delà des frontières de l'Europe.

Cette éthique est modifiée en fonction des populations, c'est-à-dire en interne pour les employés, et en externe pour les clients et les partenaires. Elle joue un rôle positif pour renforcer la confiance entre employés, ses clients, ses partenaires et les autorités.

L'éthique de BCR est le moyen d'afficher l'engagement de l'entreprise pour son respect des lois dans toutes ses activités. Cet engagement est traduit par la mise en œuvre d'un programme de conformité pour la formation de l'ensemble de ses employés et de contrôle de l'application des règles. Dans l'entreprise, les BCR permettent de respecter la loi sur la protection des données personnelles sous plusieurs aspects, elles sont considérées comme étant un standard assez élevé.

En 2014, le Parlement européen a supprimé la référence à la notion de BCR sous-traitant (*BCR for processor*). Jusqu'à nos jours, plusieurs entreprises ont adopté des BCR sous-traitant pour assurer ses garanties apportées par ce mécanisme et, pour sa part, le G29 a adressé un courrier au président du Parlement européen concernant cet événement [68].

3.2 *Safe Harbor* et *privacy Shield*

Selon la Déclaration de 2000, la Commission Européenne affirmait que l'adhésion aux normes *Safe Harbor* garantit un niveau de protection adéquat pour le transfert des données d'un pays de l'UE vers les entreprises situées aux États-Unis.

En 2015, la Cour de Justice de l'UE (CJUE) a invalidé l'accord de la sphère de sécurité / *Safe Harbor* qui a été jugé illégal. La CJUE a relevé que les autorités publiques américaines peuvent accéder de manière massive aux données, sans assurer de protection juridique aux personnes concernées.

Le scandale des écoutes de la NSA américaine relevé par Edward Snowden a marqué les esprits. Une analyse de Lexis a déchiffré l'ampleur des mécanismes de collecte de renseignement américain qui emploie environ 40 000 employés [103].

Après cette décision, il a été convenu que « Les personnes dont les données sont transmises aux États-Unis doivent être informées de manière claire et aussi exhaustive que possible des accès possibles des autorités, afin de leur permettre d'exercer leurs droits. Le contrat d'échange de données personnelles devrait prévoir un engagement des parties contractantes dans ce sens [72]. »

Après ce scandale, un vice-président de la Commission Européenne a déclaré que l'Europe et les États-Unis ont besoin d'un nouvel accord de type *Safe Harbor* en 2016. Les fonctionnaires américains et européens ont commencé les négociations pour remplacer la sphère de sécurité / *Safe Harbor* jugée illégale.

Ainsi, plus de 4 000 entreprises américaines qui adhèrent volontairement au *Safe Harbor* et les entreprises européennes qui leur transmettent des données étaient dans l'expectative.

D'après le verdict de la Cour, les entreprises européennes **peuvent transférer des données vers les États-Unis en utilisant les autres moyens, tels que des clauses contractuelles ou des règles des entreprises contraignantes**. Surtout le recours soulignait que les entreprises pouvaient transférer les données vers les États-Unis si elles possèdent le consentement du consommateur pour le transfert des données.

La CJUE a invalidé la décision d'adéquation « *Privacy Shield* », adoptée en 2016 par la Commission européenne suite à l'invalidation du « *Safe Harbor* », qui permettait le transfert de données entre l'Union européenne et les opérateurs américains. La CJUE a également validé les clauses contractuelles types permettant le transfert de données depuis l'Union européenne vers des importateurs établis hors de l'Union.

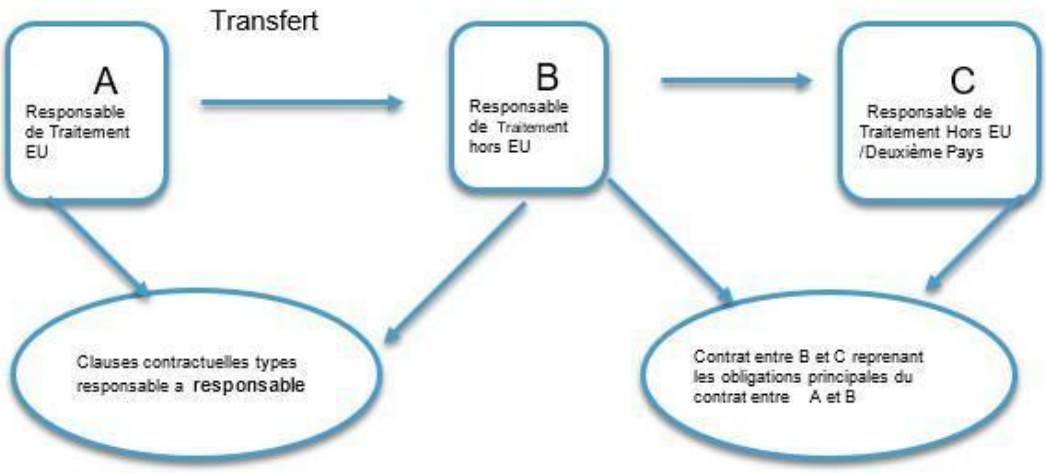
3.3 Clauses Contractuelles Types

Les Clauses Contractuelles étaient adoptées par la Commission Européenne pour encadrer les transferts de données personnelles hors de l'Union Européenne. Il existe deux types de clauses :

- Clauses contractuelles encadrant les transferts de données personnelles d'un responsable de traitement à un autre responsable de traitement
- Clauses contractuelles encadrant les transferts de données personnelles d'un responsable de traitement à un sous-traitant

Si on transfère les données personnelles par un responsable de traitement de l'EU vers un autre responsable de traitement située hors EU, qui transfère à son tour ces données à un autre responsable de traitement hors EU, on obtient le schéma suivant :

Fig. 2 : *Transfert des données personnelles par un responsable de traitement de l'EU vers un autre responsable de traitement située hors EU, qui transfère à son tour ces données à un autre responsable de traitement hors EU, CNIL*



Indices	Le prestataire pourra être qualifié de sous-traitant	Le prestataire pourra être qualifié de responsable de traitement
Niveau d'instruction : Le niveau d'instruction donné par le client indique le degré d'autonomie laissé au prestataire. Par conséquent il permet d'apprécier s'il est plus qu'un simple sous-traitant.	Le contrat de prestation et les directives données au cours de son exécution sont très précis dans les instructions et le niveau de qualité demandé.	Le contrat de prestation et les directives données au cours de son exécution sont très généraux en termes d'instruction et laissent expressément une grande autonomie au prestataire.
Niveau de contrôle : Le degré de contrôle du client sur les prestations et sur les données révèle également la liberté dont peut disposer le prestataire.	La société audite son prestataire et lui demande des comptes régulièrement.	La société laisse le prestataire réaliser ses prestations et le laisse libre d'utiliser les données comme bon lui semble.
Transparence : Le prestataire de service se présente-t-il sous son nom propre ou sous le nom de son client et peut-il les réutiliser pour des fins qui lui sont propres?	L'employé du centre d'appel en Tunisie se présente sous le nom du client et ne réutilise pas les données pour son propre compte.	Le centre d'appel en Tunisie se présente sous son propre nom et réutilise les données à des fins qui lui sont propres.
Expertise : Un prestataire qui dispose d'une expertise peut ainsi décider des moyens à mettre en place dans le cadre de la réalisation des prestations.	Le prestataire utilise l'infrastructure technique du client pour réaliser sa prestation.	Le prestataire expert dans son domaine impose des outils au client qui n'a pas de pouvoir de négociation, ne peut les modifier parce qu'il n'a pas les compétences, ou parce que l'outil est un outil qui ne fait pas l'objet d'un développement spécifiques.

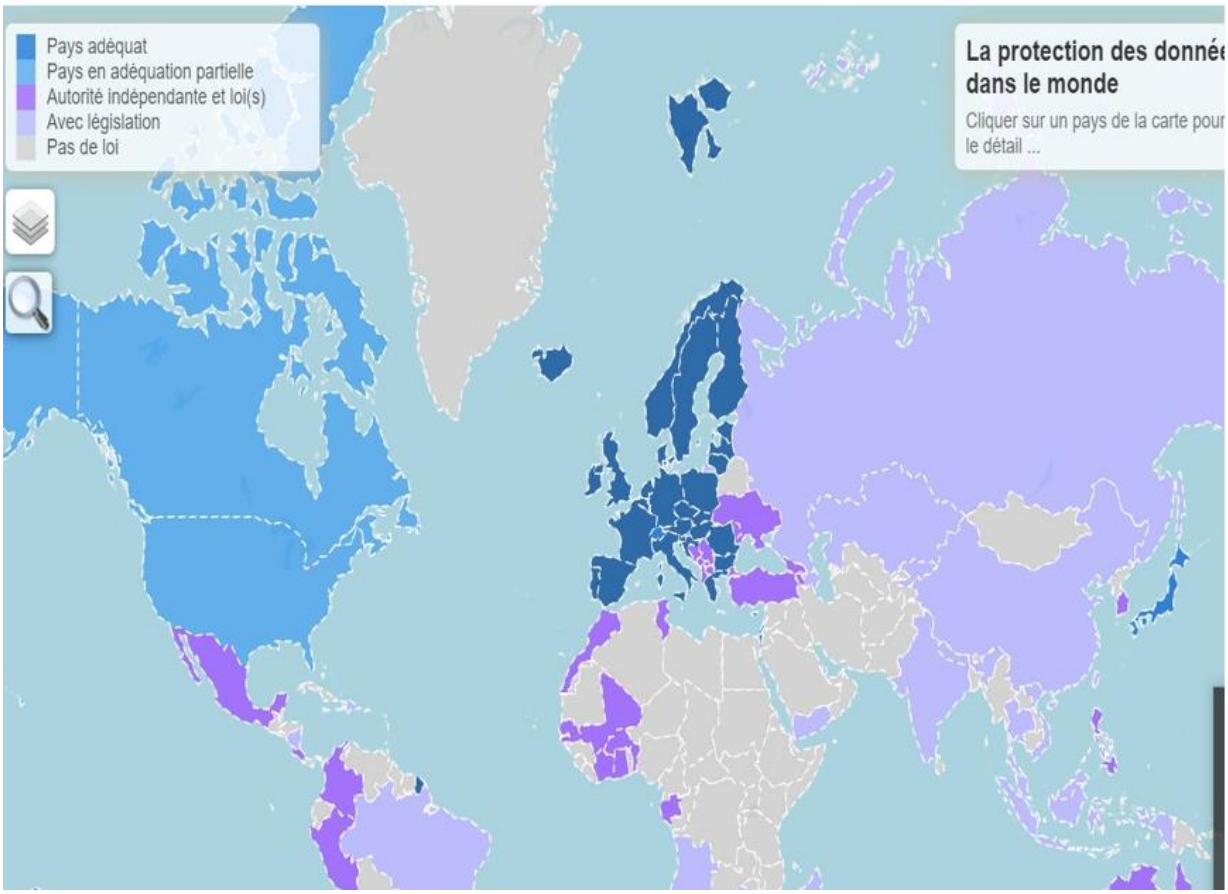
Fig. 3 : Prestataire qualifié, sous-traitant et responsable de traitement, CNIL [46]

Les modèles des contrats sont disponibles sur le site de la CNIL.

3.4 Conclusion

Avec l'utilisation des nouvelles technologies, le transfert de données hors de l'Union européenne doit être assuré avec les normes appropriées. Ces transferts doivent être réalisés en utilisant différents outils juridiques. Récemment, la CJUE a invalidé la décision d'adéquation « *Privacy Shield* », adoptée en 2016 par la Commission européenne suite à l'invalidation du « *Safe Harbor* », qui permettait le transfert de données entre l'Union européenne et les opérateurs américains. Les Clauses Contractuelles Types (CCT) peuvent toujours être utilisées pour transférer des données vers un pays tiers (qu'il s'agisse des États-Unis ou d'un autre pays tiers). Les règles d'entreprise contraignantes (BCR) restent toujours un outil d'encadrement des transferts de données personnelles hors de l'Union européenne intra-groupe. Elles sont applicables à toutes les entités d'un groupe qui adhèrent à ce dispositif.

Fig. 4 : *Carte de la CNIL pour évaluation de niveau de la protection des données au monde, CNIL [43]*



CHAPITRE 4

Aspect économique et social

Dans ce chapitre, on analyse les moyens avec lesquels plusieurs sites internet captent les informations sur les usagers. Selon les recherches d'IDC, société spécialisée dans l'analyse des informations sur Internet, la quantité de données en circulation croît de 50 % chaque année. Les économistes constatent que les entreprises prenant des décisions en fonction de l'analyse de données atteignent une productivité de 5 à 6 % de plus que les autres. Ils assurent que des requêtes Google ont la capacité de savoir plus de choses que l'Insee sur la France**.**

4.1 Introduction

Pour le secteur économique, les nouvelles technologies et la communication sont devenues de vrais enjeux. Les données personnelles sont devenues une clé importante pour pénétrer les nouveaux marchés et plusieurs firmes sont spécialisées dans leurs collectes et leurs ventes. A l'aide des profils des clients, les services marketing facilitent leurs affaires pour prévoir les comportements des clients et vaincre les concurrents.

Après la création de l'UE, la circulation des personnes, des marchandises, des différents services publics ou privés et des capitaux apparaissait évidente. Pour la circulation des personnes, les données personnelles se transfèrent d'un État à un autre soit par les douanes, soit par les services où la personne concernée voyage ou travaille. Si les travailleurs dans l'industrie de l'information s'établissent dans un autre pays de la Communauté, les données sont transférées conformément à l'article 43 de CE [126].

Dès l'établissement d'un travailleur dans un autre pays de la communauté, le transfert des données concernant par exemple des clients peut se faire. C'est le marché intérieur et la législation nationale qui précisent s'il y a empêchement de la libre circulation des données personnelles. La libre circulation des marchandises, les paiements et les données sont de plus en plus fréquents parmi les pays et la protection des données personnelles de plus en plus remise en question.

D'après le Professeur Jean Frayssinet, la libre circulation des données personnelles dans le cadre du marché unique assimile les données personnelles à des biens immatériels susceptibles d'appropriations [143 ; 48-56].

On peut considérer que la notion de marchandise englobe toutes sortes de biens et données personnelles qui peuvent être appréhendées comme des biens immatériels.

D'après les recherches de l'IDC, société spécialisée dans l'analyse des informations sur Internet, la quantité de données en circulation croît de 50 % chaque année. Et il ne s'agit pas seulement d'informations toujours très importantes, mais de flux entièrement nouveaux n'ayant pas de grande valeur. A notre époque, il existe un grand nombre de capteurs numériques installés sur les équipements industriels, les compteurs électriques et les automobiles. Ces capteurs peuvent mesurer et transmettre des informations sur la localisation, les mouvements, la température, l'humidité et même les composants chimiques de l'air. En reliant ces informations à des ordinateurs, on reçoit « l'Internet industriel ». C'est également parce qu'il est plus facile d'accéder à l'information que la tendance au déferlement de données se poursuit.

En 2017, l'IDC estimait que « le marché des technologies et des services *Big Data* augmentera à un taux de croissance annuel composé de 26,4% pour atteindre 41,5 milliards de dollars jusqu'en 2018, soit environ six fois le taux de croissance du marché global des technologies de l'information [118] ». Pour l'année 2021, les investissements mondiaux des entreprises dans le traitement et analyse de méga données devraient croître de plus 10% à 215,7 milliards de dollars, pensent les chercheurs de l'IDC [10].

Les entreprises de grande distribution analysent les ventes, les prix, même les conditions de la météo ainsi que des données démographiques pour adapter au mieux les sélections de produits selon les magasins et déterminer les prix et des périodes de promotion.

Les réseaux sociaux, surtout les sites de rencontres en ligne, analysent les listes de caractéristiques personnelles, les réactions et les commentaires, pour attirer un grand nombre de clientèle. Aux États-Unis, les services de police analysent les historiques des arrestations, les jours de paie, les précipitations et les jours fériés pour tenter de prédire les crimes et envoyer des agents dans ces zones.

Le traitement des données en général, y compris des données personnelles, permet la maîtrise de certains marchés qui font déjà transiter plusieurs informations dans certains domaines par les outils électroniques différents.

Les formations en ligne, qui connaissent une croissance rapide dans plusieurs pays gagnant ainsi un intérêt économique, finiront par révolutionner l'enseignement et permettront une maîtrise des ressources humaines, mais feront face à la question de la protection des données.

En général, un consommateur visite des sites Internet sans avoir envie de fournir ses données personnelles mais pour accéder à certaines parties des sites Internet, or l'administration du site peut demander des données personnelles. La communication de ces données est volontaire, mais si le consommateur ne fournit pas ces données, il ne pourra pas bénéficier des services proposés par les sites : il en est ainsi de la communication, du téléchargement de documents ou du recrutement.

Souvent les sites mentionnent les raisons pour lesquelles les données personnelles sont collectées. On peut en décrire quelques-unes : publicité ciblée, satisfaction des clients, perfectionnement des produits.

4.2 La publicité comportementale et la protection des données

Les démarches promotionnelles effectuées sont l'aspect le plus attractif pour les clients. L'administration promet aux consommateurs de leur donner les informations spécifiques qu'ils demandent en ligne et de leur envoyer des offres et coupons promotionnels. De plus, le consommateur pense participer à des jeux, des concours en ligne ou à des événements sponsorisés. En collectant ces données, presque tous les sites assurent les consommateurs qu'ils offrent des choix appropriés à l'utilisation de leurs données et de leurs protections. On peut constater que la « loi informatique et libertés » est inefficace pour protéger les individus des publicités ciblées sur internet. La publicité comportementale consiste à suivre les

utilisateurs sur internet et à constituer des profils, qui serviront ultérieurement à leur proposer des publicités correspondant à leurs centres d'intérêt. Elle vise à étudier les caractéristiques de ce comportement à travers leurs actions (visites successives de sites, interactions, mots clés, production de contenu en ligne, etc.). [111 ; 15-21]

Le G29 constatait que la publicité comportementale s'appuie sur les acteurs suivants :

- Fournisseurs de réseaux publicitaires, ils mettent en relation les diffuseurs et les annonceurs ;
- Annonceurs qui veulent promouvoir un produit ou un service auprès d'un public spécifique ;
- Diffuseurs qui sont les propriétaires des sites web et cherchent à tirer des revenus ;

Il existe deux méthodes pour établir des profils d'utilisateurs :

✓ Profils prédictifs qui sont établis par observation du comportement des utilisateurs dans le temps ;

✓ Profils explicites qui sont établis à partir des données à caractère personnel que les personnes concernées fournissent à un service web ;

la directive 2002/58/CE17, article 5 paragraphe 1 [92] protège la confidentialité des communications en général. Dans cet article, paragraphe 3, sont aussi prévus l'utilisation de cookies et la protection de la confidentialité des communications.[92]

4.3 Forums

Un deuxième aspect pour attirer le client se trouve dans les forums de discussion. Si le client choisit de participer à des forums, il pourra lui être demandé de fournir des renseignements personnels tels que le nom et l'adresse électronique, le numéro téléphone.

Dans ce cas, les clients sont informés que leurs commentaires pourront être largement accessibles à d'autres, à l'intérieur du forum ou à l'extérieur, selon le forum ou le groupe.

Presque tous les sites des entreprises utilisent les données personnelles pour conduire des études de satisfaction clients, en promettant d'améliorer les sites Internet et les services. Avec l'entrée en application du Règlement Général sur la Protection des Données (RGPD) en 2018, il est nécessaire de réaliser enquêtes et sondages **en toute conformité avec les nouveaux standards** :

- La personne concernée doit donner son consentement lors de la collecte de données à caractère personnel ;
- L'entreprise doit clairement expliquer la finalité du traitement aux personnes concernées, ainsi que leur durée de conservation ;
- La personne concernée peut à tout moment demander à accéder à ses données, à les faire rectifier ou effacer, demander leur portabilité, en contester les traitements ;
- L'entreprise doit garantir la confidentialité et la sécurité des données ;
- L'entreprise doit démontrer que toutes les mesures techniques ont été prises pour assurer la conformité avec la réglementation.

Le nouveau règlement, article 22, [164] consacre le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé. Par exemple, faire le profilage pour objet :

- En matière de crédit ou d'assurance ;
- De la santé ;
- Dans le cadre d'un site de recrutement ;
- Dans la modulation du tarif en fonction du profil de l'internaute ;

En pratique, ces dispositions ont ambition à éviter que les responsables de traitement ne procèdent pas au profilage de la situation de l'intéressé.

4.4 Cookies

Plusieurs sites informent sur les cookies qu'ils envoient. En utilisant les sites Internet, le client accepte que des cookies soient placés sur leur ordinateur. Ces petits fichiers de données envoyés au navigateur Internet ont pour mission de faciliter la navigation sur le site internet. Ils peuvent ensuite être stockés sur les ordinateurs des clients pour identifier leurs ordinateurs.

Les cookies peuvent être de longue ou courte durée : automatiquement supprimé lorsque l'utilisateur ferme le navigateur, ou stocké dans l'ordinateur de l'utilisateur jusqu'à sa date d'expiration. Ces périodes peuvent durer des mois. Un cookie fonctionnel pourrait montrer la zone géographique dans laquelle se trouve le consommateur et lui fournir les informations locales.

Le G29 estimait que la publicité comportementale implique le traitement de données à caractère personnel au sens de l'article 2 de la directive 95/46/CE. Le même avis existe sur la collecte d'adresses IP et le traitement d'identifiants uniques par les cookies. D'après le G29, ces dispositifs permettent d'identifier la personne et, à l'inverse, la personne est identifiable par un cookie.

Le G29 considère que « les témoins de connexion ou «cookies» sont fournis par le moteur de recherche et stockés sur l'ordinateur de l'utilisateur. Le contenu des «cookies» varie d'un fournisseur de moteur de recherche à l'autre. Les « cookies » attribués par les moteurs de recherche contiennent généralement des informations relatives au système d'exploitation et au navigateur de l'utilisateur, ainsi qu'un numéro d'identification unique pour chaque compte d'utilisateur. Ils permettent d'identifier l'utilisateur plus précisément que l'adresse IP [112]. Conformément à l'article 5, un fournisseur de réseau publicitaire qui souhaite stocker des informations dans l'équipement terminal d'un utilisateur peut le faire dans les conditions suivantes :

- ✓ S'il a fourni à l'utilisateur une information complète sur les finalités du traitement
- ✓ S'il a obtenu l'accord de l'utilisateur pour stocker des informations sur son équipement terminal

La directive dite « paquet Telecom » renforce la protection des données personnelles par un Opt-in dans le cas spécifique de l'utilisation de cookies par les opérateurs de la publicité ciblée en ligne. La CNIL considère que l'utilisateur est actif dans son consentement, et les cases pré-cochées contreviennent au régime de l'Opt-in défini par la LCEN [131].

Les représentants des réseaux publicitaires proposent souvent l'option d'«opt-out» permettant aux utilisateurs de refuser des publicités ciblées. Pour activer ce mécanisme, on doit se rendre sur le site web du fournisseur publicitaire et préciser qu'on ne veut pas être tracé. L'Opt-out n'exprime pas un

consentement des personnes concernées. Ce mécanisme ne convient pas pour obtenir un consentement informé de l'utilisateur moyen.

Le G29 considère que le consentement doit être prononcé librement et constituer une manifestation claire. L'acceptation d'un cookie par une personne concernée pourrait être comprise /interprétée comme pour l'envoi du cookie et pour la collecte de données provenant de ce cookie. Cette pratique montre que les personnes qui acceptent d'être suivies parfois l'oublient et sont suivies « une fois pour toutes. »

Le groupe de travail G29 pensait que certaines mesures devraient être mises en place, par ex. :

- Limiter le consentement dans le temps et les fournisseurs de réseaux publicitaires devraient faire l'objet d'un nouveau consentement
- Les personnes concernées devraient avoir la possibilité de révoquer leur consentement à être suivies.

Ce consentement est plus sensibles en ce qui concerne les enfants [114 ; 6-12]. Le groupe de travail avait étudié la question de la protection des données à caractère personnel des enfants. Dans ce cas, les représentants de réseaux publicitaires devront informer les parents de la collecte et de l'utilisation d'informations concernant leurs enfants et obtenir leur consentement avant de collecter.

Nul enfant ne fera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation [75].

Les cookies de ciblage sont utilisés pour des campagnes publicitaires ciblées. Ils sont généralement placés sur un site Internet par des agences publicitaires, avec l'accord de l'exploitant du site. Ces cookies sont ensuite partagés avec des tiers (telles des régies publicitaires). Mais il faut souligner qu'une grande partie des clients ne se rendent pas compte des résultats de transfert de ces données, malgré les informations proposées par les sites.

Le président de la CNIL avait raison pour s'inquiéter « lorsqu'on visite quatre sites grand public, des sociétés que nous ne connaissons pas installent une cinquantaine de cookies sur notre ordinateur. Google, Facebook, Amazon et les autres géants du Net collectent, regroupent et monétisent les données personnelles de façon non transparente."[168]

Parfois les consommateurs ont le sentiment qu'ils ne peuvent pas contrôler l'utilisation et la diffusion de leurs données qui se traduisent par un déficit de partage. Ceci correspond à l'écart entre les types de données communiquées volontairement et les types de données collectées sans leur consentement.

4.5 Conclusion

Les pays européens ainsi que la France doivent jouer un rôle plus dynamique pour améliorer le potentiel économique et sociale et informer les utilisateurs des différentes sites et réseaux de leurs droits et obligations. Aujourd'hui, les GAFA (Google, Apple, Facebook, Amazon) qui captent hors de l'Europe la valeur économique des données des citoyens européens mettent leurs informations et leur vie privée à disposition d'autrui. Si nous devions graver toutes les informations numériques créées en 2018 sur des disques Blu-ray, nous aurions besoin d'une quantité énorme : soit 660 milliards sur une capacité individuelle de 50 Go [104]. La valeur des données personnelles des internautes européens est estimée à 8% du PIB européen pour 2020, selon le World Economic Forum. Au niveau global, 162 milliards d'euros (en 2017) représentés par la publicité numérique sont directement liée aux données, selon le cabinet PwC [3].

CHAPITRE 5

Protection des données, réseaux sociaux et moteurs de recherches

Dans ce chapitre nous étudions l'influence des réseaux sociaux et des moteurs de recherche sur les usagers. La pratique du traitement et de la commercialisation des données des utilisateurs de réseaux sociaux se développe. Toutes les informations qu'il est possible d'avoir sur un individu sont récupérées. Facebook, par exemple, stocke l'ensemble de nos données sur des serveurs. Le droit à l'oubli numérique répond au souci des internautes de contrôler leur réputation en ligne, qui se double de préoccupations autour de la protection des données personnelles.

5.1 Introduction

Au mois de janvier 2014, la CNIL avait adopté une sanction pécuniaire de 150 000 euros contre la société Google dont la politique de confidentialité n'était pas conforme au droit français. Les utilisateurs n'étaient pas assez informés des conditions de traitements automatisée de leurs données par les réseaux sociaux. En 2019, l'Autorité de la concurrence a infligé 150 millions d'euros d'amende à Google pour abus de position dominante sur le marché de la publicité.

En général, pour les États-Unis, les données personnelles sont des produits de type marketing. Leur utilisation en tant que marchandise est assez fréquente. Parfois les entreprises américaines ont un faible niveau de protection et les utilisent souvent sans grande prudence. Pourtant, certains services de sécurité estiment qu'une surveillance accrue est souvent nécessaire pour mener à bien la lutte contre le terrorisme. Mais il existe plusieurs cas quand les données personnelles sont vendues par des réseaux sociaux à des entreprises pour ciblage de publicité.

D'après les recherches, les économistes constatent que les entreprises prenant des décisions en fonction de l'analyse de données atteignent une productivité de 5 à 6 % plus élevées que les autres. Ils nous assurent que des requêtes Google ont la capacité de savoir plus de choses que l'Insee sur la France.

On peut distinguer l'identité personnelle de l'identité numérique, même si l'identité numérique n'est pas reconnue juridiquement. A ce sujet, nous soulevons une autre question. Quand on crée une personne sur des réseaux sociaux, comment peut-on parler de ses droits et de son identité personnelle ? Autre question intéressante : le "mur" d'un individu a-t-il un caractère privé ou public ? Plusieurs cas étudiés à la Cour portaient sur des injures proférées par des salariés contre leur patron. Il n'existe pas de notion claire pour définir le caractère des murs des réseaux, mais d'après les cas de la Cour, le mur était considéré comme un lieu privé sous certaines conditions. Il fallait ainsi que les messages diffusés soit agréés par le titulaire du compte.

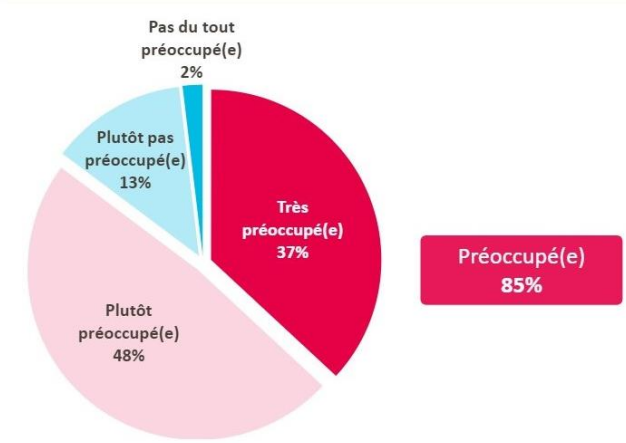
En France et en Europe, plusieurs personnes sont victimes d'usurpation de leur identité. D'après la définition du code pénal, l'usurpation de données est le fait de faire usage via des informations électroniques, de données d'un tiers qui lui sont personnelles, en vue de porter atteinte à son honneur et de troubler sa vie [63]. Donc l'action se déroule sans l'autorisation de l'utilisateur.

L'internaute incriminé pourrait être identifié grâce à son adresse IP, avant d'être assigné en justice pour avoir usurpé une identité. Plusieurs internautes se sont retrouvés assignés en référé sur le fondement de l'atteinte à la vie privée et au droit à l'image des autres, dont de "stars".

Pour le tribunal, le prénom, le nom et la date de naissance du demandeur « sont des éléments d'identité ne relevant pas de la vie privée. » En revanche, la révélation d'informations concernant les goûts, la publication de photographies de celui-ci sont des éléments majeurs pouvant relever d'une violation de la vie privée et de son droit à l'image.

D'après les recherches menées par le CSA pour Orange (fig. 5), 85% des Français se déclarent préoccupés par la protection de leurs données sur internet et 42% pensent que la situation s'est détériorée au cours des dernières années [123].

Fig. 5 : *Source CSA Consumer Science & Analytics [123]*



Etude de l'Institut CSA pour Orange, 2014 Fevrier

5.2 Réseaux sociaux, ciblage publicitaire, géolocalisation

Les réseaux sociaux offrent une possibilité de communication qui peut menacer la vie privée. Des données personnelles « images, vidéos, commentaires » deviennent publiquement disponibles et peuvent être examinés par plusieurs services.

Parfois il est difficile de soustraire des informations du web une fois qu'elles ont été publiées et ces données restent souvent accessibles via les moteurs de recherche. La pratique du traitement et de la commercialisation des données des utilisateurs de réseaux sociaux se développe. Toutes les informations qu'il est possible d'avoir sur un individu sont récupérées. Facebook, par exemple, stocke l'ensemble de nos données sur leurs serveurs. Plusieurs centaines téraoctets de données sont ainsi stockées chaque jour. Le pire, lors des élections présidentielles aux États-Unis de 2016, la société "Cambridge Analytica", dédiée au profilage des électeurs, s'est emparée des données de 50 millions d'Américains, sans leur consentement. Les données ont été +collectées grâce à une application inventée par un chercheur de l'université de Cambridge. 270 000 utilisateurs de Facebook ont été payés pour remplir un questionnaire de personnalité

et ont accepté que leurs données soient collectées pour un usage universitaire. Mais l'application a aussi récolté les données des amis Facebook de tous ces utilisateurs. Suite à la violation des droits de ces utilisateurs, le réseaux Facebook a été obligé de payer l'amende la plus importante jamais infligée (5 milliards de dollars) [116].

Il est incontestable que de nouveaux droits soient créés pour couvrir les nouveaux besoins. Il s'agit de donner à toute personne le pouvoir de décider la mesure dans laquelle les informations la concernant peuvent être traitées, communiquées, et conservées. Sur les réseaux sociaux, ce droit permettrait à tout utilisateur de pouvoir supprimer toutes les informations le concernant, le droit à l'oubli numérique est une revendication nouvelle car l'information sur le net est difficile à faire disparaître.

Aujourd'hui, plusieurs d'entreprises stockent, traitent et vendent nos informations. Ces entreprises en ont fait un business et les données personnelles sont devenues des marchandises opérant sur le marché et échangent entre elles. Le traitement et la classification des données devient un outil performant de plus en plus utilisé. Parfois certains individus pourraient être sujets d'une surveillance particulière. Les opérateurs de réseaux sociaux dressent des personnalités en fonction de leurs goûts, habitudes, loisirs. Les technologies gèrent des données analysées et tracent les différentes activités des internautes afin d'orienter leurs choix.

Suivant les goûts et les domaines d'intérêt des abonnés des réseaux sociaux, les annonceurs peuvent orienter davantage leurs publicités pour les consommateurs. Toutes les informations relatives aux membres des réseaux sociaux permettent de proposer de la publicité personnalisée, c'est-à-dire ciblée.

Les réseaux sociaux ayant une origine non européenne, pour la plupart, étaient soumis aux principes du *Safe Harbor* ou Sphère de sécurité. Les réseaux sociaux ont l'obligation de souligner, dans leur contrat, les différents droits inscrits à leurs services. Les réseaux ont l'obligation de la détermination du propriétaire des données. Cette notion de propriété va conditionner des droits accordés aux utilisateurs. On constate que le pouvoir de la CNIL n'est pas suffisant pour faire reculer les géants des réseaux.

Le réseau social Instagram a évoqué le désir de vendre les photos publiées par les utilisateurs, ce qui a provoqué une réaction négative des internautes. En conséquence, Instagram a été obligé de renoncer à la vente prévue. **En général, quand un réseau social souhaite mettre en place une nouvelle pratique, il doit le marquer de manière explicite dans le contrat.** 62% des internautes qui publient des photos pensent contrôler les paramètres de visibilité et 66% disent restreindre l'accès à leurs photos pour certaines personnes. Seuls 31% déclarent bien connaître ces paramètres. 38% seulement déclarent savoir exactement qui a accès aux photos ou vidéos publiées d'eux sur Internet. 60% pensent que les paramètres ne leur procurent pas le niveau de confidentialité souhaitée [184].

D'autre part, la publicité ciblée est réalisée par l'exploitation des données collectées, la localisation ou l'identification des internautes, ainsi elle peut toucher la protection de leur vie privée.

D'après la décision de la CNIL, l'utilisation de dispositifs de géolocalisation est un point très sensible au regard de la protection de la vie privée. Ces dispositifs doivent présenter des garanties en matière de contrôle et de protection des données [32].

La géolocalisation n'est pas qu'un moyen de se localiser, c'est aussi une façon de dévoiler des activités qui entraînent des conversations autour du lieu. Il sera très facile d'en déduire des événements et habitudes de vie. Par la suite, nos données risquent d'être traitées pour une utilisation commerciale.

Ainsi, sur les réseaux sociaux, le client peut recevoir une notification Facebook sur son téléphone l'informant qu'un de ses amis se trouve à proximité. Et vice-versa. Cette nouvelle option, appelée « amis à proximité » a été lancée par le réseau social sur son application mobile en 2015. Cette fonctionnalité doit être activée par l'utilisateur afin que ses amis savent s'il est à proximité.

Plusieurs clients mentionnent non seulement leur identité mais également leurs convictions, leurs modes de vie sur les réseaux sociaux et l'utilisation de ces données sans le consentement des utilisateurs constitue une atteinte à la vie privée.

C'est la raison pour laquelle une grande partie des internautes dit vouloir refuser la géolocalisation, puisque les services ayant recours à cette technique utilisent les données de localisation afin de les réutiliser.

Dans le même temps, aux États-Unis, Apple a commencé à commercialiser iBeacon, un service permettant de géolocaliser de manière anonyme les clients présents dans un magasin avec les smartphones, via Bluetooth. De ce fait, les commerçants peuvent analyser le comportement de leurs clients au sein des rayons. Pour cette nouveauté, la CNIL rappelle que « les images ne doivent pas être enregistrées, ni transmises à des tiers, ni même visibles par les prestataires qui proposent ces dispositifs à la vente ou à la location. [2]»

L'installation de ce type de produit est soumise à une autorisation délivrée par la CNIL. De plus, les commerçants souhaitant utiliser ce type de services devront prévenir leurs clients via un affichage au sein du magasin et devront obtenir l'accord exprès des clients.

Dès que l'exploitation de géolocalisation commence, le traitement de données à caractère personnel et ce service doivent être soumis à la réglementation sur la protection de la vie privée. Le service doit déclarer le traitement des données à la CNIL et ce traitement doit être déterminé, explicite et légitime.

- Le service doit obtenir l'autorisation de l'utilisateur pour la collecte et le traitement des données et, de son côté, l'utilisateur doit pouvoir revenir sur son consentement gratuitement et il doit pouvoir supprimer les données de localisation ;
- La durée de la conservation des données doit être déterminée et l'entreprise devra assurer la sécurité des informations traitées ;
- Les utilisateurs doivent être informés de la possible réutilisation de leurs données à des fins commerciales, et doivent avoir donné leur consentement ;

La CNIL a un arsenal de strictes sanctions au cas de non-conformité à l'obligation relative à la géolocalisation. Elle a renforcé les contrôles dans les entreprises proposant des services basés sur cette technologie. La CNIL a la possibilité d'effectuer des contrôles sur place et de demander toute documentation et tout historique. Les manquements à la loi Informatique et Libertés sont punis jusqu'à 5 ans d'emprisonnement et 300.000 euros d'amende.

Le texte du Parlement européen réduit le nombre de cas dans lesquels le marketing direct est considéré comme automatiquement licite. Il prévoit un renforcement du droit dans les cas licites de marketing direct et la personne concernée aura le droit de s'opposer « sans frais, à tout moment et sans autre justification au traitement de ses données personnelles. » [167]

5.3 Droit à l'oubli numérique comme geste de réconciliation sociale

Le droit à l'oubli numérique répond au souci des internautes de contrôler leur réputation en ligne, qui se double de préoccupations autour de la protection des données personnelles.

Lorsqu'une personne se connecte sur un site internet, elle laisse plusieurs types de traces. Des données d'identification, de géolocalisation, puis des données destinées à un cercle d'amis proches… Ces données

sont susceptibles d'être traitées par les acteurs économiques pour fournir un service en ligne, diffuser et générer du trafic.

Au-delà des bénéfices certains, plusieurs risques portent atteinte à la vie privée : un traitement de données personnelles sans avoir le consentement de l'internaute, une durée de conservation de données illimitée, une perte de leur contrôle. C'est dans ce domaine que doit intervenir le droit à l'oubli numérique.

Dans un premier temps, Google avait refusé de se mettre en conformité avec le "droit à l'oubli" imposé par la CNIL, « arguant que l'instance française n'était pas compétente "pour contrôler" les informations accessibles à travers le monde. [185] »

Après avoir contesté cette décision, Google était obligé d'accepter le jugement et a lancé un formulaire en ligne accessible aux Européens, leur permettant de demander la suppression de résultats de recherche. Un jour après cette décision, Google a reçu plus de 12.000 demandes d'internautes européens pour être effacés de ses services de recherche**.**

Le droit à l'oubli numérique est ainsi apparu au niveau de l'Union européenne depuis 2014 dans l'affaire de Conzales. La Cour de justice de l'Union européenne (CJUE) définit ce droit comme l'obligation, pour un moteur de recherche, de « supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages web, publiées par des tiers.[82]

Le droit à l'oubli ne permet pas à un internaute de demander à un hébergeur de supprimer des pages, mais donne la possibilité de demander la suppression des liens. Les pages existent toujours, mais ne sont plus référencées lorsqu'on lance une recherche à partir du nom de la personne. On parle de « déréférencement».

Depuis le 25 mai 2018 et l'entrée en vigueur du RGDP, les pays de l'Union européenne disposent d'une base légale sur le droit à l'oubli et celui de l'effacement. « La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique » : [106]

- Les données à caractère personnel ne sont plus nécessaires au regard des finalités ;
- La personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 1, et il n'existe pas de motif légitime impérieux pour le traitement ;
- Les données à caractère personnel ont fait l'objet d'un traitement illicite ;

Au niveau social, le droit à l'oubli est un geste de réhabilitation dans la société. Le « droit d'oublier » impose collectivement le silence sur les fautes et les peines des citoyens, dans certaines circonstances, pour garantir la paix et la cohésion sociale. Les lois d'amnistie, les règles relatives à la prescription, ou encore l'interdiction de mentionner les condamnations ayant fait l'objet d'une réhabilitation, illustrent bien cette approche.

5.4 Culture numérique et le niveau de délivrances des données

Le comportement des internautes est lié aux avantages dont ils ont bénéficié après avoir partagé certaines informations dans le passé. La culture du pays et les expériences commerciales influencent l'esprit des consommateurs. Si nous observons les résultats de différents pays, nous verrons que les comportements varient en fonction de l'âge, de la culture sociale et des secteurs de marques. Ainsi, les secteurs jouent un rôle important dans la perception des données susceptibles d'être collectées et

partagées. Les attitudes des clients jeunes ayant des comptes sur les réseaux sociaux diffèrent de l'attitude des consommateurs de 60 ans qui n'ont jamais eu de tels comptes.

Les consommateurs américains pensent que les entreprises utilisent leurs données à des fins commerciales et en attendent des avantages en contrepartie. La Chine présente un déficit de partage parmi les plus faibles des trois pays étudiés (France, États-Unis, Chine) [115]. Parmi les trois pays étudiés, les Français opposent la plus grande résistance au partage des données, privilégiant la nécessité de garder le contrôle. Seuls 23 % des internautes français se disent prêts à partager alors qu'ils sont 61% en Chine et 45% aux États-Unis.

Milad Doueihi décrit le numérique comme un processus faisant émerger les normes sociales marquées à la fois de la liberté d'expression et de surveillance. Selon l'auteur, « la dimension religieuse de la culture numérique a pour effet de niveler les différences et de réduire les facteurs locaux à des simples variations superficielles d'une culture technologique universelle et homogène et de son environnement numérique. [97 ; 25-26]»

La culture peut être considérée comme l'ensemble des traits distinctifs, spirituels, matériels, intellectuels, qui caractérisent une société. Elle englobe les arts et les sciences, les modes de vie, les lois, les systèmes de valeurs, et les croyances. D' après le projet des IUCD, on voudrait favoriser des interactions entre la culture et le développement et étudier les dimensions suivantes : économie, éducation, gouvernance, participation sociale, égalité des genres, communication et patrimoine [187].

La culture numérique devient un sujet très délicat qui englobe les traits de la culture générale et celui de numérique. Comme Cardon le dit : il est important de disposer de connaissances variées pour y vivre avec agilité et prudence**, car si nous fabriquons le numérique, le numérique nous fabrique aussi [21]**.

On pense que la culture numérique se comprend dans la dimension globale où se croisent la culture nationale, l'histoire et la politique de chaque nation. Au début de l'histoire du numérique, le but du progrès était le calcul et le décryptage. Le réseau Internet est né d'un impératif pour résister à une attaque nucléaire. Les chercheurs et les ingénieurs étaient mobilisés et financés pour la création du réseau qui deviendra « Advanced Research Projects Agency Network. » Depuis, nous ne pouvons pas imaginer notre vie sans internet et sans objets connectés.

Dans le rapport « repenser la formation scolaire à l'heure du numérique, » une inspectrice générale de l'Éducation nationale définissait le numérique comme «un phénomène culturel et social qui imprègne les actes les plus ordinaires de notre vie et nos représentations du monde : notre perception de l'espace et du temps, notre relation aux autres, nos façons de penser, d'imaginer et de créer, nos modes de travail et d'accès au savoir, ainsi que nos manières de produire et de diffuser les connaissances. [9 ; 11-17] **»**

5.5 Conclusion

Aujourd'hui, plusieurs d'entreprises stockent, traitent et vendent nos informations. Ces entreprises en ont fait un business et les données personnelles sont devenues des marchandises opérant sur le marché et échangent entre elles. Le traitement et la classification des données deviennent un outil performant de plus en plus utilisé. Parfois, certains individus pourraient être sujets d'une surveillance particulière. Les opérateurs de réseaux sociaux dressent des personnalités en fonction de leurs goûts, habitudes, loisirs. Les technologies gèrent des données analysées et tracent les différentes activités des internautes**.** En 2014, Google a été condamné pour la première fois par une juridiction française pour refus de droit à l'oubli. Au niveau social, le droit à l'oubli est un geste de réhabilitation dans la société. Le « droit d'oublier » impose collectivement le silence sur les fautes et les peines des citoyens, dans certaines circonstances, pour garantir paix et cohésion sociales.

CHAPITRE 6

Institutions financières et Données Personnelles

Dans ce chapitre, nous étudions le niveau de protection des données dans les institutions financières. Les données individuelles relatives au secteur bancaire et financier sont, en France, difficilement accessibles. Cela est lié à des problèmes de coût, de qualité de l'information et de confidentialité. En 2011, la Banque de France a créé un portail Internet, Web stat, dédié à la diffusion de données agrégées. Depuis 2014, les établissements financiers sont tenus de fournir publiquement un reporting « pays par pays. » En France, le Comité du secret statistique instruit toutes les demandes concernant des données individuelles collectées par des enquêtes statistiques.

6.1. Introduction

Le nouveau règlement européen des données à caractère personnel du Parlement Européen, du COREPER et de la Commission européenne porte sur les données à caractère personnel et sera le nouveau cadre réglementaire applicable à tous les acteurs économiques ou administratifs. Il va modifier la gouvernance des données, la chaîne des responsabilités et les risques associés. Dans le secteur financier, l'utilisation de FICOBA, FICP, FNCI, FCC, FIBEN pour la lutte anti-blanchiment et la lutte contre le terrorisme nécessitent d'être vigilant sur le respect des obligations réglementaires en la matière.

Le système financier et le comité du Cnis ont mené une enquête en 2013 sur l'accessibilité des données auprès d'une centaine de chercheurs. Cette enquête montre que 9 personnes sur 10 considèrent « indispensable » l'utilisation de données détaillées sur les banques pour leurs recherches ; 7 sur 10 estiment que l'accès à ces données est « difficile » ou « très difficile », 9 sur 10 évaluent l'accès aux données bancaires confidentielles plus restrictif en France que dans les autres grands pays [18].

Les données individuelles relatives au secteur bancaire et financier sont, en France, difficilement accessibles. Cela provient des problèmes de coût, de qualité de l'information et de confidentialité. En 2011, la Banque de France a créé un portail Internet, Webstat, dédié à la diffusion de données agrégées. Ce portail met aujourd'hui à disposition du public plus de 20 000 séries issues de la Banque de France et de grands organismes internationaux partenaires.

L'accès aux données macroéconomiques ne comporte pas d'obstacles importants. Les difficultés d'accès portent sur les données microéconomiques, même lorsque ces données ne posent pas de problème de confidentialité. L'exploitation de ces informations à des fins d'étude et de recherche suppose de pouvoir détenir ces données pour un large ensemble d'entités, dans un format comparable, et sur longue période.

La collecte des données individuelles sur le secteur bancaire et financier est du ressort des autorités de supervision : Banque de France, ACPR et AMF.

Pour l'accès aux données bancaires, la France a pris des engagements dans le cadre de la Charte du G8 pour l'ouverture des données publiques. Ces données sont :

- Les données des marchés ;
- Les données sur les positions bancaires bilatérales, par exemple, les dépôts bancaires des résidents français dans d'autre pays ;
- Les données sur les implantations à l'étranger ;

Depuis 2014, les établissements financiers sont tenus de fournir publiquement un reporting « pays par pays. » En France, le Comité du secret statistique instruit toutes les demandes concernant des données individuelles collectées par d'enquête statistiques.

6.2 Informations obtenues par l'ACPR et transfert à des tiers ; Article L.612-17

L'ACPR a le pouvoir de collecter des données individuelles auprès des banques, et des institutions financières intermédiaires. Ces données sont utilisées par les économistes de l'ACPR à des fins d'études et de recherche.

Pour obtenir une dérogation au secret statistique, le demandeur doit présenter un dossier complet et garantir la protection des données. Surtout, la commission doit être persuadée que la communication de ces données ne serait pas une atteinte pour la concurrence loyale.

En France, pour instruire les demandes d'accès à des données confidentielles, il existe le Conseil scientifique du Comité des données du Réseau Quételet et l'Institut des données de santé. Pour la consultation des données confidentielles les plus sensibles, il existe des accès sur site, sur des stations de travail, ce qui permet un contrôle particulier. Dans certains pays, l'accès aux données confidentielles se fait par un programme plus général. C'est ainsi, par exemple, que procède la Banque d'Angleterre.

En 2009, le Groupe des écoles nationales d'économie et de statistique a créé un équipement avec sécurité élevée qui permet aux chercheurs de travailler sur des données individuelles. Les données collectées par la Banque de France relève du règlement européen qui autorise le transfert de données confidentielles anonymisées aux besoins de recherche.

Malgré la sécurité, dans certains cas, des données permettent d'identifier un établissement de façon indirecte. C'est-à-dire qu'il est possible d'identifier dans une base de données une personne ou une institution alors qu'on ne dispose pas de l'identifiant direct. **L'identification indirecte est presque toujours envisageable, mais sa mise en œuvre demande la mobilisation de moyens importants ainsi que de processus coûteux.**

La Banque de France a investi dans des techniques très efficaces (fonctions de « hachage ») pour la gestion des identifiants cryptés. Donc, l'identification indirecte doit être difficile à mettre en œuvre car les techniques utilisées sont contingentes aux données traitées.

D'après la CNIL, l'anonymisation est une opération complexe dont la difficulté consiste à définir quelles données doivent être anonymisées, pour qui, et dans quel contexte. « **L'anonymat doit être irréversible** et la CNIL est seule habilitée à autoriser la fourniture de données non anonymisées après examen du projet scientifique. La publication ou un autre mode d'exploitation des résultats ne peut donner lieu en aucune manière à une possible identification des personnes. [40]»

Tout traitement de données personnelles à caractère direct ou indirect doit être déclaré à la CNIL. En général, l'anonymisation est l'opération par laquelle on supprime dans les données recueillies tout lien qui permettrait l'identification des personnes.

Les données collectées ont pour seule finalité le contrôle des personnes soumises au contrôle de l'ACPR ou de la BCE. Le code monétaire et financier transpose les dispositions des directives européennes. Les informations obtenues par l'ACPR ne peuvent pas être transférées à des tiers si la loi ne prévoit d'exception, comme à l'article L.612-17 ou encore à l'article L.631-1 (entre autorités nationales).

La non opposabilité du secret professionnel de l'ACPR L'article L.612-17 concerne une personne soumise au contrôle de l'ACPR, soit une procédure pénale et les juridictions administratives saisies d'un contentieux relatif à l'activité de l'ACPR [62].

L'ACPR a la possibilité d'accueillir des chercheurs travaillant dans le secteur pour leur donner accès à l'exploitation des données collectées sous conditions strictes. Ces chercheurs n'ayant pas d'accès direct aux données travaillent comme consultants avec les économistes des études de l'ACPR. Les travaux de recherche sont publiés sur le site internet de l'ACPR, dans « Débats Économiques et Financiers ».

Le centre d'accès sécurisé à distance, CASD de l'INSEE, est placé au sein de Gènes et donne la possibilité aux chercheurs de consulter les données statistiques confidentielles pour une durée limitée. Les recherches doivent s'effectuer dans une organisation qui accueille des chercheurs à la responsabilité juridique. Théoriquement, cet organisme doit être situé dans l'Union Européenne et le CASD lui confiera un ordinateur dénommé SDgBox qui sera relié au serveur central du CASD.

Si l'organisme se situe hors de l'Union Européenne, les chercheurs doivent demander une affiliation au centre de recherche considéré comme institution d'accueil en France.

Après la permission de l'obtention des données, le comité du secret statistique définit le temps de conservation et la finalité d'utilisation. Les chercheurs envoient les documents résultants de leur travail au Comité. Les chercheurs ne peuvent qu'exporter l'information de secret statistique, c'est à dire l'information qui ne donne pas la possibilité d'identifier des personnes ou des entreprises. Il est interdit de diffuser l'information pour lesquelles une seule entreprise représente plus de 85% de la valeur présentée.

Les travaux contenant des informations confidentielles peuvent être gardés sur disque pour une durée maximale de quatre ans. Pendant cette période, le chercheur peut y accéder selon des conditions simplifiées. Au bout de quatre ans, ces données seront détruites par le CASD. Avec les projets de CASD, les chercheurs réalisent des études sur des sujets qui étaient difficiles à conduire jusqu'à présent faute d'accès adapté aux données confidentielles. Aujourd'hui, grâce à ces innovations, le CASD a plus 1000 chercheurs et 350 projets en recherches [22].

6.3 Autorité des marchés financiers dénommée « l'AMF » et transfert des données

La transparence des marchés permet de déceler des tendances potentiellement dangereuses. Les collaborateurs de l'AMF ont une obligation de confidentialité concernant les données collectées, ces

données peuvent être transmises à d'autres institutions dans des conditions strictes. L'AMF a participé, en 2014, aux différents projets présentés par l'ESMA pour proposer des mesures d'application.

L'AMF publie sur son site deux types de bases de données :

- La base des décisions et informations financières (BDIF). Telles que Offres publiques d'acquisition, pactes, dérogations et examens, déclaration des dirigeants ;

- La base de GECO (des données de produits d'épargne et de sociétés de gestion agréés. Dans cette base de données sont publiées des statistiques mensuelles, la liste des produits autorisés à la commercialisation en France…)

L'AMF coopère avec Eurofidai (CNRS) pour enrichir le projet BEDOFIH (une base de données financière européenne à haute fréquence). Ainsi les chercheurs pourront s'appuyer sur des données européennes à haute fréquence, et encourager à travailler sur la régulation financière. Les données de transactions et de cotation seront communiquées par Eurofidai auprès notamment des chercheurs, après conclusion d'accords.

L'accès aux données publiques permet aux institutions et aux individus d'approfondir leurs connaissances et de progresser dans leur vie professionnelle. D'après la charte du G8, « Le monde assiste à la montée en puissance d'un mouvement planétaire favorisé par la technologie et les médias sociaux et stimulé par l'information — un mouvement au potentiel extraordinaire pour encourager l'émergence d'entreprises et de gouvernements plus responsables, efficaces, proactifs et efficients. [25]»

L'accès aux données publiques rend les services des institutions plus performants. Les citoyens deviennent plus actifs et sont plus motivés pour savoir comment les fonds publics sont dépensés. Plus particulièrement, le secteur privé est intéressé par l'ouverture de ces données qui jouent un rôle primordial pour la création de nouveaux emploi et l'innovation des technologies.

D'après la charte, les « citoyens de toutes les nations peuvent et devraient profiter des avantages liés aux données ouvertes. » Les principes de la charte d'accès aux données sont suivantes :

- Accessibles et réutilisables par tous

- De qualité et en quantité

- Ouverture des données pour améliorer la gouvernance

- Ouverture les données pour encourager l'innovation

D'après l'accessibilité des données publiques, le G8 a pour but d'améliorer le fonctionnement de nos démocraties et de diffuser toutes les informations :

Fig. 6 : *Charte du G8 pour l'ouverture des données publiques*

Statistiques sur la criminalité, la sécurité	**Exemples d'ensembles de données**
Criminalité et Justice	Statistiques sur la criminalité, sécurité
Développement mondiale	Aide au développement, sécurité alimentaire, industries extractives, terres
Données géospatiales	Topographie, codes postaux, cartes nationales ou locales
Éducation	Liste des écoles, valeur ajoutée, compétences numériques
Entreprise	registre des entreprises
Enivrement	Niveaux de pollution, consommation énergétique
Finances et Marchés	Valeur des transactions, marchés publics attribués ou à venir, budget local ou national (prévu et exécuté)
Protection Sociale	Logement, prestations sociales, assurance-maladie et assurance-chômage
Observation de la Terre	Conditions météorologiques, agriculture, foresterie, pêche et chasse
Responsabilisation des Gouvernements	Guichets et points de contact des administrations, résultats des élections, lois et règlements, salaires (échelles salariales), dons.
Santé	Données issues de prescriptions, données de performance
Science et Recherches	Données relatives au génome humain, recherche et activités pédagogiques, résultats d'expérience
Statistiques	Statistiques nationales, recensements, infrastructure, statistiques économiques et éducatives
Transport et infrastructure	Horaires des transports publics, services à large bande

6.4 Les banques et Bankscope

L'une des bases des plus connues sur les banques est la base de données Bankscope, présentée par le Bureau van Dijk, qui propose une couverture géographique mondiale. Bankscope fournit des informations générales ainsi que des informations détaillées sur l'état financier des banques, y compris les modèles d'analyse, des structures de la Banque, actualités, documentation AML. Sa couverture des banques est unique. Bankscope comporte des informations sur 32 000 banques. Il est utilisé par plus de 90 % des 1 000

banques mondiales [15]. Ses tarifs pour la recherche sont assez élevés, avec un abonnement de 12 000 euros par an qui ne couvre pas toutes les années.

La couverture de Bankscope :

- 8 000 banques européennes
- 14 000 banques nord-américaines
- 1 000 banques japonaises
- 1 200 banques de Russie
- Plus de 7 000 autres grandes banques
- 35 organismes financiers

Ces bases de données ne diffusent que des données publiques. Leur valeur est l'interface. Ces bases donnent la possibilité d'avoir un accès à des données d'un grand nombre de banques. Malgré les inconvénients, les données Bankscope restent une des grandes bases mondiales appréciées et utilisées par les institutions financières. Les bases sur lesquelles cette compagnie s'appuie sont :

- Informations sur les entreprises publiques et privées dans le monde entier
- Informations sur M & A, introduction en bourse, action des entreprises et résultat de vente des compagnies

6.4.1 Banque de données de jurisprudence, les banques et risque de la protection des données

En 2001, une recommandation portant sur la diffusion de données personnelles sur internet par les banques de Données de jurisprudence était adoptée. L**a CNIL a ainsi préconisé que les éditeurs de bases de données de décisions de justice librement accessibles sur des sites internet s'abstiennent d'y faire figurer le nom et l'adresse des parties ou des témoins au procès, quels que soient l'ordre et le degré de la juridiction et la nature du contentieux** [27]. Par la suite, le site français de bases de données de jurisprudence s'est conformée à la recommandation de la CNIL.

A la suite des modifications techniques apportées au site Légifrance, les décisions de justice qui y sont diffusées ne sont plus accessibles par une requête effectuée à partir d'un moteur de recherche. **La loi prévoit que les informations publiques comportant des données à caractère personnel ne peuvent être réutilisées, à moins que les personnes concernées y aient consenti ou qu'elles aient été anonymisées.**

En Europe, certain pays ont choisi de mettre sur internet des décisions de justice anonymisées. Le Conseil de l'Union européenne a effectué une étude sur la situation des bases de données ou des sites de jurisprudence dans différents États membres. Les résultats ont montré la volonté de s'engager sur l'anonymisation des décisions de justice publiées. La pratique française par rapport à la diffusion des bases de données de jurisprudence sur internet montre une demande accrue des citoyens sur le respect de la vie privée. La commission rappelle que « les bases de données compilant sous forme numérique les décisions prononcées par les juridictions constituent, si elles comportent le nom des parties ou des témoins, des traitements automatisés de données à caractère personnel soumis aux dispositions de la loi du 6 janvier 1978 modifiée en août 2004. » D'après le code monétaire et financier, les institutions financières doivent participer à la lutte contre le blanchiment d'argent et le financement du terrorisme. Ces institutions ont à la fois deux missions : le respect de la vie privée et la lutte contre le financement de terrorisme. Les banques doivent surveiller certaines transactions financières en respectant les principes défendus par la CNIL.

Une première démarche est la vérification des **éléments d'identification** sur présentation de tout document du client. Les banques ont le droit de demander toute donnée **sur la nature de la relation d'affaires**. La banque peut également demander un justificatif de domicile, les statuts, la situation financière…

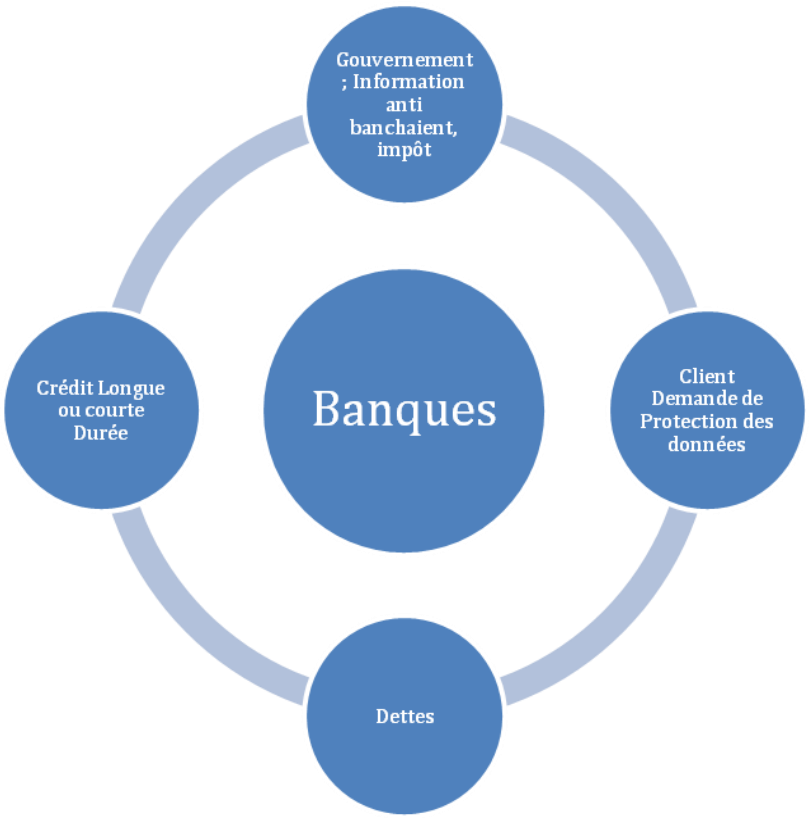
Il est obligatoire de faire connaître aux clients la finalité de la collecte des données. Chaque client doit savoir si ces données doivent être utilisées à des fins commerciales et si ces informations seront intégrées aux traitements automatisés de l'institut financier. Les clients doivent avoir la possibilité de s'y opposer.

De son côté, le responsable du traitement doit obtenir l'autorisation de la CNIL pour mettre en œuvre ce traitement de données. Le responsable doit adresser à la CNIL une demande de conformité à l'Autorisation Unique AU-003.L'autorisation unique AU-003 concerne les traitements mis en œuvre par des organismes financiers afin de leur permettre de répondre à leurs obligations légales de lutte contre le blanchiment de capitaux et le financement du terrorisme. Suite à l'entrée en application du RGPD, les autorisations uniques adoptées par la CNIL n'ont plus de valeur juridique à compter du 25 mai 2018. Dans l'attente de la production de référentiels RGPD, la CNIL a décidé de les maintenir accessibles afin de permettre aux responsables de traitement d'orienter leurs premières actions de mise en conformité.

Les données sont **conservées 5 ans,** y compris la clôture du compte ou la cessation des relations. La banque s'engage à prendre les précautions pour garantir **la sécurité et la confidentialité des données traitées.**

En aucun cas les données confiées à la Banques ne doivent être endommagées et les tiers ne doivent pas avoir la possibilité d'en prendre connaissance.

Fig. 7 : *Relation banques - Clients*



D'après les procédures spécifiques, des données personnelles peuvent être communiquées aux services des autorités nationales, aux services de l'Autorité bancaire européenne, aux membres de surveillance.

La BCE conserve les données personnelles aux demandes/notifications des dirigeants pendant une durée de quinze ans à compter de la date de demande ou de notification [83 ; 2].

Les personnes concernées dans le cadre du traitement des données personnelles ont le droit d'accéder aux données les concernant et le droit de les rectifier. Le règlement (CE) n° 45/2001 du Parlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires est applicable au traitement des données personnelles par la BCE.

Selon le règlement (CE) n° 45/2001, les transferts de données entre institutions ou organes communautaires doivent respecter des conditions spécifiques. Les données à caractère personnel peuvent être transférées si elles sont nécessaires à l'exécution légitime. D'après les règles applicables au personnel de la BCE, les destinataires du dossier individuel sont les suivants :

- **Membres du directoire**
- **Membres du personnel qui sont autorisés par le directeur des Ressources humaines**
- **Tiers autorisé par la direction des Ressources humaines - sous l'accord du directoire**

Conformément au règlement, la personne concernée a le droit d'obtenir du responsable du traitement la communication, sous une forme intelligible, toute information disponible sur l'origine de ces données. Il doit empêcher toute diffusion ou tout accès non autorisés, toute destruction accidentelle ou toute perte. Un responsable du traitement est défini comme une personne qui « seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel. [91 ; article 2]»

Le groupe de l'Article 29 plaidait en faveur d'une interprétation plus large de la notion de responsabilité conjointe qui permettra de faire face à la réalité actuelle. Dans le droit du CdE, la notion de sous-traitant a la même signification que dans le droit de l'UE. Il est défini comme une personne qui traite des données à caractère personnel pour le compte du responsable du traitement (Le Groupe de travail «Article 29» est un groupe de travail européen indépendant qui traitait les questions relatives à la protection de la vie privée et aux données à caractère personnel jusqu'au 25 mai 2018, avant l'entrée en vigueur du Règlement Général sur la Protection des Données – RGPD).

6.5 Fichiers financiers et protection des données à caractère personnel

La Banque de France produit des données financières sur les entreprises françaises dont le chiffre d'affaires est supérieur à 750 000 euros. Ces données décrivent le passif de l'entreprise et mesure sa capacité des engagements financiers pour trois ans.

Les FIBEN, fichiers bancaires des entreprises, sont accessibles aux établissements de crédit, d'assurance-crédit et d'assurance-caution. Ces informations ne peuvent pas être communiquées à des tiers non autorisés. Un accès aux informations FIBEN élargirait l'analyse économique du marché du crédit aux PME. Cette information pourrait être vendue aux acteurs économiques ou publiées dans le domaine public comme l'open data.

Le projet de loi relatif aux entreprises avait envisagé l'ouverture du FIBEN aux assureurs, aux sociétés de gestion et aux plateformes de crowd funding. En France, le financement participatif est en développement constant depuis plusieurs années, passant de **167 millions d'euros** collectés en 2015 à **401,7 millions d'euros** en 201 [102 ; 13].

Les documents publiés par les entreprises permettent de connaître l'endettement financier global et les dettes vis-à-vis des établissements de crédit.

En France, il excite plusieurs sources qui fournissent les informations financières standardisées sur les entreprises.

- La Banque de France / base de données FIBEN
- L'Insee avec une base de bilans, à partir des liasses fiscales et de données internes

Il s'agit du fichier SUSE (Système unifié de statistiques d'entreprises). Le système unifié de statistiques d'entreprises résulte de l'exploitation conjointe de deux sources d'information : l'une fiscale, qui regroupe les déclarations de bénéfices des entreprises à la Direction générale des Impôts (DGI) et l'autre statistique, les enquêtes annuelles d'entreprise (EAE). Cet ensemble cohérent de données individuelles et statistiques sur les entreprises permet ainsi de répondre à des besoins différents.

Chaque entreprise doit adresser sa déclaration annuelle de bénéfice au centre des impôts dont elle relève. La complexité de l'organisation pour le traitement de ces données (il existe 800 centres des impôts et 4 centres de saisie informatique) est une des causes de mécontentement concernant les fichiers transmis à l'Insee.

Les informations envoyées par la DGI à l'Insee contiennent les informations suivantes : les données saisies sur la déclaration fiscale, l'effectif salarié moyen, l'Activité Principale Exercée (APE), la durée et la date de clôture de l'exercice…

Au niveau européen, la nouvelle législation européenne oblige chaque pays de l'UE à fournir à 18 mois des comptes nationaux respectant la structure imposée par Eurostat. L'Office statistique des communautés européennes fournit un service d'information statistique à l'Union européenne (UE).

La source d'information émane de l'Insee qui collecte systématiquement les jugements d'ouverture et de clôture de procédures collectives. Ces jugements sont publiés au BODACC (Bulletin Officiel des Annonces Civiles et Commerciales). Ces données sont accessibles aux utilisateurs des bases de l'Insee, dans le cadre de la procédure du Comité du secret statistique.

Des données existent au sein des greffes des tribunaux de commerce – qui gèrent le Registre de commerce et des Sociétés. Ces données concernent seulement les entreprises faisant l'objet d'une procédure judiciaire. **Les greffes français ne scannent pas l'entièreté des dossiers de faillite et ils ne font pas une collecte automatisée du contenu détaillé des dossiers de défaillance**.

C'est la banque de France qui recense l'ensemble des crédits octroyés par les banques à leurs clients (au-delà de 25 000 euros). Elle dispose également de cette information pour des sociétés non françaises. Les informations sur les risques sont incluses dans le Fichier Bancaire des entreprises (FIBEN) et grâce à ces informations, la Banque de France élabore un indicateur de risque pour environ 200 000 entreprises. **La Banque de France détient un fichier exclusif sur les ménages surendettés. Ces données sont particulièrement sensibles puisqu'elles relèvent de la vie privée.**

Le Fichier National des Incidents de Remboursement des Crédits aux Particuliers (FICP) a été créé en 1989. Il recense les incidents de paiement caractérisés liés aux crédits accordés à des personnes physiques. Les établissements de crédit consultent le FICP pour apprécier la solvabilité d'une personne sollicitant un crédit [101].

Quant au fichier positif, instauré par la loi Hamon [141], il a pour objectif de lutter contre le surendettement en centralisant l'ensemble des crédits. Il est soupçonné de présenter un risque pour les consommateurs ainsi que pour la vie privée. Ce fichier positif sera une base de données recensant les Français bénéficiant d'un crédit à la consommation. Ce fichier sera placé sous la responsabilité de la Banque

de France. Ce type de fichier aurait concerné plus de 12 millions de personnes. Sa consultation aurait été obligatoire avant l'octroi d'un nouveau crédit par les banques.

Un tel fichier positif existe dans plusieurs pays européens, dont l'Allemagne, le Royaume-Uni et la Belgique, dont but est de responsabiliser les prêteurs et mettre à leur disposition un maximum d'informations avant l'octroi d'un crédit. L'association de consommateurs pense que « les établissements de crédit l'utilisent à des fins commerciales ».

D'autres grands fournisseurs d'informations sont Altares et Diane. Les études d'Altares sur les « Défaillances et sauvegardes d'entreprises en France » sont publiées trimestriellement et un bilan est édité annuellement [5]. Les bases de Données assez fiable sont celles de Diane. Diane est l'outil de référence pour la proportion commerciale et l'analyse financière des sociétés en France. Ces données financières contiennent :

- État financier, bilans, comptes
- Comptes consolidés aux normes IFRS
- Opération des fusions acquisitions
- Indicateurs des solidarités financières

La base de données de Diane a à sa disposition des informations actualisées sur les entreprises françaises et son outil de recherche est l'un des plus puissants sur le marché français [14].

6.6 Information publique et données personnelles

Depuis 2014, les établissements financiers européens sont obligés de rendre publique des informations concernant leurs activités et les impôts qu'ils payent dans chacun des pays où ils sont présents. Cette obligation, appelée « reporting pays par pays » est une recommandation des organisations de la société civile pour plus de justice fiscale.

« Le gouvernement britannique évalue par exemple le coût annuel de l'évasion fiscale à plus de 12 milliards de livres (16,5 milliards d'euros). Le Sénat américain estime que les seules falsifications des prix de transfert font perdre aux autorités fiscales plus de 50 milliards de dollars par an. [179]»

Les standards de transparence servent à savoir :

- **Les chiffres d'affaires des entreprises**
- **Les résultats avant impôts**
- **Le montant des impôts sur les bénéfices**

Les informations exigées par la loi bancaire de 2013 ne sont obligatoires que pour les entités consolidées. Les normes comptables internationales (*International Financial Reporting Standard*) prévoient des exceptions à l'inclusion d'entités dans le périmètre de consolidation. Les pays du G20 ont adopté en 2014 une série de mesures proposées par l'OCDE visant à lutter contre l'érosion des bases fiscales et le transfert des bénéfices.

Le G20 a validé en juin 2012 un dispositif d'identifiant unique des intervenants sur les marchés financiers (Global Legal Entity Identifier System, GLEIS), afin de faciliter la gestion et le contrôle des risques.

La Commission nationale Informatiques et libertés (CNIL) alerte contre les services d'agrégation de comptes bancaires disponibles sur Internet. En France apparaissent différents services PFM (Personal Finance Management), connus sous le nom d'agrégateurs de comptes sur Internet, tels que Money Center de Boursorama ou les produits de Linxo. Ces applications agrègent sur une seule interface l'ensemble des données financières de l'usager, même si ses comptes bancaires et contrats d'assurances sont détenus dans différentes enseignes. Ces informations sensibles, qui seront ensuite stockées sur des serveurs, font courir un risque de détournement des données par des pirates.

Monaydoc est l'outil pour classer ses factures tout en faisant ses comptes. Une fois son historique synchronisé, on pourrait télécharger la facture, le ticket ou la fiche de paye correspondant à l'opération.

Iswigo : « ce site combine l'agrégation automatique de comptes et la gestion manuelle. On peut ainsi y rentrer la date de paye, de prélèvement, obtenir un prévisionnel des sommes disponibles. » Le site a aussi une fonction « coffre-fort » pour stocker ses documents. En communiquant volontairement des données personnelles, par exemple en faisant une commande en ligne, on accepte de faire la saisie, l'enregistrement et le traitement des données. Les données sont transmises de façon cryptée et enregistrées dans des bases de données de ce site.

Le résident français a à sa disposition un large choix de produits d'épargne retraite, qu'ils soient individuels ou collectifs. La société Profideo édite sur la retraite collective les PERP et les contrats « Madelin ». Les données disponibles sont collectées directement auprès des gestionnaires.

Profideo est un partenaire de référence pour tous les acteurs de la banque, de l'assurance et du crédit qui souhaitent bénéficier en temps réel d'une information décisionnelle claire. Elle possède une équipe de consultants experts des marchés du Crédit, de la Banque et de l'Assurance.

Le PERCO est régi par le Code du travail et donne accès à des fonds communs de placement. En particulier, l'AMF rend disponible dans sa base GECO le Document d'informations clés pour l'investisseur (DICI) pour chaque fonds agréé en France. Ces données incluent des informations sur le niveau financier. Cette information est importante pour des fonds, mais ne permet pas d'identifier les relations entre les fonds figurant dans un même PERCO.

Depuis l'espace sécurisé sur internet, on pourrait piloter l'épargne salariale à tout moment :

- Effectuer des versements,
- Modifier les orientations de placement.

Cette plate-forme, certifiée ISO 9001, s'appuie sur un système de Gestion Électronique des Documents (GED).

La réglementation ne permet pas de rendre publique des informations relatives à la gestion des produits d'épargne retraite supplémentaire. Des données microéconomiques sont collectées par l'ACPR et l'AMF, mais elles ne couvrent pas l'intégralité du marché. La création d'un rapport uniformisé annuel pour ces produits d'épargne retraite serait très utile. Il est important que les épargnants aient accès au montant des frais. L'AMF fournit avec sa base GECO l'intégralité des OPCVM.

L'AMF et l'ACPR pourraient ainsi unir leurs efforts pour délivrer les informations microéconomiques sur les produits d'épargne retraite. Les organismes de placements collectifs en valeurs mobilières (OPCVM) sont des instruments financiers mis au point par des sociétés agréées pour gérer l'épargne publique.

Aux États-Unis, le principe de l'Open Government, donne la possibilité d'accéder aux données collectées par les organisations publiques de régulation et de contrôle. D'après ce principe, l'accès aux données doit être facilité aux niveaux techniques ainsi qu'au niveau réglementaire.

6.7. Conclusion

Selon le code monétaire et financier, les institutions financières doivent participer à la lutte contre le blanchiment de l'argent et le financement du terrorisme. Ces institutions ont à la fois deux missions : le respect de la vie privée et la lutte contre financement de terrorisme. Les banques doivent surveiller certaines transactions financières en respectant les principes défendus par la CNIL. Il est obligatoire de faire connaître aux clients la finalité de la collecte des données. Chaque client doit savoir si ces données doivent être utilisées à des fins commerciales et si ces informations seront intégrées aux traitements automatisés de l'institut financier. Les clients doivent avoir la possibilité de s'y opposer.

La Commission nationale Informatiques et libertés (CNIL) alerte contre les services d'agrégation de comptes bancaires disponibles sur Internet. En France, différents services PFM (Personal Finance Management) apparaissent, plus connus sous le nom d'agrégateurs de comptes sur Internet, tels que Money Center de Boursorama ou les produits de Linxo.

Ces applications agrègent sur une seule interface l'ensemble des données financières de l'usager, même si ses comptes bancaires et contrats d'assurances sont détenus dans différentes enseignes. Les informations sensibles, lesquelles seront ensuite stockées sur des serveurs, font jouer un risque de détournement des données par des pirates.

CHAPITRE 7

Commerce et obligation de protection des données à caractère personnel

Dans ce chapitre, nous avons étudié la problématique de la protection des données dans l'e-commerce et le marketing digital. La collecte des données peut être effectuée simultanément avec le procès d'achat ou de service. Avec la procédure de l'identification pour l'achat ou le service internet, il est possible de collecter les informations concernant les clients qui seront stockées selon les intérêts du commerçant. A l'aide des informations collectées, ce type de marketing arrive à combiner plusieurs informations et à cibler les clients potentiels. C'est le moyen de ciblage qui pose problème au niveau de la protection des données et de la vie privée.

7.1 Introduction

En effectuant des achats en ligne, le commerçant peut demander quelques informations à ses clients qui créent leur compte sur le site. En même temps, le commerçant est obligé d'assurer la sécurité de la transaction et la protection des données délivrées par le client.

Il existe des informations facultatives et obligatoires. Les informations obligatoires concernent la livraison et le transfert d'argent. Les informations facultatives sont par exemple les loisirs, les centres d'intérêt, la date de naissance. Le client est obligé de saisir le numéro de sa carte bancaire pour la relation de transaction. Après le paiement, le commerçant ne peut pas conserver ou réutiliser les coordonnées bancaires du client. **Une conservation en base « archive » est néanmoins permise pendant 15 mois, délai de contestation du titulaire de la carte. Le cryptogramme visuel ne doit pas être conservé [39]**.

Dans le commerce en ligne, les utilisations de cartes bancaires sont de plus en plus frauduleuses. Le commerçant peut utiliser un système appelé «3D Secure» de Visa et Mastercard. Pour le paiement sécurisé, un code à usage unique doit être adressé à l'internaute par sa banque via sms sur son téléphone. À défaut de renseigner ce code, la transaction ne pourra pas s'effectuer.

Pour s'assurer de l'identité de l'internaute, le commerçant peut demander un justificatif d'identité et / ou de domicile. Mais, il ne peut pas demander un relevé de compte ou une photocopie de la carte vitale ni du RIB. Les services du paiement ou de la lutte contre la fraude doivent avoir accès à ces documents. Ils ne peuvent les utiliser à d'autres fins ni les conserver au-delà de six mois. Un fichier d'un site d'e-commerce peut faire l'objet d'une déclaration de conformité à la norme n°48 (déclaration simplifiée).

Pour défendre leurs droits les consommateurs peuvent s'adresser à :

- La CNIL, Service des plaintes ;
- La Direction départementale de la concurrence, de la consommation et de la répression des fraudes (DDCCRF) ;
- Le Procureur de la république ;

Les publicités sont envoyées aux particuliers parce que leurs coordonnées figurent dans des bases de données. Il pourrait s'agir des fichiers-clients ou prospectus constitués par les sociétés commerciales. Le consentement des consommateurs est nécessaire pour échanger leurs coordonnées électroniques à des buts commerciaux. Pour recueillir ce consentement, le client doit cocher une case spécifique. La simple acceptation des conditions générales ou de vente n'est pas valable. Les exceptions au recueil du consentement préalable sont :

- Quand la publicité est envoyée sur l'adresse électronique professionnelle d'une personne physique (ex :…….@entreprise.com) et que l'objet de la sollicitation est lié avec sa profession (« B2B ») ;
- La publicité concerne des produits analogues à ceux que le consommateur a déjà du même organisme.

Les utilisations à exclure sont :

- Collecte des adresses électroniques des particuliers sur des sites internet
- Accès à un service, l'achat d'un bien ou le bénéfice d'une réduction si l'on accepte de recevoir des messages publicitaires par voie électronique.

L'utilisation du « profil » d'un consommateur, établi à partir des données le concernant, ne doit pas conduire à le priver de certains biens ou services, ni à l'exclure d'un droit [35]. À tout moment, les consommateurs doivent pouvoir s'opposer à la réutilisation de leurs données à des fins commerciales. **Les informations recueillies dans le terminal des utilisateurs permettant de les tracer ne doivent pas être conservées au-delà de 13 mois.** Les mentions d'information doivent être lisibles et compréhensibles pour le consommateur.

Les consommateurs doivent être informés :

- De l'identité du responsable de fichier (nom de la société et adresse)
- De l'utilisation qui sera faite de leurs données
- Des modalités des droits d'opposition, d'accès et de rectification

7.1.1 Parrainage

En Général, le parrainage demande à une personne de renseigner les coordonnées d'autres personnes (proches) intéressées par une offre commerciale. Pour le parrainage, il existe des règles très précises. Le destinataire du message doit être informé de l'identité de son parrain lorsqu'il est contacté par l'entreprise. **Les données du parrainé peuvent être utilisées une seule fois : pour l'offre commerciale.** L'entreprise pourra conserver les données du parrainé pour lui adresser d'autres messages si elle a déjà obtenu son consentement. Pour éviter l'abus de droits de la vie privée, il est impératif de prendre des mesures de sécurité.

• Une durée de conservation des données est limitée : Les données relatives à non-client peuvent être conservées pendant trois ans à compter de leur collecte ou du dernier contact [34].

• Les parrainés et les participants au jeu concours disposent d'un droit d'accès et de rectification aux informations les concernant.

Des mesures de sécurité doivent être prises pour garantir une protection convenable et non autorisation d'accès des tiers. Donc les formulaires en ligne doivent être chiffrés.

7.2 E-commerce et ses liens avec marketing, chiffres clés par Fevad

Les clients laissent leurs traces sur l'internet, ce qui rend facile la récolte de données par les spécialistes du marketing. Avec des moteurs particuliers, sur les forums ou via un simple accès sur un site, des informations sont générées qui demeurent dans la mémoire électronique.

Les spécialistes récupèrent ces informations, les rassemblent, les analysent, les stockent pour les vendre du mieux possible.

La collecte des données peut être effectuée simultanément lors du processus d'achat ou de service. Avec la procédure de l'identification pour l'achat ou le service internet, il est possible de collecter des informations concernant les clients qui seront stockées selon les intérêts du commerçant.

La communication entre ordinateurs sur internet n'est possible que grâce à l'utilisation de protocoles spécifiques. Le protocole TCP/IP donne la possibilité de transporter des informations sur le web et leur réunion chez le destinataire. Le destinataire est identifié par son IP. Le TCP/IP est l'ensemble des règles de communication qui se base sur la notion d'adressage IP. Les protocoles TCP/IP ont été créés dans un but militaire et répond aux critères suivants :

- Utilisation des systèmes d'adresse
- Routage, acheminement des données
- Contrôle des erreurs de transmissions des données

L'utilisation de ces protocoles montre la transmission de diverses informations telle que l'IP et la langue utilisée par le programme, type d'utilisation, date et heure de la connexion, toute requête éventuelle (page que l'utilisateur visite). Ces informations sont susceptibles d'être enregistrées par le programme de navigation et par les serveurs.

Les spécialistes traitent ces données pour offrir aux potentiels clients d'autres produits. Les représentants du e-commerce sont intéressés par la possibilité de devenir un fournisseur de données à caractère personnel dans notre monde actuel.

Les sites commerciaux de vente sur internet sont soumis à une réglementation de la vente à distance (VPC), comprenant des obligations déclaratives (protection des consommateurs, TVA) et des mentions obligatoires. Le commerçant doit en respecter les conditions suivantes :

- Informer les clients de leurs droits d'accès, de modification et de suppression des informations collectées

- Avoir une sécurité des systèmes d'information convenable
- Indiquer une durée de conservation des données.

Le responsable du site de vente en ligne qui collecte des informations nominatives et constitue des fichiers de clients doit effectuer une déclaration auprès de la CNIL. Le Conseil de l'Europe a adopté en 2001 la convention sur la Cybercriminalité qui est souvent citée lors de tout commerce électronique. Elle concerne non seulement les Etats-membres mais aussi le Japon et les États-Unis.

Au niveau de l'Union européenne, la législation relative au e-Commerce est la suivante :

- La directive 1999/93 sur la signature électronique du 13 décembre 1999 ;
- La directive 2000/31/CE sur le commerce électronique de 2000 garantissant la sécurité juridique pour les entreprises et les consommateurs ;

En droit français, trois lois concernent le commerce électronique :

- Loi relative à la preuve électronique du 3 mars 2000 [137]
- Loi pour la confiance dans l'économie numérique [138]
- Loi sur la protection des personnes physiques à l'égard des traitements de données à caractère personnel

Après les années 1990, chaque consommateur est différencié et ne plus être identifié en groupe commun. Avant d'acheter un produit, il compare et réfléchit, ses exigences sont de plus en plus grandes, il devient autonome. Les entreprises décident d'apporter une offre adaptée au consommateur. Le marketing « one to one » est un marketing individualisé, qui doit permettre aux entreprises d'avoir une relation personnalisée avec les clients. Ce type de marketing est représenté par 4 phases : Identifier, différencier, interagir et personnaliser.

Le CRM, outil de marketing « one to one » se concrétise avec internet. Cet outil aide à établir le fichier de base de données pour la fidélisation des clients. Ainsi on arrive à créer le profil du client en traitant et en exploitant ces données. La loi prévoit la reconnaissance d'un droit d'opposition de la personne concernée. L'exercice de ce droit est gratuit.

L'intérêt commercial d'une entreprise est suffisant pour légitimer la collecte et le traitement de données non sensibles relatives à ses clients actuels ou potentiels en vue d'une finalité de marketing.

Le transfert de données à des tiers contient un risque de perte potentielle de contrôle de la personne sur ses données. Le client ne sait pas à qui ses données vont être communiquées et dans quel but elles serviront. Il y aura toujours des risques que le tiers ne respecte pas les lois sur la protection des données.

Au cas où l'internaute refuse que ses données soient collectées, le responsable de service peut lui interdire l'accès à son site. Le consommateur doit avoir la possibilité de conserver et reproduire la vente sur internet comme une proposition de contrat d'après les conditions contractuelles applicables (article 1369-4 du Code Civil) [37].

Le droit de rétractation permet au consommateur de revenir sur ses engagements. Le délai de rétractation est de quatorze jours en France. Il existe des exceptions et certains cas prévus par la loi ne sont pas concernés par ce délai (articles L.121-20-2 et L.121-20-4) : ventes de biens, de transport et de restauration. En cas de non-respect de l'obligation liée au droit de rétractation, il est encouru une amende administrative de 15 000 € maximum pour une personne physique et de 75 000 € pour une personne morale.

La France est le deuxième marché d'e-commerce d'Europe après le Royaume-Uni.

Fig. 8 : *Chiffre d affaire E commerce de 2018, Source : Fédération e-commerce et vente à distance, « Les chiffres clés 2019 »*

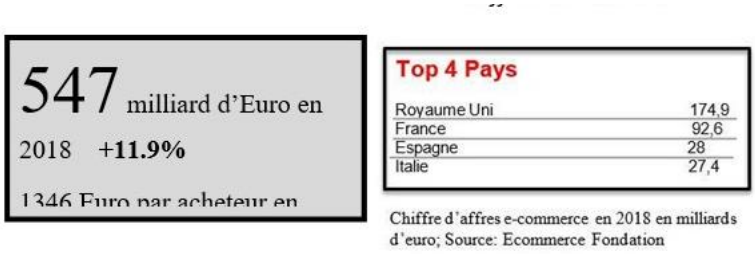
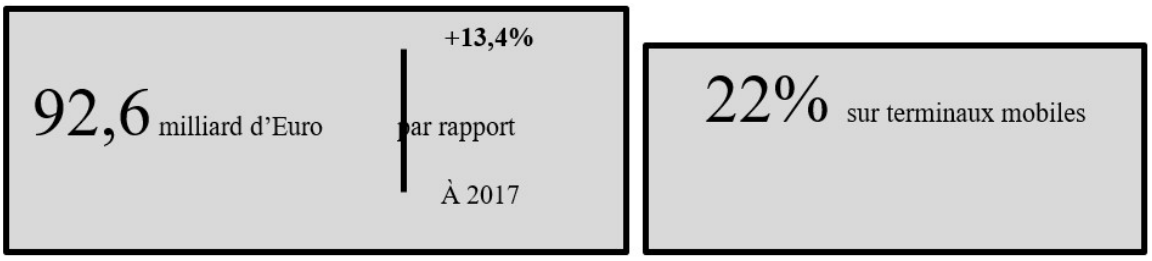
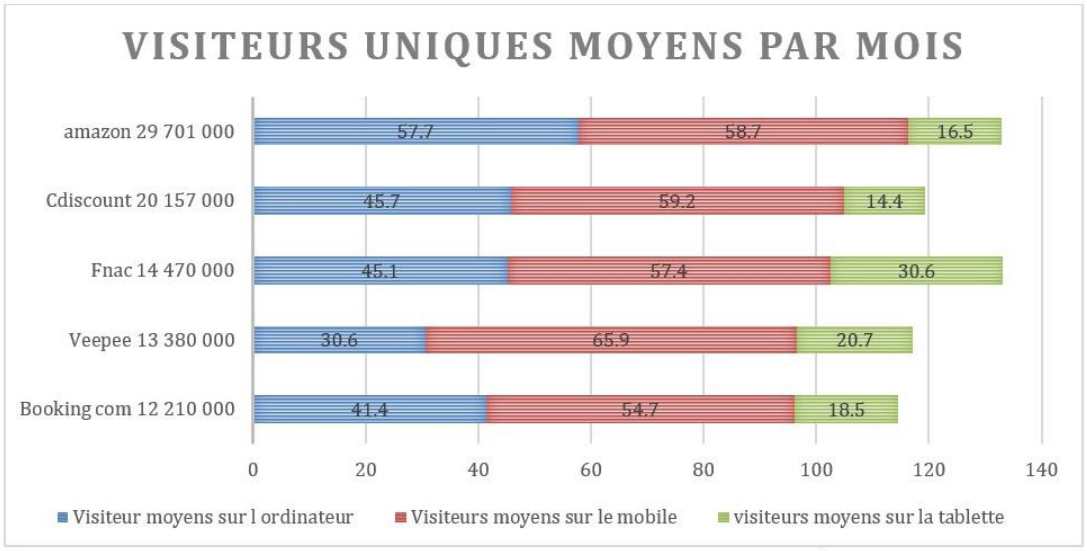


Fig. 9 : *Nombre de consommateurs utilisant l'E Commerce en 2018. Source : Fédération e-commerce et vente à distance, « Les chiffres clés 2019 »*



Le chiffre d'affaires de ventes internet continue d'enregistrer des progressions à deux chiffres.

[57]



Source Médiamétrie//Net ratings Moyenne – T1 2019 France - Audience internet

Fig. 10 : Sites les plus visités en France en 2019. Source Médiamétrie.

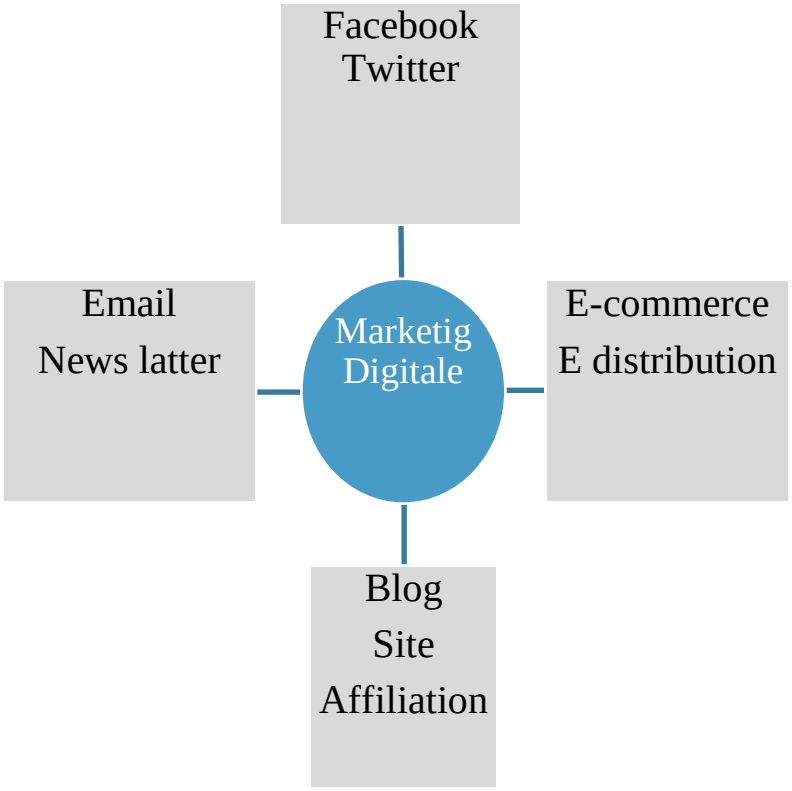
Site	visiteurs par mois	Visiteurs par jour
Amazon	16 832 000	1 878 000
C Dicount	10 501 000	68 000
Fnac	8 847 000	676 000
E Bay	7 989 000	969 000
voyage. sncf.com	6 768 000	488 000

7.3 E-Marketing, moyen de ciblage et atteinte à la vie privée

Le marketing digital favorise le marketing participatif et actif des clients. A l'aide des informations collectées, ce type de marketing arrive à combiner plusieurs informations et cibler les clients potentiels. C'est le moyen de ciblage qui pose problème au niveau de la protection des données et de la vie privée.

Le marketing digital exerce ces activités avec des moyens différents.

Fig. 11 : *Marketing digital (par l'auteure)*



Les outils jouent différents rôles sur le parcours client en fonction du secteur. Dans le secteur du voyage, le contact direct, par e-mails, intervient dans la phase d'accompagnement avec publicités. Dans la distribution, la publicité est efficace comme premier contact avec la marque par les réseaux sociaux et l'envoi d'e-mails.

Il est intéressant de connaître le droit sur le marketing one-to-one et ses finalités. Le marketing direct est "l'ensemble des activités ainsi que tout service auxiliaire à celles-ci permettant d'offrir des produits et des services ou de transmettre tout autre message publicitaires par le moyen du courrier, du téléphone ou d'autres moyens directs dans un but d'information »[70].

On peur légitimer l'intérêt commercial d'une entreprise pour la collecte et le traitement de données non sensibles relatives à ses clients actuels ou potentiels dès qu'un droit d'opposition est reconnu à la personne concernée.

La loi prévoit en son article 12 la reconnaissance d'un droit d'opposition en faveur de la personne concernée. Les données qui seront traitées visent souvent à tracer l'internaute dans ses déplacements sur les sites visités. Ces **techniques permettent d'être utilisées sans que l'internaute n'ait la possibilité de le contrôler.**

La technique numérique permet de traiter ces informations pour soi ou pour des tiers. Souvent, les transferts de données à caractère personnel sur l'internet ne sont pas sécurisés.

La nouvelle loi prévoit la reconnaissance d'un droit d'opposition en faveur de la personne concernée. L'exercice de ce droit est gratuit. **L'obligation de passer par le consentement de la personne est confirmée par différents textes internationaux.**

Le groupe européen de protection des données, le « groupe 29 » - déclare dans sa recommandation : « Toute collecte des données sur des personnes navigantes sur la Toile doit cependant se faire dans la transparence avec le consentement éclairé de l'internaute concerné. Les personnes souhaitant de manière anonyme naviguer sur des réseaux doivent être entièrement libres de pouvoir le faire (Le Groupe de travail «Article 29» (GT art. 29) est le groupe de travail européen indépendant qui traitait les questions relatives à la protection de la vie privée et aux données à caractère personnel jusqu'au 25 mai 2018). »

L**'internaute doit connaître, pour chaque type de collecte et de transfert, les finalités d'utilisation. La nouvelle loi reconnaît un droit d'opposition par rapport de marketing**.

Les responsables de marketing cherchent à conquérir les clients et les fidéliser le plus vite possible. Les buts des marqueteurs sont les suivants :

- Développer un marketing convenable pour les clients
- Faire rapprocher marketing et IT pour être leader sur le marché
- Faire des fichiers clients approfondis pour mieux répondre à leur exigence.

Ce marketing enrichi par les données des clients donne la possibilité d'accéder à une expérience personnalisée et attirante.

A l'aide du marketing digital, le consommateur est habitué à être reconnu et à avoir des produits ou des services en fonction du lieu où il se trouve, de la date et de leur intérêt…

Les risques de marketing digital consistent non seulement en la collecte des données et leur utilisation par des tiers mais aussi en leur garde en sécurité.

C'est toute une nouvelle manière d'aborder le processus d'achat qui émerge pour le consommateur. L'achat en ligne est le confort des clients, mais cela contient des risques au niveau de la sécurité des données personnelles qui peuvent être réutilisées ou simplement piratées. Malgré ces risques, d'après les recherches du Fevad en 2015, les transactions d'achat en ligne ont augmenté de 13 % par rapport à 2013 et cette augmentation se poursuit.

Les chiffres progressent ces dernières années et 65 % des Français ont effectué leurs achats avec internet en 2015 [100].

Le plus risqué en effectuant un achat en ligne est la sécurisation des données bancaires qui doivent être traitées et conservées d'après des règles spécifiques. Au niveau du contrôle des données, seuls le service de lutte de fraude et le service de paiement ont le droit de vérifications des données. Tout de même, ils n'ont pas le droit de les réutiliser ni de les conserver plus de six mois.

Le commerçant a le droit de faire appel à un prestataire de service qui lui garantira ou non le paiement des transactions. De son coté, le prestataire va définir un niveau de risque acceptable ou non par le commerçant. Si la transaction est considérée comme non risquée, le paiement et la livraison s'effectueront normalement et, en cas de contestation ultérieure, le prestataire remboursera le commerçant.

Malgré les transactions risquées, les chiffres des rapports du Fevad sont impressionnants. D'après les études menées par la société Dashlane, spécialiste de la gestion de l'identité en ligne, le consommateur n'est pas bien protégé du piratage quand il fait des achats en ligne. La société a étudié 25 sites Internet en prenant en compte plusieurs critères (obligation d'utiliser un mot de passe, nombre de tentatives de connexion successives possibles…). Selon leur rapport, 52 % des sites analysés ont un score négatif. 52 % des sites autorisent au moins 10 tentatives de connexion successives et 36 % acceptent des mots de passe faibles [89]. En réalisant des achats, des portefeuilles électroniques (aussi appelés « wallets ») sont souvent proposés. Ils peuvent être proposés par certaines banques mais aussi des opérateurs de téléphonie, etc. Dans ce cas, on confie à un « tiers » les données personnelles et de paiement, qui sont stockées en vue de réaliser des opérations de paiement. Après cette démarche, on n'a plus à saisir ni le cryptogramme ni le code 3D Secure habituellement demandés et les données de carte ne sont pas communiquées au site marchand.

Face au piratage et à la surveillance, l'internaute voudrait de plus en plus naviguer en tout anonymat sur l'internet. Mais d'après les institutions françaises, l'anonymat est une question complexe d'intérêts éthiques, économiques et politiques [180 ; 47]. Le processus pour devenir anonyme consiste à passer par un serveur intermédiaire qui vous renverra à son tour les pages. Ce serveur est dit Proxy. La question de l'anonymat sur internet est tellement importante que même le président de république s'exprime sur ce sujet. ***« Nous travaillons avec Jean-Marc Ayrault (...) pour éviter la tranquillité de l'anonymat qui permet de dire des choses innommables sans être retrouvé »,*** **a déclaré le président [188].** La loi sur la Confiance dans l'Economie Numérique (dite « loi LCEN ») de 2004 distingue différents participants de l'Internet et leur applique un régime de responsabilité différent. Lorsqu'il s'agit d'un non-professionnel, comme dans le cas d'un blogueur anonyme, la loi lui permet de garder le masque de l'emblème de son choix. L'anonymat pourra être levé par une simple demande adressée à un juge et avec des moyens différents (Web bug).

7.4 Conclusion

Les représentants de l'e-commerce sont intéressés de devenir fournisseur de données à caractère personnel dans notre monde actuel. Les sites commerciaux de vente sur internet sont soumis à la réglementation sur la vente à distance (VPC), comprenant des obligations déclaratives (protection des consommateurs, TVA) et des mentions obligatoires. Le commerçant doit en respecter plusieurs conditions.

On peut légitimer l'intérêt commercial d'une entreprise pour la collecte et le traitement de données non sensibles relatives à ses clients actuels ou potentiels dès qu'un droit d'opposition est reconnu à la personne concernée. **Les risques de marketing digital consistent non seulement en la collecte des données et en leur utilisation par des tiers, mais aussi par leur mise en sécurité.**

CHAPITRE 8

Contrat de vente et risques de protection de la vie privée

Dans ce chapitre, nous parlons des contrats de vente, des responsabilités et obligations des vendeurs et des clients. Nous avons étudié le facteur de DUA (durée d'utilité administrative) dans la protection des données. C'est une « durée légale ou pratique pendant laquelle un document est susceptible d'être utilisé par le service producteur ou son successeur, au terme de laquelle est appliquée la décision concernant son traitement final. »

8.1 Introduction

Un **contrat de vente** est une convention par laquelle une personne s'oblige à livrer une chose, et une autre à la payer. Quand il s'agit de l'action de vente, on a les éléments caractéristiques suivants :

- Prix
- Chose (ou service)
- Transfert

Le prix dans la vente doit être déterminé ou déterminable. Il n'y a pas de difficulté quand le prix est indiqué lors de la conclusion du contrat, puisque le prix est alors définitif. Mais lorsque les ventes s'étalent dans le temps, le prix n'est pas fixé définitivement et il sera fixé le jour où le bien sera livré. Pour avoir l'objectivité du prix, dans le contrat est prévue une clause de détermination du prix par un tiers. Il existe d'autres techniques de fixation :

✓ Le recours à une clause indexation du prix ou

✓ La référence à la rentabilité de la chose

Le prix doit être réel et sérieux. Si le prix réel est plus élevé, ou plus bas, que le prix apparent, il s'agit d'une simulation. Un prix dérisoire n'est pas un prix simplement déséquilibré mais un prix si bas, qu'en fait c'est comme s'il n'y avait pas de prix. Il existe des règles de protection des consommateurs qui imposent une information et une transparence sur les prix de vente. Dans les contrats, il y a toujours l'obligation d'affichage des prix et l'obligation de transparence dès la publicité. En matière de vente, les pouvoirs de révision du prix par le juge sont très limités.

Fig. 12 : *Dépendance de chose, prix et réalisation (par l'auteure)*

La chose vendue se traduit par une variété très large d'objets de vente : un bien corporel ou incorporel ; un bien matériel ou immatériel, etc. Pour distinguer la vente du contrat d'entreprise, on parle de la spécificité du travail effectué, de la chose à réaliser. Une question se pose lors des services liés à la vente. Dans de nombreux contrats de vente, le vendeur s'engage à effectuer des prestations de services (la livraison à domicile ou le service après vente) ; ces prestations constituent des accessoires à la chose vendue, utiles à l'utilisation de cette chose. Ces prestations supplémentaires impliquent des règles particulières. Ces prestations sont prévues dans le Code de la consommation.

La chose doit exister ; être déterminée ou déterminable. La vente de choses futures est un contrat commutatif où le transfert de propriété aura lieu quand la chose existera ; mais dans des cas exceptionnels, la vente de choses futures est un contrat aléatoire. L'article 1130 du Code civil propose un principe sur des choses futures (par exemple un immeuble à construire) [50].

La loi interdit toute vente portant sur le corps humain ; les stupéfiants ; les successions futures ; les droits civils ou politiques tels que le droit de vote, la vente de la chose d'autrui…

L'article 1129 du Code civil impose que la chose objet du contrat soit déterminée ou déterminable.

Il existe deux techniques pour déterminer la chose dans la vente :

- Vente en bloc : cette technique permet de déterminer la chose en référence. La chose est déterminée dès la conclusion du contrat de vente et le transfert de propriété se fait immédiatement ;

- Vente au poids, ou à la mesure : dans ce cas, l'individualisation de la chose ne se fait pas au moment de la conclusion du contrat ; le transfert de propriété de la chose est repoussé au moment de son individualisation ;

L'effet de la vente est d'opérer le transfert de propriété de la chose. L'article 1583 du Code civil est un modèle proposé aux parties. Le transfert de propriété dès l'échange des consentements est une règle supplétive de volonté.

Lors de la vente de choses, le vendeur et l'acheteur peuvent établir un autre schéma. Quand le contrat est affecté d'une condition, l'obligation naîtra au jour où l'événement incertain se réalisera.

D'après le droit, nous avons le principe que toute acquisition de la propriété se fait par le biais d'un contrat. Un « contrat de vente, d'échange ou une donation. » Mais il existe le principe selon lequel le transfert de propriété s'effectue par la volonté des parties sans qu'aucune autre formalité ne soit requise. C'est ce que l'on appelle le transfert de propriété *solo consensu*.

La jurisprudence n'a pas éprouvé le besoin de fonder ses solutions sur l'existence d'une obligation de donner dans les espèces dans lesquelles était en jeu la question du transfert *solo consensu* d'un droit de propriété.

Quand la nature des choses tient en échec le transfert *solo consensu* de la propriété, parce qu'il s'agit d'une chose indéterminée, ce transfert pourra se réaliser quand cette chose sera identifiée ou créée. Dans ce cas, il faut étudier la question de l'obligation.

On peut distinguer l'obligation de faire et l'obligation de donner. Les sources de la vente sont différentes :

- Normes nationales ; (constitutions)
- Directives (prises par les institutions de l'UE)

- Convention de Vienne (ratifiée par la France en 1988). Elle s'applique aux professionnels ayant leurs établissements dans des pays différents.

Le contrat peut être écrit ou oral. Les contractants sont libres de choisir la forme du contrat. Il existe quelques types de contrat qui imposent une forme écrite. Par exemple : vente de maison, assurance …

La justification du contrat écrit est plus facile et en cas de litige, le problème est facile à prouver.

Il existe certaines conditions pour rédiger les contrats :

- Aucun des cocontractants ne doit être mineur ou majeur protégé. C'est l'article 1154 du Code civil qui en dispose.

- **L'objet doit faire partie des choses dans le commerce** (article 1128 du Code civil : « Il n'y a que les choses qui sont dans le commerce qui puissent être l'objet des conventions » [49]

- **l'objet du contrat doit appartenir au vendeur [53]**

- **Le consentement doit être libre et éclairé**

- Obligation de l'information : Le vendeur doit définir les caractéristiques essentielles du bien ou du service offert (nature du produit, prix).

- **Tout contrat dont la valeur excède quelque somme, doit faire l'objet d'un écrit**.

Depuis 1970, il existe un certain nombre de dispositions pour protéger le consommateur, dont dispose le Code de la consommation. Par ex. :

« La loi Consommation étend la garantie légale des produits de 6 mois à 2 ans. Durant cette période, le consommateur sera protégé des éventuelles défaillances du produit qu'il aura acheté, sans avoir à prouver que la défaillance technique n'est pas liée à l'usage qu'il en a fait. »[147]

Avec la loi Consommation, les indications géographiques, qui existaient déjà pour les produits naturels, agricoles ou viticoles (AOC), sont étendues aux produits manufacturés, comme la porcelaine ou la dentelle. L'objectif est d'apporter une garantie sur l'origine géographique et la qualité du produit au consommateur, de contribuer à préserver les patrimoines artisanaux et industriels locaux et à redynamiser les territoires, en incitant à la relocalisation. Les professionnels doivent déposer un dossier à l'INPI pour obtenir une indication géographique. »[133]

Dans le commerce, il existe le droit de rétractation. Le consommateur a le droit de ne pas justifier le motif et à ne pas payer de pénalités, à l'exception, le cas échéant, des frais de retour.

Le consommateur peut déroger à ce délai au cas où il ne pourrait se déplacer. Actuellement le consommateur dispose d'un délai de 14 **jours** pour se rétracter. Cette faculté de rétractation doit être **mentionnée** sur le contrat. « La loi Consommation permet au consommateur de bénéficier d'un temps de réflexion plus long suite à une commande en ligne. Le délai de rétractation est désormais de 14 jours, contre 7 aujourd'hui. »[176] Si cette possibilité n'est pas mentionnée dans le contrat de vente, le délai est prolongé à **3 mois.**

Les droits de restriction ne s'appliquent pas dans les cas suivants :

- Biens personnalisés, objets portant une gravure personnalisée
- Vente conclue pendant une enchère publique
- Service de restauration et activité loisir

- Objets d'hygiène ou sanitaires
- Logiciels informatiques ayant été ouverts

Le consommateur a toujours la possibilité d'effectuer son droit de rétractation en envoyant une lettre en recommandé avec accusé de réception. Dans le cas où le professionnel a manqué de donner l'information, le délai est prolongé de 12 mois.

Depuis le 1er juillet 2015, les majorations sur les sommes dues sont à charge du professionnel à l'expiration du délai de 14 jours ou de la récupération du bien sont :

Au plus 10 jours : 4,29%

Entre 10 et 20 jours : 5%

Entre 20 et 30 jours : 10%

Entre 30 et 60 jours : 20%

Entre 60 et 90 jours : 50%

Il existe plusieurs **articles sur les obligations du vendeur** dans le Code civil (article 1603) [54].

La première obligation du vendeur est **l'obligation de délivrance**, c'est-à-dire qu'il **doit délivrer l'objet du contrat**, en la mettant à disposition de l'acheteur. Délivrance ne signifie pas livraison ; sauf disposition particulière dans le contrat, c'est à l'acheteur de venir retirer l'objet, et non au vendeur de le livrer.

De la part du vendeur, il existe une obligation de garantie légale [55]. Cette garantie légale est obligatoire, gratuite et illimitée dans le temps. La loi Consommation instaure l'obligation pour le professionnel de livrer le bien acheté par internet à la date indiquée dans son offre commerciale. Le professionnel est tenu de livrer au plus tard dans les 30 jours à compter de la commande.

8.2 Conditions de CGV et diverses ordonnances

Les conditions de vente à l'international s'appuient sur des règles différentes, telle que la Convention de Vienne. Cette convention signée en 1980, compte plus de 70 pays signataires. Elle réglemente les échanges des marchandises dans les pays étrangers ainsi que les obligations des vendeurs et des acheteurs. Le droit impose une obligation d'exécution du contrat. Tout non respect à cette obligation entraînera des sanctions [76].

Les exportateurs doivent être très précis sur l'objet du contrat, notamment sur leur quantité, le prix, les conditions de paiement et de livraison, retour, échange…

Dans la grande majorité des systèmes juridiques, l'envoi d'une facture est recommandé. Cette facturation n'a pas de valeur légale et peut être remise en cause lors de négociations. Les conditions générales de vente export (CGV) sont un document établi par l'exportateur.

Les CGV permettent aux entreprises de fixer à l'avance le cadre juridique de leurs rapports commerciaux. Le CGV doit bien définir les sujets suivant :

- Identification de la société
- Conditions générales de vente. Droits et Obligations
- Prix et mode de paiement.

Le montant de l'indemnité forfaitaire pour frais de recouvrement doit figurer dans les conditions de paiement sur la facture ainsi que dans les conditions générales de vente [56].

- Transport / livraison (il est conseillé de définir les engagements du vendeur et de l'acheteur sur les formalités douanières).

- Interdiction de vente des Produits protégés par des droits de propriété industrielle, en dehors du pays où ils ont été livrés ou pour l'exportation.

Le vendeur est tenu envers l'acheteur de deux garanties :

✓ **La garantie légale de conformité**

✓ La garantie légale des vices cachés :

« Lorsque vous achetez un produit, le vendeur (ou le fabricant) doit vous garantir contre ses défauts cachés.» (depuis mars 2015, les conditions générales de vente (CGV) doivent inclure une information sur la garantie et sa mise en œuvre)

La France est bien signataire de la Convention de Vienne mais celle-ci s'applique exclusivement en cas de problèmes liés à la formation du contrat de vente des parties contractantes. L'application de la convention de Vienne dépend entièrement de la volonté des deux parties. Les entreprises peuvent l'exclure totalement ou partiellement [76 ; article 36].

De nombreuses parties du code civil français issu de la loi du 30 Ventôse an XII, devenu par la suite code Napoléon puis code civil, n'ont pas été modifiées depuis plus de deux siècles. Ces règles ont certes été depuis complétées par une jurisprudence abondante.

L'ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations. Au cours de ces vingt dernières années, les projets internationaux d'harmonisation du droit des contrats se sont multipliés :

- Principes Unidroit relatifs aux contrats du commerce

- Principes du droit européen des contrats (PDEC)

- Code Gandolfi, publié en 2000,

- Projet de cadre commun de référence (DCFR) remis officiellement au Parlement européen en 2008,

Les démarches effectuées ont permis de recueillir les observations des professionnels du droit et des acteurs du monde économique qui ont permis au gouvernement d'adopter un texte convenable à la situation.

Il faut remarquer que le style du code civil n'est pas facilement compréhensible pour les citoyens. Ce nouveau texte part d'un vocabulaire contemporain qui est plus lisible pour une grande partie des citoyens tout en conservant sa précision. L'ordonnance propose de simplifier le plan du livre III du code civil en adoptant un plan plus pédagogique. Il est apparu nécessaire de consacrer certains mécanismes juridiques essentiels pour les praticiens. Par exemple, l'ordonnance définit et prévoit le régime juridique de notions bien connues de la pratique. L'ordonnance met également fin à certaines hésitations jurisprudentielles nuisibles à la sécurité juridique, en déterminant par exemple à quelle date se forme le contrat.

L'ordonnance propose également de consacrer dans la loi certains mécanismes issus de la pratique, tels que la cession de contrat ou la cession de dette. Il est prévu d'alléger la procédure des offres réelles, longue et coûteuse, qui permettait de faire obstacle et encore d'assouplir les formalités nécessaires à l'opposabilité de la cession de créance. Le sous-titre intitulé « Le contrat » se subdivise en quatre chapitres :

- Relatifs aux dispositions liminaires ;
- Formation du contrat ;
- Son interprétation ;
- Ses effets ;

Art. 1101 : Le contrat est un accord de volontés entre deux ou plusieurs personnes destiné à créer, modifier, transmettre ou éteindre des obligations. Les articles 1102, 1103 et 1104 énoncent les principes de liberté contractuelle, de force obligatoire du contrat et de bonne foi.

Chacun est libre de contracter ou de ne pas contracter, de choisir son cocontractant et de déterminer le contenu et la forme du contrat dans les limites fixées par la loi. Bien sûr, la liberté contractuelle ne permet pas de déroger aux règles qui intéressent l'ordre public [175]. La loi ou le contrat peuvent prévoir un délai de réflexion, qui est le délai avant l'expiration duquel le destinataire de l'offre ne peut manifester son acceptation.

Les « Contrats sous forme électronique » sont regroupés aux articles 1369-1 à 1369-9. La voie électronique peut être utilisée pour mettre à disposition des stipulations contractuelles ou des informations sur des biens ou services. Les informations qui sont demandées peuvent être transmises par courrier électronique si leur destinataire a accepté l'usage de ce moyen.

La commande, la confirmation de l'acceptation de l'offre et l'accusé de réception sont considérés comme reçus lorsque les parties auxquelles ils sont adressés peuvent y avoir accès. Un avis de réception peut être adressé à l'expéditeur par voie électronique ou par tout autre dispositif lui permettant de le conserver. La remise d'un écrit électronique est effective lorsque le destinataire en a accusé réception.

8.3 Validité des contrats et durée de conservation

D'après l'ordonnance, il faut satisfaire trois sujets pour la validité du contrat. Ces trois sujets sont : [47]

- Consentement des parties ;
- Leur capacité de contracter ;
- Un contenu licite et certain ;

La section III est consacrée à la durée du contrat. Cette section est composée de six articles. L'ordonnance propose donc d'introduire dans le code civil des règles sur la durée du contrat, ainsi que renouvellement, prorogation et tacite reconduction. La durée de conservation des contrats ainsi que des données est très importante dans la protection de la vie privée.

Art. 1211 : Lorsque le contrat est conclu pour une durée indéterminée, chaque partie peut y mettre fin à tout moment, sous réserve de respecter le délai de préavis contractuellement prévu.

Surtout en mettant fin au contrat indéterminée, il faut respecter un délai de préavis. Lorsque le contrat est à une durée déterminée, chaque partie doit l'exécuter jusqu'à son terme. Nul ne peut exiger le renouvellement du contrat. Il est tout à fait possible qu'un contractant cède sa qualité de partie au contrat à un tiers, le cessionnaire, avec l'accord de son cocontractant. La cession doit être constatée par écrit, sous peine de nullité [50].

Le terme DUA est le plus employé dans les services d'archives publiques : Durée d'Utilité Administrative. C'est une « durée légale ou pratique pendant laquelle un document est susceptible d'être utilisé par le service producteur ou son successeur, au terme de laquelle est appliquée la décision concernant son traitement final. Le document ne peut être détruit pendant cette période qui constitue sa durée minimale de conservation » [7 ; 260-261]. Les règles applicables de conservation des archives des données sont fixées par la loi en fonction des délais de prescription applicables ou des contrôles à effectuer.

Délais de conservation des documents civils et commerciaux :

- **Contrats conclus entre commerçants et entre commerçants et non-commerçant /5 ans (Article L. 110-4 du Code de commerce)**

- **Contrats d'acquisition et de cession de biens immobiliers et foncier /30 ans. (Article 2272 du Code civil)**

- **Correspondance commerciale (bons de commandes, bons de livraison, etc.)/10 ans à compter de la clôture de l'exercice comptable (Article L. 123-22 alinéa 2 du Code de commerce)**

- **Documents bancaires (relevés bancaires, talons de chèque, etc.) 5 ans (Article L. 110-4 du Code de commerce)**

- **Documents établis pour le transport de marchandises /5 ans (Article L. 110-4 du Code de commerce)**

- **Factures clients et/ou fournisseurs/10 ans à compter de la clôture de l'exercice comptable (Article L. 123-22 alinéa 2 du Code de commerce)**

- **Contrat conclu par voie électronique, pour une somme égale ou supérieure à 120 euros, le délai de conservation est de 10 ans à compter de la conclusion du contrat lorsque la livraison du bien ou l'exécution de la prestation est immédiate.**

Quant à la sanction, l'absence de tenue, la destruction avant les délais prescrits ou le refus de communiquer les documents soumis au droit de communication sont punis d'une amende de 1 500 euros [61]. Pour garantir une conservation correcte des documents, des contrats sont conclus. Il existe des services d'archivage qui peuvent effectuer deux types de missions:

- La prestation de conseil liée à l'externalisation

- La mission de conseil en organisation pour la conservation des archives en interne

Chaque entreprise a ses propres particularités qui dépendent de son activité et des types de documents à conserver. La durée de conservation est fixée par la législation ou la réglementation.

La « durée de conservation » est indiquée par les textes réglementaires, des lois nationales, européennes ou des besoins internes si le document n'est soumis à aucun délai spécifique. La conservation des documents correspond à un besoin précis : dans les discours, on utilise souvent le terme « archivage » au lieu de « conservation ». Ces deux termes ont une portée juridique différente :

Conserver : il s'agit de maintenir intacts les documents et de les préserver de toute altération, modification ou destruction, à des fins juridiques. Dans ce cadre, la conservation doit se conformer à certaines règles.

Les archives [58]« sont l'ensemble des documents, quels que soient leur date, leur lieu de conservation, leur forme et leur support, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité ».

Le responsable du traitement liste les durées de conservation envisagées dans les différentes catégories de données et va présenter l'ensemble au C.I.L. ou le chargé de la protection des données. Le C.I.L. recherche des textes réglementaires de la CNIL en rapport avec la finalité du traitement présenté. Si de tels textes existent, il compare les durées de conservation qu'ils recommandent. Au contraire, si aucun texte normatif n'est trouvé, il détermine lui-même des valeurs proportionnées à la finalité.

En cas d'écart entre les durées préconisées par la CNIL (ou celles qu'il a lui-même définies) et celles présentées dans le projet, le C.I.L. invite le chargé de projet à justifier ses choix ou à les amender. Malheureusement, les durées de conservation ne font pas, aujourd'hui, partie des informations qui doivent être fournies aux personnes concernées.

Les données à caractère personnel peuvent être collectées et traitées pour la poursuite de plusieurs finalités. Une même donnée peut figurer dans plusieurs traitements au sein d'une même entreprise. Selon la loi, cette donnée pourra par conséquent être soumise à des durées de conservation différentes au regard de la finalité des traitements.

Au-delà de la durée nécessaire à la finalité du traitement les données, elles peuvent encore être conservées en vue de respecter des durées de conservation particulières (conservation des documents comptables et pièces justificatives, archivage des contrats électroniques B to C, etc.).

Un même document (papier ou électronique) peut être soumis à des durées de conservation différentes.

✓ **Les factures doivent être conservées pendant 5 ans en tant que preuve d'un contrat avec un particulier,**

✓ **6 ans en tant que pièce justificative dans le cadre de la déduction de T.V.A.**

✓ **Au moins 10 ans en tant que pièce comptable et document commercial.**

Le responsable de traitement est responsable des données à caractère personnel qu'il collecte. La durée de conservation dépend de la fonction de la finalité du traitement. Le responsable de traitement est obligé de gérer plusieurs durées suivant les catégories de données. La CNIL précise que les durées de conservation doivent être définies de manière adéquate pour chaque catégorie de données. La CNIL souhaite que le responsable du traitement procède à des procédures d'archivage distinctes suivant « les catégories de données ». La Commission distingue trois catégories de données :

- les données d'utilisation courantes, « les données concernant un client dans le cadre de l'exécution d'un contrat ».

- En second lieu, les données intermédiaires « qui présentent encore pour les services concernés un intérêt administratif et dont les durées de conservation sont fixées par les règles de prescription applicables », par exemple en cas de contentieux.

- Enfin, les données définitives « présentant un intérêt historique, scientifique ou statistique justifiant qu'elles ne fassent l'objet d'aucune destruction »[29].

Sur la sécurité des données archivées, la Commission recommande, s'agissant des archives intermédiaires ou des archives définitives, un accès limité. Également, l'accès aux archives définitives ne devrait être possible que par un « accès distinct. »

En outre, la CNIL recommande, pour des données sensibles relevant de l'article 8 de la loi « Informatique et Libertés », des procédés d'anonymisation. Certaines données peuvent être conservées pour plusieurs finalités ou raisons légales : lutte anti blanchiment, recours des tiers ou des héritiers et ayants droits….

Si le responsable de traitement souhaite conserver les données au-delà du besoin justifié par la finalité du traitement, il peut indiquer la durée de conservation sur sa déclaration.

Le responsable de traitement ne peut communiquer que les données à caractère personnel qu'il a conservées. Lors de la déclaration CNIL du traitement, le responsable mentionne une durée de conservation des données qu'il doit respecter. Dans ce cadre, seules les archives courantes et intermédiaires sont soumises au droit d'accès. La CNIL recommande de mettre en œuvre des dispositifs de traçabilité des consultations des données archivées. Le droit à l'oubli des personnes garantit à une personne physique de ne pas voir ses données à caractère personnel conservées par une société pendant des durées qui pourraient être excessives.

L'adaptation du droit aux technologies de l'information et de la communication vise les écrits électroniques sans tenir compte des préoccupations relatives aux durées de conservation applicables. Pendant l'archivage, on devra respecter les durées de conservation prescrites par les textes en fonction de la nature et du statut juridique du document concerné. **Les durées recommandées par la CNIL concernent généralement les archives courantes (cf. définitions) mais pas les archives intermédiaires. Les durées de conservation de celles-ci peuvent être fournies par les juristes.**

8.4 Contrat en ligne et données personnelles

Les contrats en ligne doivent être réglementés pour que les droits de consommateur soient défendus. L'offre doit être déterminée et claire. Les conditions du droit commun des contrats ont dû être précisées par des textes spécifiques. En général, le contrat de vente en ligne ne correspond à aucun standard et ses conditions spécifiques sont assez fréquentes.

L'offre peut concerner la France comme les autres pays de l'union Européenne ou les pays tiers. Dans ce cas, on voit apparaître dans des contrats le « lieu d'ouverture de l'offre ». Le contrat de vente en ligne de France, par exemple, mentionne que « les offres ne sont valables qu'en France Métropolitaine. »

Il existe deux façons de conclure un contrat en ligne :

- La première : conclure un contrat à travers un échange de courriers électroniques entre les deux parties [51]

- La deuxième : utiliser un formulaire au moyen d'une interface web sur laquelle le client pourra s'identifier. Ce formulaire lui permettra de cocher une case par laquelle il accepte les conditions du contrat [52]. (Voir notamment l'article 1369-3 du Code civil). Le fait de cocher cette case a valeur de signature manuscrite.

Les conditions de l'offre dans le contrat de vente en ligne ne sont pas différentes du droit commun. Le message affiché sur le site commercial doit contenir tous les éléments nécessaires à la conclusion d'un contrat. C'est-à-dire le produit où son prix doit être bien défini.

Dans le contexte d'Internet, les échanges sont multipliés, instantanés et internationaux. En considérant les spécificités de l'Internet et du commerce électronique, le législateur a la responsabilité de poser une réglementation adaptée à l'offre en ligne.

Une offre en ligne peut être retirée une fois acceptée et le contrat est formé. La concurrence oblige les sites marchands à innover et à proposer toujours plus de produits nouveaux. La jurisprudence admet que l'offre doit être maintenue pendant un certain temps qui va donner au consommateur les moyens d'exercer ses droits.

La Loi pour La Confiance en l'Economie Numérique de 2004 intègre un nouvel article concernant la validité de l'offre. D'après cet article, sans préjudice des conditions de validité mentionnées, l'auteur du site reste engagé tant qu'elle est accessible par voie électronique de son fait.

Le commerçant des produits en ligne s'adresse à un ou plusieurs consommateurs du monde entier. Dans ce contexte, il faut prendre en considération des règles à la vente internationale de marchandises. Ainsi, on considère toujours la Convention de Vienne de 1980 sur les contrats de vente Internationale de marchandises et le projet « Electronic Agreement » élaborée par la Commission Economique des Nations-Unies pour l'Europe.

Le contrat de vente en ligne se définit comme un contrat à distance, entre absents. L'internaute, du fait de la législation, dispose d'un certain nombre d'informations obligatoires pour savoir avec qui il contracte, et le vendeur vise un public national ainsi qu'international. Certaines marchandises peuvent être commercialisées en ligne sans restriction majeure, mais certaines sont considérées « à risque » et peuvent faire l'objet de restrictions. Tout ne peut être vendu sur Internet. L'article 1128 du code civil concrétise la vente de ce qui est hors commerce.

En France, l'internaute français a la possibilité d'avoir accès sur le web à des produits de toutes origines. Un vendeur va pouvoir mettre en ligne un produit licite dans son pays d'origine mais considéré comme illicite (ou hors commerce) dans d'autres pays du monde. Si le site du vendeur est hébergé en France, la loi française sera appliquée. Par conséquent, les informations et l'offre notamment doivent être en français, conformément à la loi [135].

La loi du 4 août 1994 relative à l'emploi de la langue française impose des mesures sur des domaines différents : quelle que soit l'origine des produits ou services, le mode d'emploi, la garantie ou la publicité doivent être réalisés en français.

Cependant, beaucoup de sites fournissent des informations en anglais pour viser un plus large public. A ce propos, la loi de la langue française prévoit dans son article 4 une possibilité de traduction en langue française. Selon l'article 4 de la directive de 1997 sur les contrats à distance, les informations suivantes doivent être fournies :

- Noms et prénom du vendeur/ personne physique,
- Raison sociale s'il s'agit d'une personne morale, son numéro d'immatriculation, adresse, numéro de téléphone,
- Prix du produit ainsi et frais de livraison et mention de taxes

La directive sur le commerce électronique, transposée en droit français par la Loi pour la Confiance en l'Economie Numérique, prévoit un accès direct aux informations. Le commerce dit B to C doit respecter les règles protectrices des consommateurs applicables aux contrats à distance. Ces règles sont issues du droit interne ainsi que des conventions de Rome relatives à la loi applicable aux contrats.

8.5 Sécurité de paiement

Certains sites ont un logo « Verified by Visa » ou « Mastercard SecureCode ». Ce logo indique que le site possède un système de sécurité appelé 3D Secure : après quelques informations nécessaires, on se retrouve sur une page site Internet de notre banque ou d'un prestataire de paiement. Dans ce cas, on doit confirmer l'identité en fournissant de nouvelles données : Date de naissance, code unique envoyé par mail ou SMS. Pour plus de sécurité, plusieurs consommateurs utilisent le système de Carte Bleue. Le service e-Carte Bleue est un service rattaché à la carte bancaire pour que les consommateurs règlent par carte à distance sans avoir à transmettre les coordonnées de carte bancaire réelle. Ce système génère un numéro

de paiement à usage unique à utiliser sur le site choisi ; Le code secret à 4 chiffres de la carte bancaire ne sera jamais demandé sur Internet. Seuls les sites frauduleux le demanderont.

Certains sites marchands stockent le numéro de carte bancaire lors du premier paiement, il est recommandé de ne pas utiliser ces sites. En aucun cas le cryptogramme visuel de la carte bancaire ne doit être enregistré. On doit recevoir un e-mail récapitulatif de la commande juste après le paiement. Surtout il faut s'assurer que les coordonnées bancaires ne sont pas conservées sur le site marchand.

En général, le consommateur peut autoriser que ses données soient transmises dans un État tiers, notamment en dehors de la Communauté européenne. La Loi pour la Confiance en l'Economie Numérique définit que toute manifestation de volonté est libre par laquelle une personne accepte que des données à caractère personnel la concernant soient utilisées à des fins de prospection directe. Plusieurs options sont possibles pour que le vendeur obtienne le consentement :

- En utilisant la méthode dite de « l'opt-in », les données n'étant envoyées que si le consommateur coche la case à cet effet.

- Téléphoner à la personne et lui demander expressément si elle autorise le transfert de ses données dans un pays tiers.

La facilité de transfert avec Internet met en avant les risques de sécurité de transfert dans les différents pays du monde. La directive européenne de 1995 transposée en droit français par la loi de 2004 fait obligation aux États membres de veiller à ce que les transferts de données personnelles vers un pays tiers n'aient lieu que si ce pays assure un niveau de protection « adéquat ».

Le consommateur doit être informé du traitement de sa demande pour qu'il ne fasse pas un consentement automatique. D'après la CNIL, le consommateur ne doit pas se retrouver engagé dans un contrat en cliquant simplement sur quelque lien. Pour cette raison, il est demandé de faire des formulaires de contrat licite et explicite. En général, le consommateur doit avoir un formulaire récapitulatif à la fin de la commande pour savoir de quoi est faite la transaction en ligne.

Selon l'article 1109 du code civil, le consentement du consommateur doit être libre. Sinon il va être considéré comme provoqué par des démarches frauduleuses et ce qu'on appelle le dol [48]. Le contrat pourrait être annulé si l'acheteur prouve qu'il a été victime de dol ou de violence.

Tout fichier ou traitement automatisé contenant des informations à caractère personnel doit être déclaré avant sa création, en ligne ou par courrier adressé à la Commission nationale de l'informatique et des libertés (CNIL). Les données à caractère personnel relatives aux clients ne peuvent être conservées au-delà de la durée strictement nécessaire à la gestion de la relation commerciale. Conformément aux dispositions en vigueur, il convient de prévoir à cet effet une base de données d'archives dédiée ou une séparation logique dans la base de données active, après avoir opéré un tri des données pertinentes à archiver [34].

Pour pouvoir conserver, au-delà de la durée de conservation fixée au regard de l'article 6.5 de la loi, des informations relatives à des clients ou des prospects, les données doivent être anonymisées de manière irréversible [33].

8.6 Rachat des fichiers contenant des données à caractère personnel

Quand une entreprise souhaite acheter un fichier de clients contenant des données à caractère personnel, elle doit s'assurer de la conformité des fichiers avec les exigences de la loi Informatique. Après l'achat, l'entreprise est soumise à des obligations en matière de protection des données personnelles.

La vérification auprès de la CNIL est obligatoire. A défaut d'accomplir cette formalité, la cession pouvait en effet être frappée de nullité. Une ancienne entreprise doit avoir la preuve de la déclaration du fichier auprès de la CNIL ou de son inscription au registre du Correspondant Informatique et Libertés (CIL). Les personnes concernées par le traitement doivent être informées et leur consentement recueilli. Ainsi, le responsable d'un traitement a l'obligation d'informer les personnes dont les données personnelles sont collectées.

Le responsable d'un traitement de données à caractère personnel qui n'a pas recueilli les données personnelles directement auprès des personnes a toujours l'obligation d'information en présence d'une collecte indirecte de données personnelles.

Lorsque les données personnelles ne sont pas collectées auprès des personnes mais auprès de tiers, la collecte est indirecte. En effet, dans la loi, on précise que « lorsque les données à caractère personnel n'ont pas été recueillies auprès de la personne concernée, le responsable du traitement ou son représentant doit fournir à cette dernière les informations énumérées dès l'enregistrement des données »[130]

La loi Informatique et Libertés prévoit que les modifications des fichiers doivent être portées à la connaissance de la CNIL.

La chambre sociale de la Cour de cassation a rappelé [81] qu'une mise à jour d'un logiciel de traitement de données à caractère personnel n'entraîne pas cette obligation.

Tout fichier ou traitement automatisé contenant des informations à caractère personnel doit être déclaré avant sa création, en ligne ou par courrier adressé à la Commission nationale de l'informatique et des libertés. La forme déclaration peut être :

- **Déclaration normale** pour les fichiers qui concernent la vie privée ou les libertés individuelles des personnes : fichiers de clients, gestion des horaires des salariés, géolocalisation des véhicules utilisés par les salariés

- **Déclaration simplifiée** pour les fichiers qui ne portent pas atteinte à la vie privée et aux libertés individuelles des personnes. Les sites commerciaux de vente en ligne de biens ou de services, qui collectent des informations nominatives (nom, courriel) pour constituer des fichiers des clients.

L'entreprise qui détient des données personnelles doit informer la personne concernée : de l'identité du responsable du fichier, de la finalité du traitement des données, du caractère obligatoire ou facultatif des réponses, des droits d'accès, de rectification, d'interrogation et d'opposition et des transmissions des données.

Un commerçant en ligne par exemple doit respecter certaines obligations :

- Informer les clients de leur droit d'accès, de modification et de suppression des informations collectées

- Indiquer une durée de conservation des données

- Indiquer l'objectif de la collecte d'informations

“Pour pouvoir conserver, au-delà de la durée de conservation fixée au regard de l’article 6.5 de la loi, des informations relatives à des clients ou des prospects à des fins d’analyses ou d’élaboration de statistiques agrégées, les données doivent être anonymisées de manière irréversible, en procédant à la purge de toutes les données à caractère personnel, y compris les données indirectement identifiantes. A cet égard, le G29 a adopté un avis le 10 avril 2014 sur les techniques d’anonymisation. » [34]

8.7 Conclusion

La Loi pour La Confiance en l’Economie Numérique de 2004 intègre un nouvel article concernant de la validité de l’offre. D’après cet article, sans préjudice des conditions de validité mentionnées, l’auteur du site reste engagé tant qu’elle est accessible par voie électronique de son fait.

Le commerçant des produits en ligne s’adresse à un ou plusieurs consommateurs du monde entier. Dans ce contexte, il faut prendre en considération des règles à la vente internationale de marchandises. Dans ce contexte, on considère toujours la Convention de Vienne de 1980 sur les contrats de vente internationale de marchandises et le projet « Electronic Agreement » élaboré par la Commission Economique des Nations Unies pour l’Europe. Le consommateur peut autoriser que ses données soient transmises dans un État tiers, notamment en dehors de la Communauté européenne. La Loi pour la Confiance en l’Economie Numérique définit que toute manifestation de volonté est libre par laquelle une personne accepte que des données à caractère personnel la concernant soient utilisées à des fins de prospection directe

Chapitre 9

Le niveau de la protection de la vie privée en Géorgie

Dans ce chapitre nous étudions la situation de la Géorgie, petit pays caucasien post-soviétique. La Géorgie accumule des difficultés économiques et subit des guerres de sécession. Elle est considérée comme faisant culturellement, historiquement et politiquement partie de l'Europe. L'institution chargée de veiller à la protection des données personnelles contenues dans les fichiers et traitements informatiques ou papiers, a été fondée trente-cinq années après son homologue français.

9.1 Introduction

C'est seulement en 2013 que la Géorgie s'est dotée d'une nouvelle autorité gouvernementale chargée de protéger le droit de la vie privée. Des centaines de personnes étaient contrôlées et surveillées systématiquement par le ministère de l'Intérieur sans aucun contrôle judiciaire et plusieurs centaines de personnes étaient arrêtées à cause de la surveillance illégale. Tamar Kaldani, qui avait déjà dirigé les programmes de bonne gouvernance et de droits de l'homme à la Fondation *Open Society Georgia* a été choisie pour diriger cette nouvelle institution gouvernementale.

Bien évidemment, cette institution, qui a été fondée 35 ans après son homologue français, ne possédait pas de grande expérience mais elle avait l'intention d'assumer sa responsabilité et de défendre les droits de l'homme et la vie privée. Cette autorité a des fonctions bien définies :

- Le Bureau de l'inspecteur de la protection des données à caractère personnel de la Géorgie consultait les citoyens, les organisations privées et publiques sur les questions liées à la licéité du traitement et de la protection des données à caractère personnel ;
- Le Bureau étudie des plaintes des citoyens et prend les mesures prescrites par la loi. L'inspecteur a le droit de demander des renseignements supplémentaires et d'inspecter le responsable du traitement

- Demande une cessation temporaire ou définitive du traitement des données ;
- Demande l'effacement, la destruction des données ;
- Demande la clôture du flux de données transfrontalières ;
- Fournit des recommandations au contrôleur de données ;
- Impose une responsabilité administrative au responsable du traitement des données ;
- **Le bureau de l'inspecteur de la protection des données à caractère personel est nommé par le service de l'inspecteur de l'État en 2019.** Le service de l'inspecteur de l'État a un pouvoir de surveillance du traitement des données dans le secteur de la police, pouvoir qui a été confié à l'inspecteur conformément aux engagements internationaux. « Le groupe de travail a été créé pour mettre en œuvre la décision de la Cour constitutionnelle du 14 avril 2016. Le service de l'inspecteur de l'État est une autorité indépendante de l'État qui, en tant que successeur légal de l'Office de « the Personal Data Protection Inspector », opère en Géorgie depuis le 10 mai 2019. » Ses activités sont les suivantes :

- Surveillance de la légalité du traitement des données à caractère personnel ;

- Surveillance des actions et les activités d'enquête secrètes ;

- Enquête sur les crimes graves commis par un représentant des autorités chargées de l'application de la loi ; ou par un fonctionnaire ;

La décision de l'inspecteur de la protection des données est exécutoire et peut faire l'objet d'un recours devant la Cour, conformément aux procédures. L'inspecteur de l'État contrôle la légalité du traitement des données de sa propre initiative ou sur la base d'une plainte des citoyens. L'inspecteur peut examiner la conformité du système de classement, des enregistrements de la divulgation de données à caractère personnel avec les exigences légales établies et la légitimité du transfert de données vers des pays étrangers. Au cours de l'inspection, l'inspecteur a le droit de demander des documents à toute personne physique ou morale, y compris des renseignements portant sur le secret commercial et professionnel, ainsi que des documents reflétant les activités de recherche opérationnelle et les enquêtes criminelles classées comme secret d'État et nécessaires à l'inspection. Le responsable du traitement des données est tenu de fournir à l'inspecteur les informations et documents nécessaires immédiatement ou dans les 10 jours au plus tard si la demande le requiert : **L'inspecteur a le droit d'inspecter toute organisation et d'avoir accès aux informations quel que soit leur contenu et leur forme de stockage [177].**

Bureau de l'Inspecteur de l'État a l'ambition de sensibiliser le public et d'informer les citoyens sur leurs droits et obligations. Ils organisent régulièrement des formations et des réunions d'information sur les questions liées à la protection des données personnelles. Le Bureau coopère avec différents centres de formation et établissements d'enseignement, comme le Centre de formation de la justice, et d'autres organisations publiques et privées. Le Bureau de l'inspecteur d'État coopère avec les organisations internationales et les autorités de protection des données des autres pays. Cette Institution représente la Géorgie au sein du Comité consultatif du Conseil de l'Europe de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD) et du Bureau du Comité. **A partir de 2014, le Bureau de l'Inspecteur de l'État est membre des Autorités de Protection des Données du Centre et de l'Est (CEEDPA) et de la Conférence européenne des Autorités de Protection des Données.**

En 2015, le Bureau a été accrédité comme membre de la Conférence internationale des commissaires à la protection des données et de la vie privée (ICDPPC) et est devenu membre du Réseau mondial d'application des lois sur la protection des renseignements personnels (GPEN).[155 : 2015]

Pour augmenter la productivité de l'institution, il est divisé en départements :

- Département juridique

Le service juridique traite les plaintes des citoyens et organise des consultations auprès des responsables du traitement des données, des personnes chargées du traitement des données et des personnes

concernées. Ce service prépare des documents analytiques sur les questions liées à la protection des données à caractère personnel sur la base de l'expérience internationale.

- Département des inspections

Le département des inspections est responsable de la vérification de la légitimité du traitement des données par la planification, l'organisation et la conduite des inspections. Le Ministère met en œuvre la méthodologie d'inspection basée sur les normes internationales, assure une surveillance efficace des organismes chargés de l'application de la loi, surveille la mise en œuvre des normes de sécurité de l'information tout en traitant les données personnelles, met en œuvre des projets pour améliorer la protection des données et les normes de sécurité.

- Département des relations internationales

Le Département est chargé de coordonner les relations internationales du Bureau de l'Inspecteur de la protection des données personnelles et de représenter le Bureau au niveau international et national, ainsi que de mener des activités d'éducation, de recherche et d'analyse de la pratique internationale.

- Administration

L'Administration fournit un soutien administratif au Bureau de l'Inspecteur.

Les principales fonctions de cette division sont : fournir un appui organisationnel, logistique et technique au Bureau. Inscrire et systématiser les actes juridiques individuels de l'inspecteur ; Gérer les archives du Bureau.

- Département IT

Le service informatique a été créé en 2015. Les principales fonctions du Département sont les suivantes : Surveillance technique, administration et gestion du système électronique interne de contrôle des activités d'investigation dissimulées - écoutes téléphoniques et enregistrement.

D'Après le rapport annuel de l'inspecteur des données, « l'année 2015 était très importante en raison de la mise en œuvre de la législation sur la protection des données personnelles et du développement des pratiques judiciaires ; l'activation du système de supervision sur les activités d'enquête liées aux écoutes téléphoniques et aux données informatiques et l'augmentation des plaintes des citoyens. »

9.2. Les missions de Service de l'inspecteur d'État et statistiques

En 2015, le Bureau de l'Inspecteur de l'État est devenu membre des syndicats des Autorités internationales et européennes de protection des données ; il a été représenté au sein du comité et bureau spéciaux du Conseil de l'Europe, qui a mené des travaux intensifs sur la modernisation de la Convention du Conseil de l'Europe et du Règlement général sur la protection des données de l'Union européenne.

L'accès des organisations à de grands volumes de données personnelles ou à des informations périmées crée certains obstacles pour les citoyens dans l'obtention de différents services et l'exercice de leurs droits ; dans certains cas, en raison d'un dossier de condamnation passé ou d'une divulgation de données sur la santé, plusieurs citoyens ont été soumis à certains traitements discriminatoires.

Dans le secteur public, la duplication de bases électroniques contenant des données personnelles a été multipliée. Par exemple, dans plusieurs organisations, plusieurs copies d'une seule et même base de données électroniques sont conservées.

En 2015, le Ministère de l'Intérieur de la Géorgie a réglementé les cas de l'accès des employés aux ressources d'information du Ministère ; il a fixé des délais pour le stockage, la suppression et l'archivage des données à caractère personnel dans les systèmes de classement du Ministère. Le contrôle de l'accès légal des employés aux bases de données est devenu plus strict. L'accès aux ressources d'information archivées n'est autorisé que sur la base d'une demande écrite bien raisonnée.

Le Ministère de l'Intérieur de la Géorgie a interjeté appel de la décision de l'inspecteur au tribunal de la ville de Tbilissi ; le motif de l'appel était que, en raison de l'accès hors service aux données des citoyens, l'employé du ministère a reçu un avertissement strict et, par conséquent, le ministère n'était pas censé être imposé d'une responsabilité administrative supplémentaire. Le tribunal (affaire N4 / 563515) n'a pas partagé la position du ministère et a confirmé la décision de l'inspecteur.

Statistiques des rapports annuels de Géorgie :

Fig. 13 : Nombre de plaintes dans les années 2013 - 2018, Source https://personaldata.ge/en [155]

Fig. 14 : *Nombre de demandes de conseils dans les années 2013 - 2018, Source rapports annuels du Bureau de l'inspecteur d'État, https://personaldata.ge/en* [155]

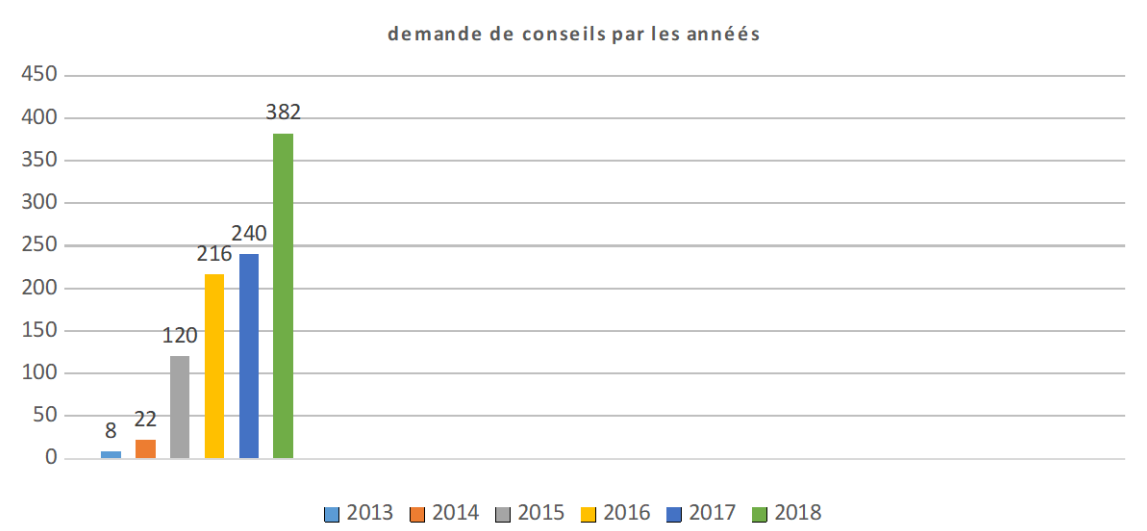


Fig. 15 : *Nombres de contrôles menés par le bureau dans les années 2013 - 2018, Source rapports annuels du Bureau de l'inspecteur d'État, https://personaldata.ge/en* [155]

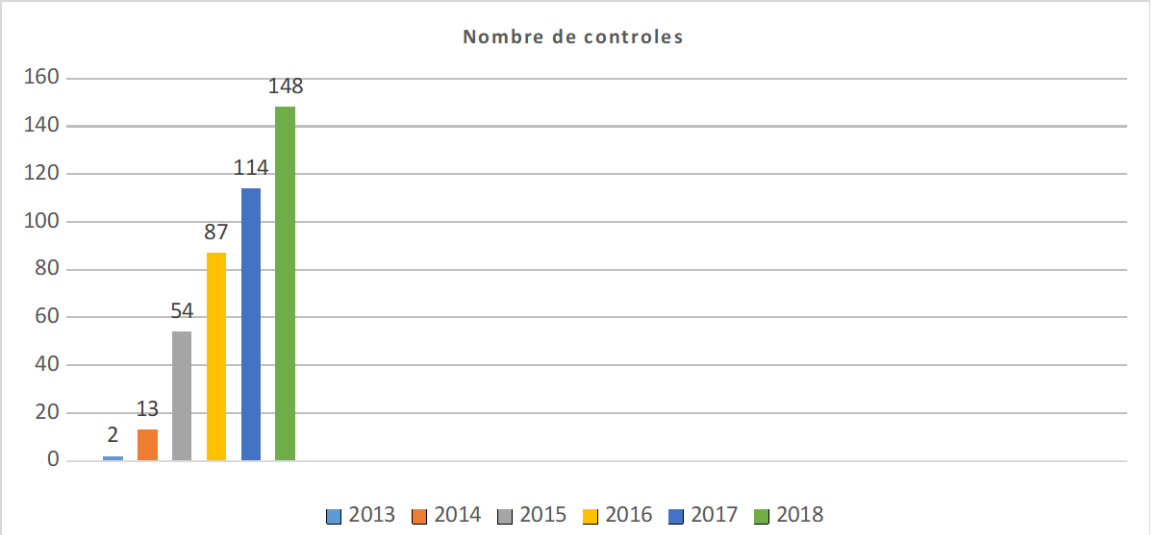


Fig. 16: *Nombre de sanctions dans les années 2013- 2018, Source rapports annuels du Bureau de l'inspecteur d'État, https://personaldata.ge/en* [155]

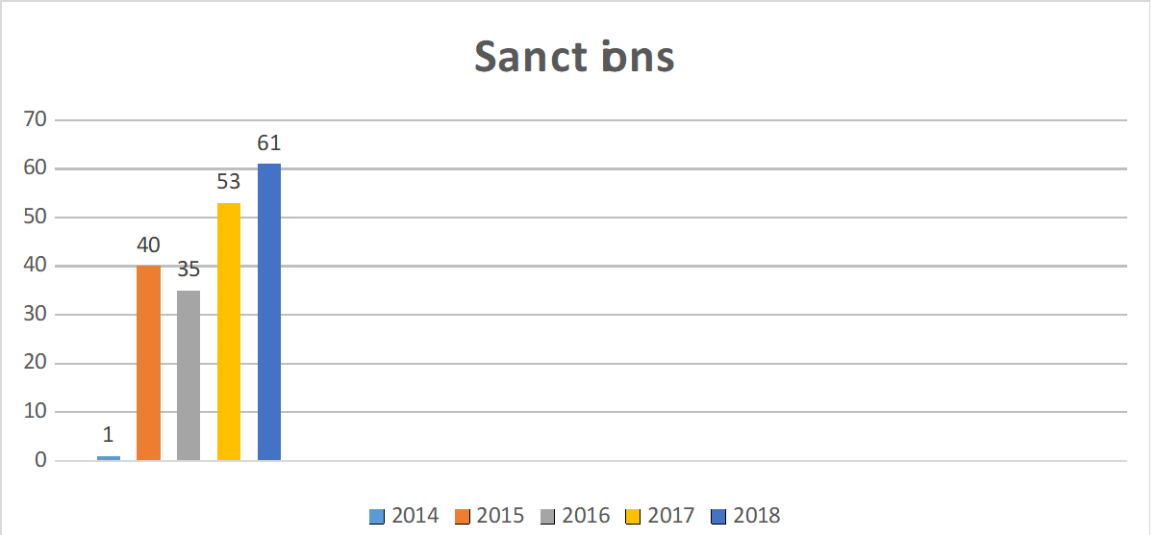
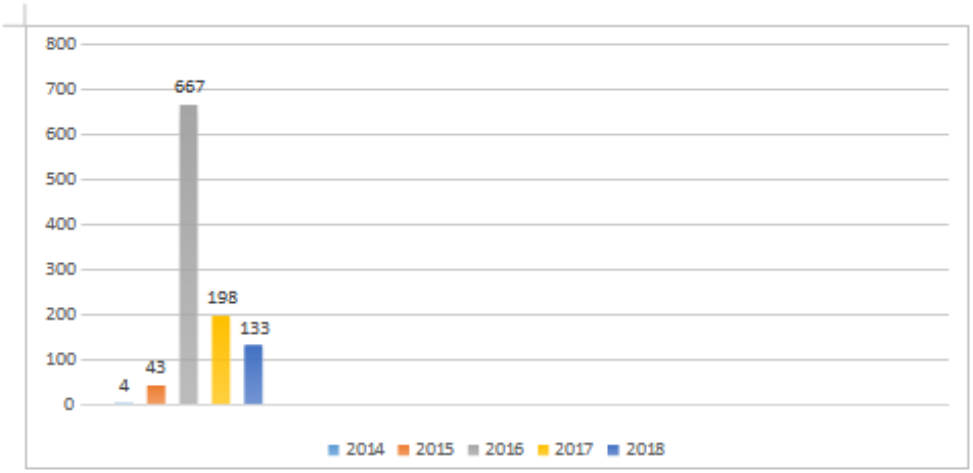


Fig. 17 : *Nombre de consultations dans les années 2013 - 2018, Source rapports annuels du Bureau de l'inspecteur d'État, https://personaldata.ge/en* [155]



Les activités du Service de l'Inspecteur d'État augmentent chaque année. Au total, le Bureau a effectué 115 inspections entre le 1er juillet 2013 et le 1er juillet 2016. Parmi celles-ci, on compte 58 institutions publiques et 904 unités de 57 organisations privées. Des violations ont été révélées dans 155 cas. De plus, le Bureau de l'inspecteur a fourni plus de 3 000 consultations et examiné 229 plaintes de citoyens. Une table ronde a été organisée avec l'aide financière de l'UE dans le cadre du programme « Droits de l'homme pour tous » mis en œuvre conjointement par les grandes agences des Nations Unies : le Programme des Nations Unies pour le développement (PNUD), le Fonds des Nations Unies pour l'enfance (UNICEF), le Bureau du Haut-Commissaire aux droits de l'homme (HCDH). L'UE accorde une attention particulière au fait que les mêmes normes de protection des données sont appliquées dans le pays qui bénéficiera du statut de pays sans visa en tant que pays membres de l'UE.

9.3 Etudes des cas et recommandations de l'inspecteur de l'État

Le problème parmi les plus sensibles pour des Géorgiens est le suivant : avec quelques recherches sur différents sites, il est possible d'acquérir des informations très sensibles sur les personnes. Par exemple :

- Au cours du traitement des plaintes, il a été déterminé qu'il était possible de trouver les noms, prénoms et numéros d'identification personnels des personnes qui ont remporté une vente aux enchères liée à la gestion des biens de l'État sur www.privatization.ge. Comme la période de disponibilité de l'information n'est pas déterminée, les données des gagnants des enchères sont publiées pour une période indéterminée. Dans le même temps, la page Web n'a pas de fonctionnalité de protection contre les moteurs de recherche et il est aisé d'obtenir le numéro d'identification personnel en indiquant le nom complet d'un sujet de données dans n'importe quel moteur de recherche.

C'est ainsi le cas lorsqu'il existe une base légitime pour la publication de données à caractère personnel. Par conséquent, l'Office a reçu l'ordre de déterminer la période de disponibilité des données à des fins de publicité,et d'autres fins légitimes, et de mettre en œuvre de telles mesures organisationnelles et techniques qui limitent la disponibilité facile du numéro d'identification personnel de la personne concernée dans le moteur de recherche.

- Deuxième cas globalement inquiétant : l'utilisation du site de la Commission électorale pour des buts différents et souvent discriminants. **Bien que la page Web soit réservée aux électeurs pour vérifier les données de leurs membres de la famille, le site est une source d'informations (**photo, adresse d'inscription et données des personnes inscrites auprès des électeurs à la même adresse) **pour les différents services. La loi n'impose pas de restriction pour le traitement ultérieur des données publiées.**

- Troisième cas : il y a un grand intérêt pour la disponibilité des données dans le registre des personnes morales (non commerciales) et dans la base de données des biens immobiliers de l'Agence nationale du registre public. Selon la législation applicable, la page Web publie les données des propriétaires immobiliers, des gestionnaires et des représentants d'organisations privées, également des documents d'enregistrement d'une organisation, y compris une copie du document d'identité du pétitionnaire. **Il a été déterminé qu'une certaine organisation recueille les données disponibles de la page Web via un algorithme spécial et les publie sur sa page Web sous une forme plus facile d'accès**. En indiquant les données d'identification d'une personne dans les options de recherche, il est possible d'obtenir une information complète liée à une personne. Contrairement à www.napr.gov.ge, cette page Web n'a pas de fonctionnalités limitant l'accès aux moteurs de recherche et l'information devient disponible en indiquant simplement le nom complet d'une personne dans n'importe quel moteur de recherche.

Étant donné que la législation permet l'utilisation des données publiques, aucune violation des règles de traitement des données n'a été constatée. Toutefois, l'organisation a reçu une recommandation pour évaluer les critères d'accès algorithmique des données publiées.

- Conformément au Code des infractions administratives de Géorgie, le Ministère géorgien de l'Intérieur crée une base de données unifiée pour l'enregistrement des infractions administratives. Les données contenues dans la base de données unifiée ont été stockées en permanence. Mais par la décision n° 1/2/622 du 9 février 2017, la Cour constitutionnelle de Géorgie a jugé la norme juridique inconstitutionnelle [155 ; 2018 : 59].

Sur la base des plaintes, l'inspecteur a examiné la question du stockage permanent dans la base de données unifiée (sous forme électronique). Afin de se conformer à la décision de la Cour constitutionnelle, le Ministère travaille à déterminer les délais de stockage des données détenues dans la base de données unifiée.

À la suite de l'examen, l'Inspecteur a constaté que le stockage de données sur l'imposition au plaignant d'une responsabilité administrative à partir du 31 octobre 2007 dans la base de données unifiée du Ministère, après l'entrée en vigueur de la décision de la Cour constitutionnelle (en particulier, depuis le 9 février 2017), **est le traitement des données sans la base juridique envisagée par la loi de Géorgie et contraire aux principes envisagés par cette loi. Par conséquent, le Ministère a reçu l'ordre d'effacer les données relatives à l'imposition de la responsabilité administrative sur la personne concernée à partir de la base de données unifiée ou de les stocker sous une forme qui exclut l'identification de la personne**.

- Une des questions les plus importantes est le rôle de l'inspecteur en surveillance des enquêtes secrètes.

Conformément à la législation géorgienne, l'une des principales fonctions qui incombent à l'Inspecteur est la surveillance des activités d'enquête secrètes et le contrôle des activités menées dans la base de données centrale des données d'identification des communications électroniques.

Tout au long de l'année 2018 et 2019, le Bureau de l'inspecteur a constamment observé le processus d'enquêtes secrètes**. L'analyse du processus indique qu'au cours de la période considérée, le nombre d'activités d'enquêtes secrètes en termes de statistiques a considérablement augmenté par rapport aux années précédentes**. Toutefois, il convient de noter que les enquêtes secrètes sont principalement menées sur la base d'une décision de justice.

- **À la suite de la modification législative de 2017, l'inspecteur a obtenu le pouvoir de suspendre l'interception d'une communication téléphonique** si le Bureau n'a pas reçu de décision de justice ou de résolution du procureur, que ce soit sous forme électronique ou originale, ou si les données contenues dans les résolutions électroniques et originales d'un procureur sont incompatibles, ou si elles contiennent une ambiguïté ou une inexactitude. En 2018, le mécanisme de suspension a été utilisé pour 96 décisions/résolutions.

L'article 1439 du Code de procédure pénale de Géorgie prévoit l'obligation pour le Parquet d'informer la personne faisant l'objet d'activités d'enquêtes secrètes sur la conduite de ses activités, sur le contenu des documents obtenus et la destruction des documents. En 2018, à l'initiative de l'inspecteur, le Parquet de Géorgie a été inspecté afin d'examiner le respect de l'obligation mentionnée. Sur la base d'une sélection aléatoire, l'Office a examiné les activités d'enquête secrètes envisagées en vertu de l'article 1431 du Code de procédure pénale de Géorgie. À la suite de l'inspection, plusieurs faits de violation des principes envisagés par la loi géorgienne et des règles de sécurité des données ont été identifiés. Le Bureau du Procureur a reçu des instructions obligatoires pour s'assurer d'informer correctement les personnes concernées conformément à l'article 1439 du Code de procédure pénale de Géorgie.

En ce qui concerne les renseignements personnels conservés par les institutions publiques, la loi établit le droit d'accès d'une personne à ses données personnelles et d'obtenir des copies de ces données, sauf dans les cas où le paiement d'une redevance est exigé. Le compte rendu du nombre de plaintes soumises au Bureau de l'Inspecteur et de la demande des consultations montre que l'intérêt des citoyens à l'égard de leurs données personnelles conservées par différentes institutions a considérablement augmenté ces dernières années.

Les informations existant sur les documents officiels relatifs à la santé de l'individu, à ses finances ou à d'autres affaires privées ne sont accessibles à personne sans le consentement de la personne concernée, sauf dans les cas déterminés par la loi, lorsque cela est nécessaire pour assurer la sécurité ou la sécurité publique, la protection de la santé, des droits et des libertés d'autrui [74].

Il faut tenir compte du fait que les informations sur le revenu ou la situation financière de la personne constituent des données personnelles. Toutefois, l'information sur les fonctionnaires publics, en raison du grand intérêt du public envers leur rendement et en raison des principes de transparence, est plus ouverte et accessible que l'information sur les autres personnes.

Conformément au Code administratif général de la Géorgie, chaque organisme public est tenu de ne pas divulguer des données à caractère personnel (sans le consentement d'un particulier ou dans les cas prévus par la loi - sans décision judiciaire motivée), à l'exception des fonctionnaires. Par conséquent, le Code administratif général de la Géorgie permet la publication et la divulgation d'informations aux personnes intéressées sur les fonctionnaires, y compris leurs salaires et le montant des primes.

9.4 Données à caractère personnel, la publication des actes judiciaire et statistiques 2019/2020

Il est important que les responsables du traitement des données soient particulièrement prudents en ce qui concerne la publication d'une catégorie spéciale de données, qui relèvent d'une réglementation juridique différente. La publication de données sensibles nécessite le consentement écrit d'un individu et l'organisme administratif est tenu de protéger ces informations contre la divulgation jusqu'à ce que cette personne exprime la volonté de divulguer les informations. Il convient également de mentionner qu'en dépit d'un intérêt public élevé, la législation actuelle ne prévoit pas la possibilité de divulguer certaines catégories spéciales de données, sans leur consentement.

Cependant, la législation permet la divulgation des informations contenant des données personnelles si ces informations sont dépersonnalisées. La dépersonnalisation (anonymisation) des données devrait être

effectuée de telle sorte qu'il soit impossible de les lier à une personne concernée ou nécessiterait des efforts, des coûts et du temps démesurés pour établir un tel lien.

En raison de l'intérêt élevé porté à la question, le Bureau du défenseur public de la Géorgie et le Bureau de l'inspecteur de la protection des données personnelles ont commencé à élaborer des recommandations conjointes. A l'initiative de l'Inspecteur, en décembre 2015, une réunion de travail a eu lieu sur la protection des données personnelles dans le système judiciaire. La réunion a été suivie par les juges des tribunaux suprêmes, des cours d'appel et des membres du personnel judiciaire chargés de la diffusion de l'information publique. La réunion a abordé la question de l'équilibre entre l'accès à l'information publique et la protection des données à caractère personnel, ainsi que la promulgation et la publication des décisions judiciaires. La nécessité d'un règlement pour la publication de la décision du tribunal est devenue très évidente à la réunion. À partir de janvier 2016, à l'initiative de la Cour suprême de Géorgie, un groupe de travail spécial a été créé pour élaborer les règles de publication des décisions judiciaires. Le groupe de travail comprend des membres du Bureau de l'Inspecteur. En ce qui concerne la question de la publication des décisions de justice, les défenseurs des droits pensent que l'équilibre entre l'accès à l'information et les intérêts de la protection des données à caractère personnel doit être maintenu.

Conformément à l'article 28 du Code administratif général de la Géorgie, « l'information publique est ouverte, sauf dans les cas prévus par la loi et considérés comme des données à caractère personnel, des secrets d'État ou commerciaux ».

La procédure d'examen de cas par les tribunaux communs de Géorgie est entièrement réglementée par la législation. Conformément à la loi organique de Géorgie sur les tribunaux communs, toutes les affaires devant les tribunaux sont jugées en séance publique, sauf dans les cas prévus par la loi ; il est évident que les règles de protection des données personnelles ne s'appliquent pas aux procédures judiciaires. Cependant, une fois la décision finale annoncée, l'objet de la procédure judiciaire est accompli et les contrôleurs des données, y compris les tribunaux, sont tenus de se conformer aux normes pertinentes de traitement des données.

Conformément à l'article 2, point a), de la loi de Géorgie sur la protection des données à caractère personnel, la décision judiciaire, qui contient des données sur un individu, représente le document contenant des données à caractère personnel. Les décisions judiciaires qui contiennent des renseignements sur l'appartenance raciale ou ethnique de l'individu, son appartenance politique, ses croyances religieuses ou philosophiques, son appartenance à des syndicats, son dossier médical, sa vie sexuelle, son casier judiciaire, sa détention administrative, sa mise en liberté contiennent également une catégorie spéciale de données.

Le tribunal définit que la publication d'informations qui n'indiquent pas une personne, bien qu'elle permette facilement son identification, doit être considérée comme un traitement de données à caractère personnel. Il convient de prêter attention à la forme de dépersonnalisation des données à caractère personnel. Conformément à la loi de la Géorgie sur la protection des données à caractère personnel, la dépersonnalisation des données est définie comme un type de modification des données qui rendrait impossible la liaison avec une personne concernée ou nécessiterait des efforts, des coûts et du temps disproportionnés pour établir un tel lien.

Nous pourrons citer des exemples : un citoyen s'est adressé à l'inspecteur en déclarant qu'au cours de la contestation judiciaire, il a découvert que l'opposant avait connaissance de sa condamnation passée. Le citoyen a demandé à l'inspecteur de la protection des données personnelles d'étudier la légalité de la collecte et du traitement des données relatives à sa condamnation.

Un autre citoyen s'est adressé au Bureau de l'Inspecteur avec une demande similaire et a déclaré qu'une des organisations non gouvernementales diffusait des informations comme s'il avait été condamné pour crime particulièrement grave. À titre de preuve, la copie d'une décision judiciaire a été renvoyée. Le plaignant a indiqué qu'il n'avait pas de condamnation antérieure et que le jugement rendu public par le

tribunal de la ville de Tbilissi se référait à une autre personne. Les faits énoncés par l'organisation n'étaient pas exacts et visaient à discréditer le plaignant. **L'examen de la question a révélé que, dans les deux cas, le tribunal a publié une copie du jugement comme information publique, sans données personnelles, sous forme cryptée, en ne mentionnant que les initiales.**

L'une des principales composantes du plan d'action pour la libéralisation des visas était la recommandation de procéder à des réformes dans le domaine de la protection des données à caractère personnel. À cette fin, la Géorgie a adopté une législation sur la protection des données et créé une agence indépendante chargée de superviser sa mise en œuvre. Des experts de l'UE ont indiqué que la Géorgie avait mis en œuvre avec succès une législation sur la protection des données à la fois dans le secteur public et le secteur privé. Toutefois, la Géorgie continue sa réforme de protection des données dans le cadre de l'accord d'association.

Statistique et Evaluations des plaintes [155 ; 2019 : 11]

Fig. 18 : *Source: State Inspector's Service of Georgia, "Protecting personal data with you", 2019 , https://personaldata.ge/en*

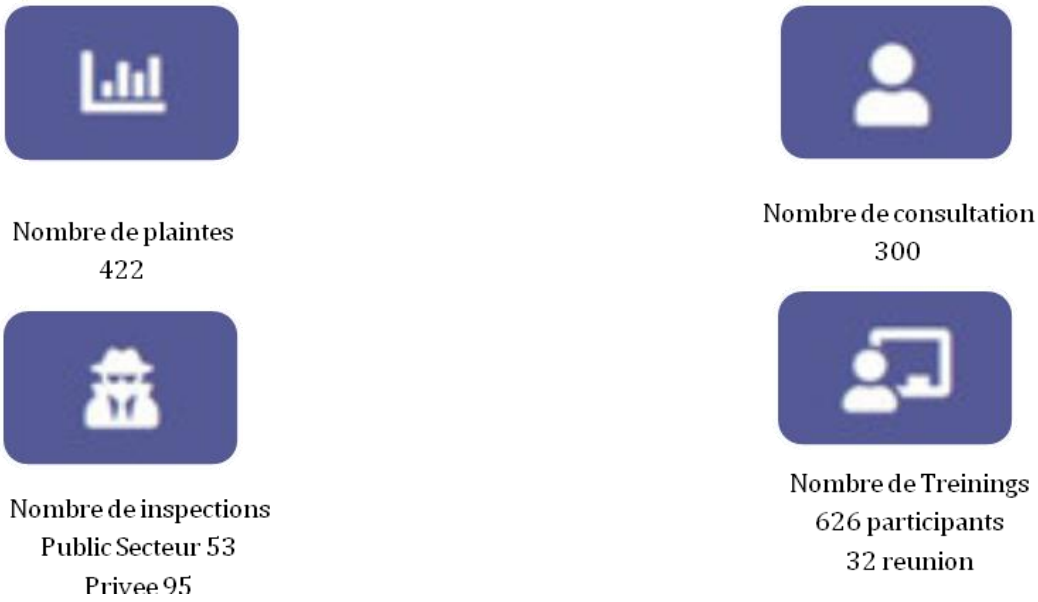
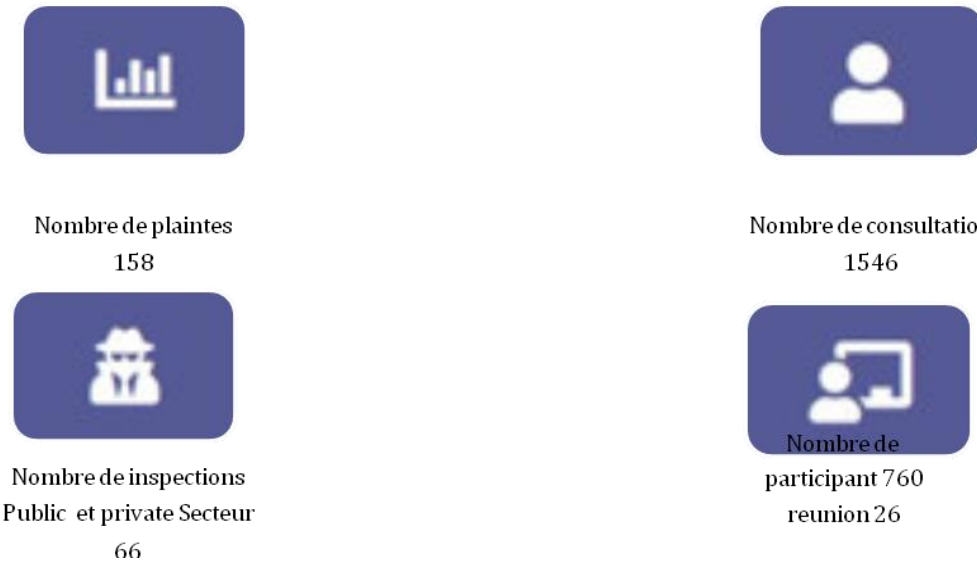


Fig. 19 : Statistiques du rapport 2020, Source : rapport annuels du Bureau de l'inspecteur d'État, *https://personaldata.ge/en* [155]



Conformément à l'article 41 (1) de la Constitution de la Géorgie, tout citoyen de la Géorgie a droit de connaître, conformément à une procédure prescrite par la loi, les informations le concernant stockées dans les institutions publiques ainsi que les documents officiels, à moins qu'ils ne contiennent un secret d'État, professionnel ou commercial. **L'article 21 de la loi sur la protection des données à caractère personnel garantit le droit des personnes concernées de demander des informations.**

Tout citoyen a le droit de demander des informations concernant le traitement de ses données auprès de contrôleurs de données privées ou publiques. Le responsable du traitement est tenu de fournir les informations suivantes : quelles données personnelles sont traitées ; l'objectif du traitement des données et des motifs juridiques de traitement ; moyens de collecte des données ; à qui les données personnelles ont été communiquées ; et les motifs de cette divulgation. Le citoyen doit recevoir les renseignements ci-dessus immédiatement sur demande, ou dans les 10 jours suivant la demande.

9.5 Les problématiques de la surveillance vidéo en Géorgie

Les principes et les normes de la loi de Géorgie sur la protection des données à caractère personnel établissent un cadre réglementaire strict à la protection des droits et des libertés universellement reconnus dans une société démocratique. La videosurveillance constitue une exception. Il convient de noter que la vidéosurveillance dans les lieux publics diffère des autres moyens de traitement des données, car le traitement des données à des fins d'intérêt public élevé ne dépend pas de la volonté d'une personne concernée.

Par conséquent, la loi définit strictement l'objectif du traitement des données par la vidéosurveillance, comme la prévention de la criminalité, la protection de l'ordre public, la protection de la sécurité et des biens personnels, la protection des mineurs contre les influences néfastes, la protection des informations secrètes. La surveillance vidéo doit être utilisée en tant que de besoin et non comme un mécanisme supplémentaire de contrôle des citoyens. En outre, conformément à la loi, en cas d'installation de système de surveillance vidéo, **tous les responsables du traitement des données sont obligés de placer un panneau**

d'alerte approprié dans un lieu visible afin de garantir le respect et la protection des droits des citoyens en les informant en traitement.

Le Bureau de l'inspecteur de la protection des données personnelles examine souvent la légalité du traitement des données par la vidéosurveillance dans de nombreux organismes privés ou publics. À la suite de l'examen, plusieurs cas où les systèmes de vidéosurveillance ont une fonction d'enregistrement audio ont été identifiés. L'examen des plaintes des citoyens et les inspections menées ont révélé que la surveillance vidéo-audio par différents systèmes était particulièrement fréquente dans les services (points de vente au détail, pharmacies, organisations financières).

Conformément à la loi de Géorgie sur la protection des données à caractère personnel, les données ne peuvent être traitées qu'à des fins légales clairement définies. Il n'est pas permis de traiter davantage les données à d'autres fins incompatibles avec le but principal. La même loi définit clairement les objectifs de la vidéosurveillance sur les lieux de travail. La réalisation des objectifs ci-dessus par d'autres moyens doit être impossible.

L'utilisation d'enregistrements vidéo pour contrôler les employés ne relève évidemment pas de l'objet du traitement des données prévues par la loi. Malgré le fait que la loi de Géorgie sur la protection des données personnelles établit clairement la règle et les objectifs légitimes de la vidéosurveillance dans la rue, à la suite de l'examen, **il a été établi que la majorité des organisations utilisent des enregistrements de vidéosurveillance à d'autres fins, qui sont incompatibles avec la loi.** Par ex : dans les points de vente d'une société, des caméras vidéo installées dans le périmètre intérieur des installations ont été utilisées pour la surveillance vidéo permanente afin de surveiller la qualité du service, contrôler le personnel des ventes et leur apparence. Dans certains cas, la surveillance vidéo est utilisée pour contrôler le temps d'arrivée et de départ des employés sur le lieu de travail.

Cas pratique de vidéosurveillance / doute raisonnable sur le contrôle des gens ayant une opinion politique opposée.

L'une des organisations politiques s'est adressée au Bureau de l'inspecteur de la protection des données personnelles. L'organisation a déclaré que, contrairement à la façade centrale de la construction de leur parti politique, il y avait un pôle d'éclairage, sur lequel le ministère de l'Intérieur de la Géorgie a installé caméra de surveillance de haute qualité pour enregistrer toutes les manœuvres autour de l'établissement. Selon la plainte, la caméra de surveillance vidéo était dirigée vers le kiosque d'entrée dans la cour du bureau central du parti ; **comme ces caméras ont des capacités de manœuvre, cette caméra observait l'espace de travail du bâtiment du parti.**

Sur la base des informations reçues, une inspection du Ministère de l'intérieur a été effectuée. L'installation de matériel photographique et vidéo dans les rues et sur le périmètre extérieur du bâtiment par le Ministère de l'intérieur de la Géorgie sert les objectifs de l'ordre public, notamment : la prévention de la criminalité, la sécurité des personnes et la protection des biens. L'emplacement de l'équipement vidéo est choisi en tenant compte des statistiques sur les incidents de circulation, de l'intensité du trafic et des autres menaces liées à la circulation. Au moment de l'inspection, le Ministère ne pouvait justifier par écrit la décision concernant l'installation de l'équipement à cette adresse particulière.

L'inspecteur a pris en compte le fait qu'en raison des paramètres techniques et des capacités de la caméra vidéo installée à l'adresse ci-dessus, la couverture du contrôle vidéo pourrait également inclure des bâtiments et des institutions différentes de la route, y compris le siège social dudit parti politique. Le contrôle vidéo sur le bâtiment et le territoire adjacent pourrait faciliter l'identification directe et / ou indirecte des membres du parti, des partisans, des employés de bureau et des visiteurs. Ainsi, le traitement direct et / ou indirect de données spéciales, à savoir des informations sur les affiliations politiques des personnes, a été rendu possible, ce qui contredit les objectifs de la vidéosurveillance.

Afin d'éviter un traitement disproportionné et inapproprié d'une catégorie spéciale de données et d'assurer l'accomplissement de l'objectif légal du traitement des données, **le Ministère de l'intérieur de la Géorgie a été chargé d'ajuster l'angle de la caméra de surveillance, de son orientation et de sa trajectoire de manière à ce que la surveillance ne couvre pas le bureau central du parti politique et son entrée, à l'exception des cas où le LEPL «112» recevrait un appel concernant un incident.** En outre, le Ministère a

été chargé d'évaluer la nécessité de la surveillance vidéo par la caméra fonctionnant selon un régime d'essai et de fournir des informations sur ces besoins et la décision finale à l'inspecteur.

9.6 Transfert des données de la Géorgie

Les flux transfrontaliers de données à caractère personnel restent encore importants. Les accords bilatéraux et multilatéraux de coopération entre la Géorgie et d'autres pays, l'activité internationale des sociétés géorgiennes, la création de filiales de sociétés étrangères et les projets d'investissement demandent une régularisation stricte. Il convient de mentionner qu'en 2015, une attention particulière a été accordée au transfert de données à caractère personnel et à la sécurité des données transférées tout en concluant des accords internationaux avec d'autres États et organisations internationales. **Plusieurs organismes publics ont adressé au Bureau de l'Inspecteur des consultations sur les accords internationaux à conclure. L'existence de garanties en matière de protection des données en Turquie et de trois organisations internationales (Communauté des États Indépendants, Centre Interpol et Asie centrale d'information et de coordination pour la lutte contre le trafic illicite de stupéfiants, de substances psychotropes et de leurs précurseurs) a été évaluée.**

Le transfert des données à caractère personnel reste toujours important en 2021. De nombreuses institutions privées opérant en Géorgie transfèrent des données à l'étranger à la demande des actionnaires et des partenaires étrangers. En tant que partie de la Convention 108 du Conseil de l'Europe pour la protection des personnes, la Géorgie a pris des engagements internationaux afin d'assurer un niveau élevé de protection des données conformément aux normes européennes. Les amendements législatifs élaborés par le Bureau de l'Inspecteur visent les obligations mentionnées. Les modifications législatives prévoient l'application de la loi sur la protection des traitements des données à caractère personnel à des fins de prévention du crime, d'enquête, de l'ordre public considéré comme un secret d'État. L'institution de l'Inspecteur de l'État a défini la liste des pays où la protection des données est garantie et le transfert est permis. Ces pays sont :

1. L'Australie

2. La république d'Autriche

3. La république d'Albanie

4. La Principauté d'Andorre

5. La république argentine

6. La Nouvelle-Zélande

7. Le Royaume de Belgique

8. La Bosnie-Herzégovine

9. La Bulgarie

10. La République Fédérale d'Allemagne

11. Le Danemark

12. La Grande-Bretagne et l'Irlande du Nord

13. L’Espagne

14. La république d'Estonie

15. L'Irlande

16. La république d'Islande

17. Israël

18. La république italienne

19. Le Canada

20. La république de Chypre

21. La république de Lettonie

22. La république de Lituanie

23. La Principauté de Liechtenstein

24. Le Grand-Duché de Luxembourg

25. La république de Malte

26. République de Moldova

27. La Principauté de Monaco

28. La Rrépublique du Monténégro

29. Les Pays-Bas

30. La Norvège

31. La république de Pologne

32. La république du Portugal

33. La Roumanie

34. La Grèce

35. La république française

36. La république de Serbie

37. République slovaque

38. La république de Slovénie

39. L’Ukraine

40. La Hongrie

41. L'Uruguay

42. La république de Finlande

43. La Suède

44. La Suisse

45. La République tchèque

46. L'ex-République yougoslave de Macédoine

47. La République de Croatie

Le traitement non automatique des données est irrecevable s'il est destiné à éviter l'exécution des exigences de la présente loi. La présente loi s'applique également :

- Au traitement des données par les représentations diplomatiques et consulaires de la Géorgie à l'étranger ;

- Aux activités d'un transformateur de données qui n'est pas immatriculé sur le territoire. Dans ce cas, le responsable du traitement des données doit nommer un représentant en Géorgie.

Quant aux données secrètes : Les informations relatives aux jugements rendus dans le cadre d'enquêtes secrètes, ainsi que les destructions des informations obtenues par des enquêtes secrètes doivent être fournies à la fin de chaque trimestre à la Commission de destruction des renseignements / données à caractère personnel par le biais d'enquêtes secrètes menées par le Parlement de Géorgie. La Commission sur la destruction des informations se compose de 7 membres : l'inspecteur de l'Etat ; le vice-président de la Cour suprême de Géorgie (nommé membre de la Commission par le président de la Cour suprême de Géorgie), le procureur général adjoint de la Géorgie (qui sera nommé membre de la Commission par le Procureur général de la Géorgie), le Défenseur public de la Géorgie, le président du Comité des droits de l'homme et de l'intégration, deux membres de la Commission élus par le Parlement.

9.7 Recommandations de différentes organisations pour l'application du nouveau champ législatif en Géorgie

Comme nous l'avons constaté, l'institution de l'inspecteur de l'Etat est une organisation assez jeune n'ayant pas beaucoup d'expérience. La législation a été renouvelée en 2019 et plusieurs organisations non gouvernementales avaient des recommandations, y compris l'Association des jeunes juristes GYLA [108]. Nous avons eu la possibilité de rencontrer les responsables de cette organisation pour discuter de la législation géorgienne concernant la protection des données à caractère personnel. Les recommandations (que nous partageons aussi) de la *Georgian Young Lawyers Association* GYLA étaient les suivantes :

- Champ d'application - Conformément à l'article 2 du projet de loi sur la protection des données personnelles, « afin de réglementer la liaison directement liée au traitement des données personnelles, cette loi peut utiliser la liaison la plus proche par analogie avec les normes »

➢ En raison de la nature spécifique des données personnelles, l'utilisation de normes juridiques analogues réglementant d'autres domaines peut être dangereuse en termes de protection. Dans ce cas, le projet de loi ne précise pas ce qui pourrait être considéré comme «la relation la plus proche » aux fins des données personnelles.

- **Motifs de traitement et de divulgation des données sensibles - Selon l'article 6, paragraphe 1, du projet de loi, l'un des motifs de traitement des données pourrait être « l'intérêt public significatif ».**

➢ Nous devons veiller particulièrement à maintenir un équilibre entre les droits de l'homme et l'intérêt public. Le projet de loi ne devrait pas autoriser le traitement de tous les types de catégories spéciales de données à des fins d'intérêt public.

- Surveillance audio - Selon la première partie de l'article 11 (d) du projet de loi, l'un des motifs de la surveillance audio pourrait **être la « protection de l'intérêt légitime du sous-traitant de données » qui, contrairement à d'autres motifs, est vague.**

➢ Le responsable du traitement des données aurait un large pouvoir discrétionnaire afin de décider lui-même de ce qui peut être considéré comme un « intérêt légitime supérieur » aux fins de l'audio surveillance. Une telle situation présente des risques lors du traitement des données personnelles**.**

- Profilage - L'article 21-2 2 du projet de loi donne à la personne concernée le droit de faire appel de la décision de profilage**, sauf si "le profilage est prévu par la loi" (article 21 1 1) Sous-paragraphe «c »).**

➢ En raison de la nature du profilage, la personne concernée devrait avoir le droit de faire appel de la décision prise sur la base du profilage dans tous les cas. Le risque de violation de ses droits existe en présence des motifs prévus ou non prévus par la loi.

- Les délais de stockage des données d'identification des communications électronique - la loi géorgienne sur les communications électroniques et le code de procédure pénale de Géorgie sont interdépendants. Selon le premier paragraphe de l'article 85 de la loi géorgienne sur les communications électroniques, **« une entreprise de communications électroniques est autorisée à conserver les données d'identification des communications électroniques pendant au plus quatre ans après la résiliation du contrat de fourniture de services de communications électroniques ».** Selon l'article 136, partie 31 du code de procédure pénale, aux fins d'enquête sur un crime, de poursuites pénales et d'administration de la justice, une entreprise de communication électronique est autorisée de délivrer les informations sur les communications électroniques durant quatre ans.

➢ Le délai de quatre ans dont dispose l'entreprise de communications électroniques pour maintenir les communications électroniques et délivrer ces informations à des fins procédurales est excessivement long. Une durée de 2 ans dans ce cas réduira considérablement les risques de non-respect violant des données [109].

9.8 Service de l'Inspecteur de l'État et les médias et les expériences des homologues

Le Bureau de l'Inspecteur, en coopération avec les experts du Conseil de l'Europe, a commencé à élaborer des lignes directrices pour les médias afin d'assurer un équilibre entre la vie privée et la liberté d'expression. Un bon équilibre signifie fournir une information au public tout en protégeant la vie privée

des individus. Cette question est de plus en plus aiguë à l'ère des technologies modernes. La rapidité de la circulation des données est un défi pour la protection de la vie privée.

Des représentants du Bureau de l'Inspecteur et du Conseil de l'Europe ont rencontré toutes les parties prenantes. Les représentants des médias en ligne et de la presse, de la Charte de l'éthique journalistique et du Fonds de développement des médias ont discuté des pratiques et des défis actuels en Géorgie, ainsi que des mécanismes d'autoréglementation et des principes de leur mise en œuvre. **La loi géorgienne sur la protection des données à caractère personnel ne couvre pas le traitement des données à des fins journalistiques ; par conséquent, les lignes directrices élaborées en coopération avec les experts du Conseil de l'Europe ne seront pas obligatoires pour les médias et auront un pouvoir de recommandation.** Le comité consultatif de la Convention 108 (T-PD) travaille également sur Projet de principes de la protection de la vie privée dans les media.

En France, la communication en ligne est régularisée par la loi. L'exercice de cette liberté ne peut être limité que dans la mesure requise, d'une part, par le respect de la dignité de la personne humaine, de la liberté et de la propriété d'autrui, du caractère pluraliste de l'expression des courants de pensée et d'opinion et, d'autre part, par la sauvegarde de l'ordre public, par les besoins de la défense nationale, par les exigences de service public, par les contraintes techniques inhérentes aux moyens de communication, ainsi que par la nécessité, pour les services audiovisuels, de développer la production audiovisuelle [138].

N'ayant pas trop d'expérience, le bureau de l'inspecteur collabore avec ses homologues étrangers. En janvier 2017, des représentants du Bureau de l'inspecteur de la protection des données de Géorgie a visité Rome (Italie), lors d'un voyage d'étude. La visite a été organisée avec le soutien de l'Union européenne (UE) et le Programme des Nations Unies pour le développement (PNUD). Le renforcement de la protection des données personnelles en Géorgie est une des priorités de l'initiative conjointe de l'Union européenne (UE) et de l'ONU, « Droits de l'homme pour tous ». Avec un budget de 4 millions euros, le programme prend en charge la mise en œuvre et le suivi de la stratégie nationale de droits de l'homme et le Plan d'Action de Géorgie. Le Groupe de travail international sur la protection des données dans les télécommunications s'est réuni pour la 60ème fois à Berlin. Les questions de l'enseignement des plateformes Internet, le traitement des données biométriques, les défis actuels à l'ère des appareils intelligents ont été discutés lors de la réunion. Les représentant géorgiens en ont fait partie.

Le Bureau de l'inspecteur de la protection des données personnelles est devenu membre du Groupe de Berlin le 21 mars 2016. Le groupe a pour objectif d'élaborer des recommandations visant à améliorer la protection des données dans les télécommunications, y compris l'Internet. Le groupe se compose d'autorités chargées de la protection des données, ainsi que d'autres organismes publics, d'organisations internationales et d'experts du monde entier. L'inspectrice du service d'État de la Géorgie participe régulièrement aux réunions du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Lors de la réunion, différents projets sont examinés, par ex : l'utilisation de données personnelles dans le secteur de la police ou le traitement des dossiers des passagers et des principes relatifs à la protection de la vie privée dans la couverture médiatique. En générale, Le Conseil de l'Europe met à jour sa Convention pour la protection des données à caractère personnel («Convention n° 108») dans un double but :

- Traiter les problèmes liés au respect de la vie
- Renforcer le mécanisme de contrôle de la Convention.
- Rassembler les divers cadres normatifs élaborés dans différents pays du monde et constituer un cadre multilatéral flexible contre les abus.

Il faut savoir que la convention a été ouverte le 28 janvier 1981. Elle reste aujourd'hui encore le seul traité international dans ce domaine. Elle est ouverte à tout pays et pourrait devenir une norme internationale. 46 Etats-membres du Conseil de l'Europe en font partie. L'île Maurice, le Maroc, le Sénégal et la Tunisie ont été invités à y adhérer. L'adhésion au Bureau a constitué une reconnaissance internationale pour le service de l'Inspecteur d'État de la Géorgie, ainsi qu'une solide plate-forme internationale. C'est également une occasion supplémentaire pour la Géorgie de participer au processus de création et de développement de règles européennes dans le domaine de la protection des données à caractère personnel. Le Bureau de l'inspecteur est représenté au bureau du T-PD depuis 2014. Les activités du Service de l'Inspecteur durant les trois années de son établissement et ses perspectives d'avenir ont été discutées lors d'une table ronde organisée avec l'aide de l'Union européenne et du Programme des Nations Unies pour le développement (PNUD) en 2016. Les participants du secteur non gouvernemental ont mis l'accent sur les lacunes en matière de protection des données personnelles en Géorgie et ont présenté leurs points de vue et leurs idées sur la sensibilisation du public aux questions de ce sujet. Les parties se sont déclarées prêtes à coopérer plus étroitement

9.9 Comparaison des situations numériques en Europe (Géorgie et France)

La France s'avance dans le plan numérique et elle a déjà choisi le ministre d'État numérique et le conseil national de numérique, qui est un organisme consultatif français créé en 2011 par le décret n° 2011-476. « Le numérique est partout, il a envahi l'économie, la société, l'école… », expliquait au *Monde* Axelle Lemaire, secrétaire d'État au numérique au gouvernement, lors d'une présentation de cette stratégie numérique gouvernementale [189].

Au cours des années précédentes, nous pouvons constater que les pays de l'UE ont amélioré leurs performances numériques. Plus concrètement, la Finlande, la Suède, le Danemark et les Pays-Bas ont obtenu les meilleures notes en 2020 et figurent parmi les leaders mondiaux de la numérisation. Ces pays sont suivis par Malte, l'Irlande et l'Estonie [90 ; 19].

En 2019, le nombre des personnes ayant des compétences numériques de base a atteint 58 % (contre 55 % en 2015). Toutefois, une grande partie de la population de l'UE n'a toujours pas les ces compétences de base, malgré la demande accrue du marché. En 2018, 9,1 millions de personnes travaillaient comme spécialistes des TIC dans toute l'UE, c'est-à-dire 1,6 million de plus qu'en 2015.

64 % des grandes entreprises et 56 % des PME ont recruté des spécialistes des TIC en 2018. Dans la dimension capital humain du DESI, la Finlande, la Suède et l'Estonie sont les plus avancées. L'utilisation d'Internet par les particuliers a fortement augmenté pendant la pandémie. Cette tendance était déjà en place avant le Covid, l'utilisation d'Internet continuait d'augmenter. 85% des Européens l'utilisent au moins une fois par semaine (contre 75% en 2014). Les chiffres vont de 67% à 95% au Danemark, en Suède et aux Pays-Bas. Les services bancaires sur Internet et les achats sont également très populaires.

D'après le dernier rapport de DESI, il est frappant que les pays de l'UE les plus puissants en termes de PIB ne figurent pas parmi les leaders du numérique, ce qui a un impact sur la performance globale du marché unique. L'Allemagne, qui se classe au 1er rang des pays de l'UE, a lancé plusieurs mesures dans le but de faire progresser la numérisation et mène des initiatives dans le domaine de la sécurité informatique, de l'intelligence artificielle et de la block Chain.

La France souhaite de faciliter la numérisation des services publics et des entreprises et mettre en place un écosystème dynamique pour les start-up technologiques.

En décembre 2019, l'Italie a adopté « Italia 2025 », un plan quinquennal qui place la numérisation et l'innovation au centre d'un « processus de transformation structurelle et radicale du pays ».
Ces initiatives pourraient entraîner une progression de ces États membres sur le DESI dans les années à venir. Selon les termes de la Commissaire européenne à l'économie et à la société, Marya Gabriel, « L'indice de l'économie et de la société numérique de cette année (2020) montre que le rythme de la transformation numérique doit s'accélérer pour que l'Union européenne reste compétitive au niveau mondial »[160].

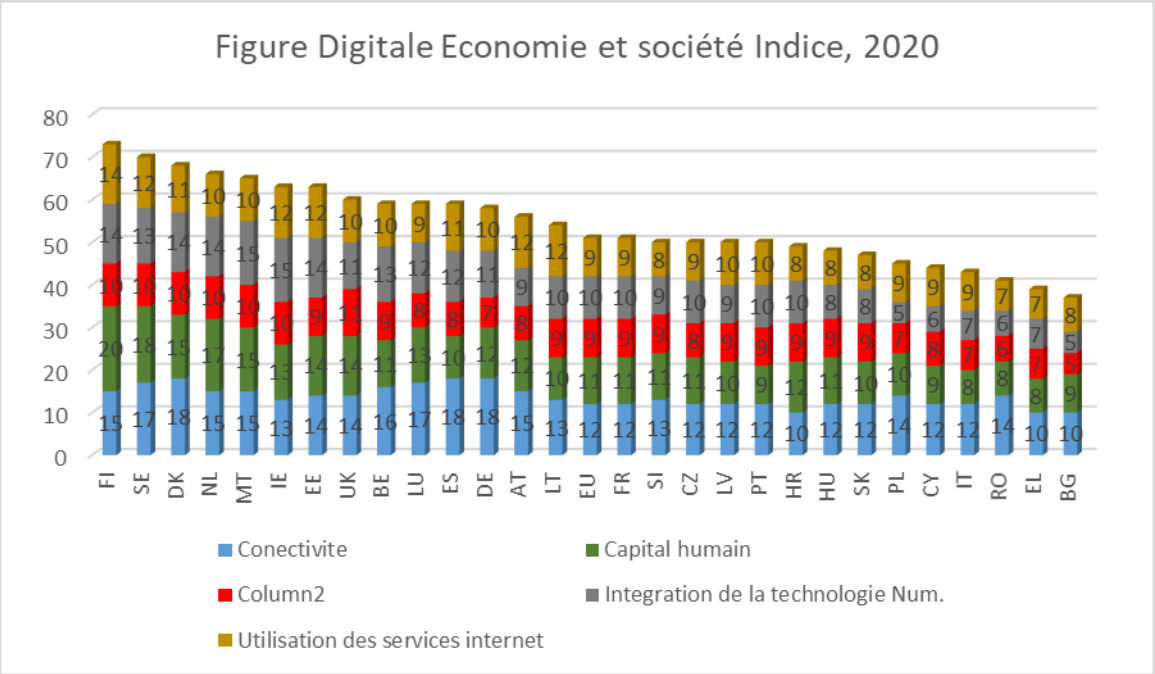


Fig. 20 : *Digitale économie et Société Indice, 2010, Source : DESI 2020. Commission Européenne*

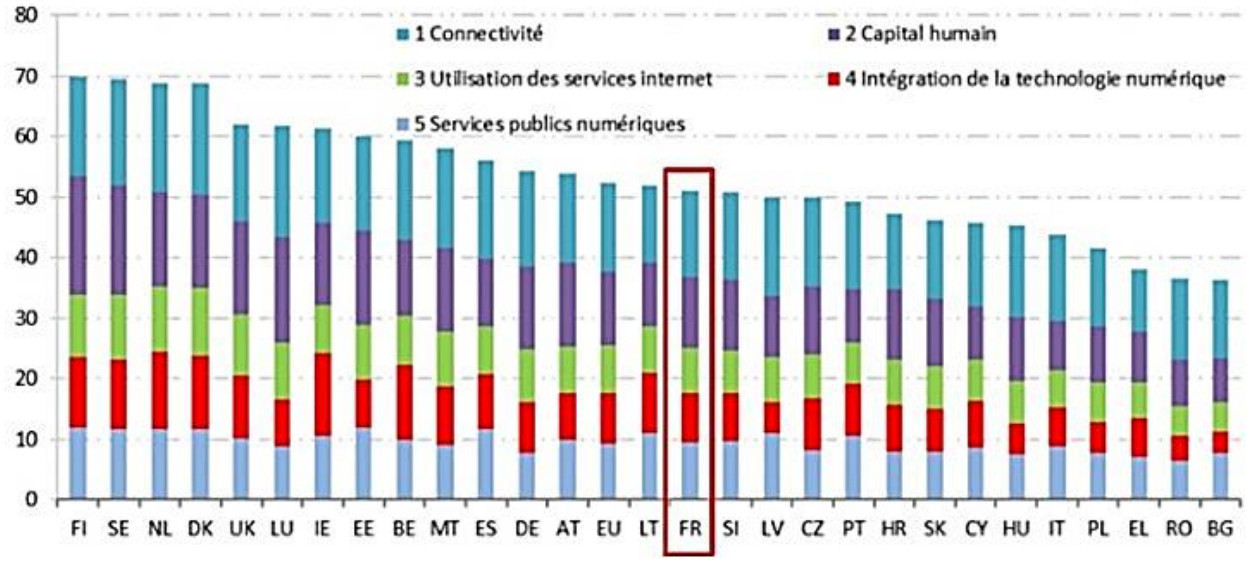
Les rapports sur l'indice relatif à l'économie et à la société numériques (DESI) permettent à la Commission européenne de suivre la compétitivité numérique des États membres. La France se classe à la 15e place du classement de (DESI) 2019.

Fig. 21 : *Classement de la France , Source DESI 2019, European Commission*

	France		EU
	Classement	Note	Note
DESI 2019	15	51	52.5
DESI 2018	16	47.7	49.8
DESI 2017	14	45.6	46.9

Fig. 22 : *Classement de la France , Source DESI 2020, European Commission*

Classement 2019 de l'indice relatif à l'économie et à la société numériques



Source: DESI 2020, European Commission

- Avec une note de connectivité de 56,6, la France occupe la 20e position du classement des États membres de l'UE. Les ménages français sont presque entièrement couverts. D'après la décision du gouvernement à partir de 2020, la 5G devrait être commercialement disponible dans les grandes villes et en 2025, les grands axes devraient être couverts par la 5G.

- La France se situe dans la moyenne du classement relatif au capital humain. Environ 57 % des personnes âgées de 16 à 74 ans possèdent des compétences numériques. Dans le cadre du Plan d'investissement dans les compétences, un montant de 77 millions d'euros a été engagé pour des actions de formation. Plus de 500 événements ont été organisés en ce sens en France. En 2018, bon nombre d'écoles et d'autres organisations ont participé à la Semaine européenne du code [64].

- La part de la population française utilisant internet reste élevée. La note globale de la France dans cette dimension a augmenté par rapport à l'année précédente 49,2 en 2019 et 48.0 en 2018.

- En 2018 et 2019, le nombre d'entreprises françaises utilisant la facturation électronique et l'informatique en nuage a aussi progressé. À l'intégration de la technologie numérique par les entreprises, la France s'élève à la 14ème place du classement de 2019. Pour faciliter l'accès des TPE et PME aux technologies, France NUM propose des solutions pour financer tout projet de transformation numérique. Delphine Gény-Stephann, secrétaire d'État auprès du ministère de l'Économie et Mounir Mahjoubi, secrétaire d'État au Numérique, ont lancé la **plateforme France Num** en 2018 [151]. Cette plateforme vise à renforcer la **numérisation des petites et moyennes entreprises** à travers une offre de témoignage.

La France se positionne parmi les pionniers pour la modernisation des services publics grâce au numérique. Elle est 15ème dans le classement avec 64,1 points supérieurs de note par rapport à la moyenne de l'UE.

Quant à la Géorgie, son classement de gouvernance électronique et de participation électronique s'est légèrement amélioré dans le cadre de l'Enquête des Nations Unies sur l'administration électronique 2020. Malgré une amélioration dans le classement mondial de l'e-participation, la Géorgie se classe 10ème sur onze pays de la région et ne dépasse que la Lettonie. La part d'utilisateurs d'Internet en Géorgie est faible par rapport à d'autres pays de la région. Selon cette composante, environ 63% de la population géorgienne seulement utilise Internet. Selon l'évaluation de 2020, le score de l'administration électronique de la Géorgie est de 0,72, ce qui la place à la 65e place sur 193 pays [120].

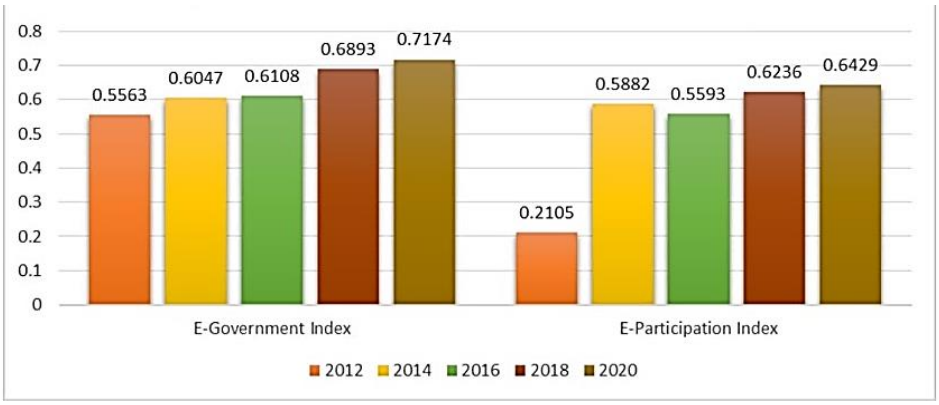


Fig. 23. *Classement de la Géorgie, Source: Georgia in the UN E-Government Survey – Review of 2020 Results*

E -gouvernance E- participation

Fig. 24 : *Positionnement de la Géorgie selon les années, Source : Georgia in the UN E-Government Survey, Review of 2020 Results*

Quant aux cinq premiers pays du classement, les leaders en termes de gouvernement électronique sont : le Danemark, la République de Corée, l'Estonie, la Finlande, l'Australie et la Suède.

Il faut respecter l'équilibre entre la vie privée et l'intérêt public. La Convention du Conseil de l'Europe sur la cybercriminalité de 2001 est ouverte à la signature aux membres du Conseil de l'Europe et également aux États-Unis, au Japon et à l'Afrique du Sud, qui ont participé à sa négociation et l'ont d'ailleurs signée. Ses dispositions de droit matériel sont complétées par des mesures relatives à l'instruction et à la coopération internationale. Les États qui en feront partie devront instaurer des sanctions effectives. Ils ont

quatre types de sanctions. Les trois premiers types d'infractions concernent les données et les systèmes informatiques, le quatrième type d'infraction concerne la propriété intellectuelle et les droites annexes.

9.10 Conclusion

Le décalage de dizaines d'années dans la fondation des institutions responsables de veiller sur la vie privée dans l'informatique en Géorgie a ses conséquences. Malgré des démarches positives et des succès de mission de service de l'inspecteur de l'Etat, il reste encore beaucoup à accomplir. Les délais de stockage des données d'identification des communications électroniques, la loi géorgienne sur les communications électroniques et le code de procédure pénale de Géorgie sont interdépendants. Le désir de certaines administrations et des ministères de contrôler illégalement collègues et citoyens reste un problème. La question des media et la protection des données est un sujet assez délicat. Il est difficile de définir la frontière entre la liberté d'expression et la vie privée. La divulgation des vidéos concernant la vie privée est une arme dans la bataille politique non encore traitée convenablement par le pouvoir. D'après le dernier rapport de DESI, il est évident que les pays de l'UE les plus puissants en termes de PIB ne figurent pas parmi les leaders du numérique et il est ainsi logique que la Géorgie rencontre aussi des problèmes de digitalisation. L'Allemagne, qui se classe au 1er rang des pays de l'UE, a lancé plusieurs mesures dans le but de faire progresser la numérisation. Quant à la Géorgie, malgré une amélioration dans le classement mondial de l'e-participation, elle se classe 10ème sur onze pays de la région et ne dépasse que la Lettonie. La part des utilisateurs d'Internet en Géorgie est faible par rapport à d'autres pays de la région. Selon cette composante, seulement environ 63% de la population géorgienne utilise Internet. Selon une évaluation de 2020, le score de l'administration électronique de la Géorgie est de 0,72, ce qui la place au 65ème rang sur 193 pays.

Chapitre 10
RGPD /GDPR : Nouvelles règles appliquées

Ce chapitre présente les enjeux du Règlement Général sur la Protection des Données (RGPD) depuis le 25 mai 2018, promulgué par la Commission Européenne. Ses dispositions sont applicables dans les 28 pays de l'Union Européenne par l'ensemble des organismes dans le monde ainsi que celles qui hébergent et manipulent des données personnelles de résidents européens. Ce sont désormais sept droits (dont deux nouveaux) qui sont renforcés par le RGPD : Transparence des informations et des communications, Droit d'accès à la donnée de la personne concernée, Droit de rectification, Droit à la limitation du traitement, Droit d'opposition, Droit à la portabilité des données et Droit à l'oubli, (nouveaux)

10.1 Introduction

A partir du 25 mai 2018 (date d'entrée en vigueur du règlement européen relatif aux données personnelles), de nouveaux droits et de nouvelles obligations sont fixés. Le RGPD (« règlement général sur la protection des données ») est un nouveau règlement européen qui encadre les règles de protection des données personnelles (règlement UE 2016/679). Toutes les entreprises, les PME et les TPE qui effectuent des traitements de données sont concernées. Même les sous-traitants des grandes sociétés devront démontrer leur mise en conformité. **Apres l'application de ce règlement, les Etats membres de l'UE disposent d'une législation uniforme et actualisée en matière de protection des données**. Le vote du Parlement finalise plus de quatre ans de travaux sur une réforme complète des dispositions européennes relatives à la protection des données. La réforme remplace la directive datant 1995 sur la protection des données.

Ce nouveau règlement impose de nouvelles obligations pour les responsables de traitements de données. Surtout, il impose la désignation d'un délégué à la protection des données « Data Protection Officer » (DPO), une personne en charge de la protection des données personnelles traitées par un organisme. Sa désignation est obligatoire pour un grand nombre de responsables de traitement de données personnelles.

- En collectant les données d'une personne, le responsable du traitement doit fournir à la personne concernée un certain nombre d'informations dont l'identité et les coordonnées [166: articles 13, 14].

- Dans le règlement du RGPD, un droit à l'effacement /droit à l'oubli est bien souligné : après la demande de l'effacement de ses données par la personne concernée, le responsable du traitement devra procéder à la suppression des données dans les meilleurs délais. Alors que le droit au déréférencement avait été introduit par la CJUE dans un arrêt du 13 mai 2014 [82] dans le règlement, l'obligation du responsable du traitement est doublé.

- **Le droit à la portabilité** diffère du droit d'accès. Le droit d'accès donne la possibilité d'exercer son intérêt sur les données détenues par un organisme et demander la rectification ou l'effacement. Le droit à la portabilité permet de manipuler les données « portables » et de les transmettre à d'autres plateformes.

- Calcul d'amende changé - Avant le règlement, toute amende était fixe. À partir du RGPD, elle peut monter jusqu'à 20 millions d'euros ou 4% chiffres d'affaires mondial des entreprises.

De nouvelles missions sont confiées à la CNIL. L'autorité administrative indépendante devra promouvoir « *l'utilisation des technologies protectrices de la vie privée ».* La Commission aura pour rôle d'organiser une *réflexion sur les problèmes éthiques.*

Ce règlement apportera de la force aux entreprises grâce à une législation unique dans l'UE. La nouvelle loi renforcera la confiance et garantira une concurrence plus loyale. La directive sur la protection des données couvre le traitement des données par la police et la justice pénale. Elle demande que les données des victimes, des témoins et des suspects de crimes soient dûment protégées [69]. La confidentialité des communications des consommateurs sera protégée dans toute l'UE, quelle que soit la technologie utilisée. En remplaçant l'actuelle directive "vie privée et communications électroniques" par un règlement directement applicable, les entreprises et les particuliers bénéficieront d'un seul ensemble de règles dans toute l'UE. L'utilisation de témoins de connexion et d'autres technologies de suivi à des fins de publicités sera soumise à des règles plus claires. **Les règles actualisées visent à renforcer la confiance et la sécurité dans le marché unique numérique de l'UE**.

10.2 Résultats de RGPD après son application

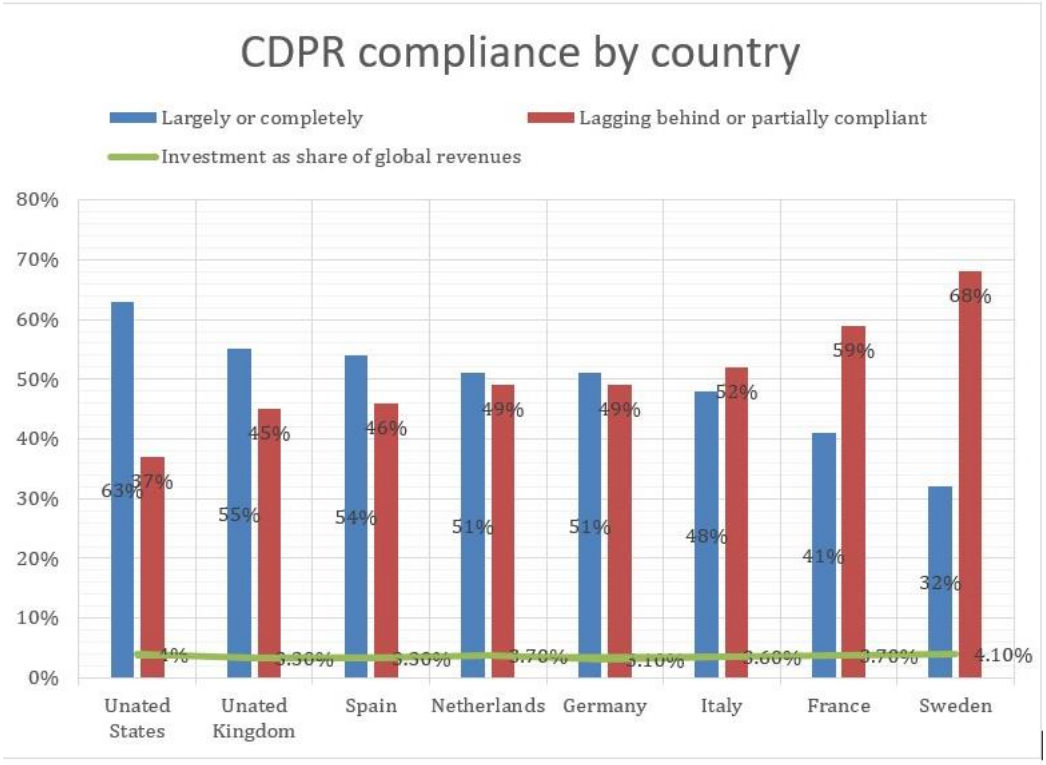
Le RGPD est en application depuis plus de deux an, mais un grand nombre d'entreprises ne sont pas encore en conformité avec le règlement. 28% des entreprises interrogées affirment être conformes, et seules 30% des entreprises se déclarent être « presque conformes ». Au niveaux de la conformité, les entreprises américaines sont en tête (35%), suivies par les entreprises britanniques, allemandes (33%), espagnoles (21%), italiennes (21%) et suédoises (18%).

L'étude révèle un écart entre les organisations conformes et les retardataires. Les entreprises conformes au RGPD utilisent davantage les technologies telles que :

- Le Cloud (84% contre 73% pour les entreprises non conformes),
- Le chiffrement des données (70% contre 55%),
- L'automatisation robotique des processus (35% contre 27%)
- l'archivage des données industrialisé (20% contre 15%) [19].

Capgemini, leader mondial des services informatiques et de la transformation numérique, a mené une enquête significative :

Fig. 25 : *Conformité de la régularisation par pays, Source: Capgemini research institute reports 2019*



Source: Capgemini research institute reports 2019

10.3 Politique et législation européenne pour le numérique

La ligue française pour la défense des droits de l'Homme et du citoyen a mis en place un programme de sensibilisation des jeunes adultes sur la protection de la vie privée et des données personnelles. La ligue est une association française destinée à défendre les principes énoncés dans la déclaration des droits de l'homme et la déclaration universelle de 1948. L'association européenne pour les droits des hommes et d'autres ONG ont contribué à ce projet comparatif. Il s'agissait de comparer les législations des cas pratiques dans certaines payses européennes au niveau de la défense de la vie privée. Ils ont mené de travaux importants comprenant les sujets suivants :

- Cadre juridique européen ;
- Identité biologique ;
- Autorités nacionales et ses particularités au niveau de la protection des données personnelles ;

En 1981, a été signée la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Le but de la présente Convention est de garantir, sur le territoire de chaque partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant « protection des données ». A partir de l'accord de Shengen, dans l'objectif de parvenir à une surveillance plus efficace de leurs frontières extérieures, les Etats membres visent à créer un fichier commun des personnes recherchées (ainsi que des objets, œuvres d'art et véhicules volés). Le contrôle se renforce après les grandes immigrations et un grand nombre de demandeur d'asile. Si les gouvernements demandent un contrôle par des moyens biologiques,

les cartes à puce avec des éléments biologiques sont créées. Pour équilibrer la situation, les défenseurs des droits de l'homme demandent des moyens plus efficaces pour la protection des données personnelles.

La directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concerne le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques. D'après cette directive, il convient que les fournisseurs de services tiennent toujours leurs abonnés informés des types de données qu'ils traitent, des finalités de ces traitements et de leur durée.

Le Traité d'Amsterdam ouvre une nouvelle ère pour l'Europe. La lutte contre le racisme, la xénophobie et les discriminations en découlant, et en faveur du principe d'égalité de traitement, a été initiée par les organisations non gouvernementales au niveau européen et national. Ce traité vise à assurer la libre circulation des personnes et à protéger les citoyens.

La directive 2006/24 prévoyait l'obligation des fournisseurs de services de communications électroniques, accessibles au public ou des réseaux publics de communications, de conserver les données relatives au trafic et aux données de localisation concernant tant les entités juridiques que les personnes physiques, pour identifier l'abonné ou l'utilisateur enregistré. La directive impose la conservation de toutes les données relatives au trafic concernant la téléphonie fixe, la téléphonie mobile, l'accès à Internet, le courrier électronique par Internet ainsi que la téléphonie par Internet, aucune différenciation ou exception ne soient opérées en fonction de l'objectif de lutte contre les infractions graves. Elle a été déclarée invalide dans un arrêt rendu le 8 août 2014 par le CEJU, au motif qu'elle n'était pas en conformité avec les droits fondamentaux garantis par l'article 7 (respect de la vie privée et familiale) [94]. Pour les défenseurs des droits de l'homme, la durée de conservation des données est aussi problématique, en raison de l'absence de distinction entre les catégories de données, en fonction de leur utilité éventuelle ou selon les personnes concernées.

Le traité de Prüm renforce la coopération transfrontalière, en vue de lutter contre le terrorisme, la criminalité et l'immigration illégale. Il prévoit l'échange des données génétiques et d'empreintes et de données à caractère personnel. Ce traite a été signé en 2005 par 7 pays européens, dont la France (Le traité de Prüm (également appelé « Schengen III » ou « Schengen plus ») signé le 27 mai 2005 à Prüm, en Allemagne, par sept États membres de l'Union).

Décision-cadre 2008/977/JAI du conseil du 27 novembre 2008 **relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.** L'échange de données à caractère personnel dans le cadre de la coopération policière et judiciaire en matière pénale, et notamment de la mise en œuvre du principe de disponibilité des informations au sens du programme de La Haye, devrait être étayé par des règles claires qui renforcent la confiance mutuelle entre les autorités compétentes [95].

En 1988, la première loi sur les fichiers de données personnelles est entrée en vigueur - en Finlande. Cette loi visait à empêcher les violations de l'intégrité à toutes les étapes du traitement des données. En 2004, la loi sur la protection de la vie privée dans la vie professionnelle a été promulguée.

En 2009, « la loi Nokia » a été adoptée. Elle a introduit un amendement à la loi finlandaise sur la protection des données dans les communications électroniques de septembre 2004. La nouvelle loi a été votée au parlement en février 2009 et est entrée en vigueur début juin 2009. La loi est appelée « loi Nokia » en reconnaissance au soutien de l'entreprise Nokia pour celle-ci. Selon certains journaux, « Ce projet permet aux entreprises de surveiller le courrier électronique de leurs employés, est censé lutter contre les fuites liées à l'espionnage industriel. Mais les dénégations de Nokia (16 000 employés en Finlande, 1,3 milliard d'euros de recettes fiscales, 4 % du PIB, 20 % des exportations) n'y font rien. " [186]

Selon la jurisprudence francaise :« Chacun a droit au respect de sa vie privée. »[79] Le 23 juillet 1999, le Conseil Constitutionnel a donné valeur constitutionnelle au droit à la vie privée. La vie privée est une notion juridique qui englobe :

- La vie familiale : informations telles que la correspondance, la domiciliation, la maternité, le PACS ;
- Les relations sexuelles ;

- Situation financière d'un individu et de sa famille ;
- Etat de santé ;
- Convictions politiques ou religieuses : les opinions politiques et croyances religieuses des personnes font l'objet d'une obligation au secret.

L'article. 226-1 du code pénal punit l'atteinte volontairement portée à l'intimité de la vie privée d'une personne en écoutant, en enregistrant ou en transmettant au moyen d'un procédé quelconque, sans son consentement, ses paroles prononcées à titre privé ou confidentiel, ainsi qu'en fixant ou en transmettant son image lorsqu'elle se trouve dans un lieu privé.[139]

L'article L34-1 du CPCE détaille ces obligations. Elles sont de plusieurs ordres. Le respect du « droit à l'oubli » impose d'effacer les données de connexion. Mais d'autres droits entrent en conflit avec cet impératif : le droit de l'opérateur à conserver les éléments justifiant sa facturation, ainsi que le besoin des autorités d'accéder éventuellement aux données en cas d'enquête pénale.

Les données peuvent être conservées pendant une durée maximale d'un an pour les données nécessaires aux enquêtes judiciaires, et les données sortant de ces cadres sont tenus d'être effacées ou rendues anonymes. La loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) traite de différents thèmes, dont certains relatifs à la protection des données personnelles. Dans cette loi est affirmé le principe de neutralité des réseaux et le droit de récupération de ses données par le consommateur. Le texte introduit également le droit à l'oubli numérique pour les mineurs, le testament numérique pour donner des directives aux plateformes numériques, la confidentialité des correspondances privées [142].

Conclusion Avant l'introduction du GDPR, il était difficile de faire respecter les obligations de la législation en matière de protection de la vie privée aux responsables de traitement de données et aux sous-traitants établis hors de l'UE. La Commission européenne espere qu'en disposant d'une autorité de surveillance unique pour l'ensemble de l'UE, il sera plus simple pour les entreprises d'opérer dans la région. Le non-respect de GDPR peut entrainer une amende allant de 10 millions d'euros à 4% du chiffre d'affaires global annuel de l'entreprise. Une organisation doit nommer un délégué à la protection des données (DPD) si elle effectue un traitement à grande échelle de données. le GDPR permet aux organisations de devenir plus cyber-sécurisées et compétitives sur le marché et d'établir un plus grand niveau de confiance avec leurs clients.

Chapitre 11

Vérification automatisées et la protection des données

11.1 Introduction Vérification automatisée

"Lorsque vos clients s'enregistrent, notamment à distance, il est parfois nécessaire de vérifier leur identité. Cela peut parfois prendre beaucoup de temps et être fastidieux au quotidien. Intégrez ce processus directement dans vos parcours afin d'offrir à vos clients une expérience digitale fluide et agréable.

Notre API analyse tous les documents d'identité et extrait les informations de manière totalement automatisée. Ensuite, grâce à des algorithmes de pointe et à l'intelligence artificielle, nous vérifions les données en temps réel et vous donnons un verdict sur l'authenticité du document. De cette manière, notre **API de vérification des documents** détecte tout document altéré ou falsifié."[119]

Ce sont les citations d'un site qui propose son soutien pour la vérification des documents. En général, ce n'est pas la vérification automatisée qui pose problème mais son usage sans contrôle et sans respect des standards qui peuvent abuser les droits de l'homme.

Les plaintes déposées auprès de la Commission nationale de l'informatique et des libertés (CNIL) ont augmenté de 27% en 2019. Parmi ces plaintes, 10,7% en 2019 sont en rapport avec la surveillance des employés sur leur lieu de travail au moyen comme la vidéosurveillance, les écoutes téléphoniques par exemple.

Dans ce contexte, la CNIL a prononcé son avis et recommandations dans un communiqué demandant la minimisation prévue par l'article 5(1.c) du RGPD. Ainsi, les données collectées dans ce cadre doivent être adéquates, pertinentes et limitées.[42]

Une utilisation «manuelle» d'un ordinateur n'entre pas dans la catégorie des traitements automatisés [80]. Envoyer un courriel à quelqu'un, en utilisant son adresse, qui est une donnée personnelle, obligerait sinon à respecter toutes les obligations : demander le consentement du destinataire, lui donner un droit

d'accès aux messages envoyés, interdire de conserver les courriels lorsqu'ils ne sont plus d'actualité, etc. Ainsi, le carnet-répertoire téléphonique comme un fichier papier n'a donc pas à être déclaré à la CNIL.

L'expression **système de traitement automatisé de données** (ou **STAD**) est une expression utilisée en droit français. Cette notion a été introduite en droit français par l'informatique et liberté de 1978, puis reprise par la loi Godfrain. Aucune définition de cette expression n'est apportée par les textes de loi. Une définition en avait été proposée lors des débats parlementaires.

11.2 Algorithmes et accès aux données

Le traitement algorithmique des informations suscite les questionnes. Un algorithme est une instruction permettant de résoudre un problème. Il peut être considéré comme une méthode pour résoudre un ensemble de problèmes.

On retrouve des algorithmes dans de nombreuses applications, par ex. dans le fonctionnement des ordinateurs, la cryptographie, la planification des ressources, le traitement d'images, le traitement de texte. Un algorithme va résoudre un problème particulier. Les procédés algorithmiques (*data mining* ou fouilles de données, *machine learning*, *Social Network Analysis, Predictive Analytics*, *Visualization*) permettent de trier la statistique des données, selon des structures de comportement. Sur internet, les algorithmes classent ainsi les informations, font des recommandations ou mettent en contact les personnes entre elles. Mais si les avantages des traitements algorithmiques sont incontestables, les risques aussi doit être clairement identifiés.

Un algorithme est une méthode générale pour résoudre un ensemble de problèmes. Il est dit correct lorsque s'il résout le problème posé. On mesure son efficacité par sa consommation de mémoire RAM, par la précision des résultats obtenus.

L'algorithme fait des calculs à partir des données collectées, sans aucune vérification de leur véracité, exactitude, pertinence, adéquation au regard du but recherché. Au final, le responsable du traitement des données ne sait pas comment la recherche est menée et par quelle méthode le profilage a été réalisé. Une question importante est suivante : **Comment contrôler la machine si son raisonnement échappe à l'homme ?**

Si on prend l'exemple du moteur de recherche de Google, dans l'hypothèse où cette société voudrait mettre en avant ses propres services par décision algorithmique de son moteur : l'activité humaine est chiffrée pour être catégorisée sans conscience des individus concernés. Les acteurs publics et privés à l'origine des traitements algorithmiques sont aussi variés (États, entreprises commerciales) et leurs finalités (lutter contre la criminalité, améliorer la connaissance des individu). Selon les auteurs, la « gouvernementalité algorithmique » se définit en trois temps :

- Récolte de quantité massive de données (*big data*) ;
- Traitement des données ;
- Production de connaissance (*data mining*) ;

Cette troisième partie est celui de l'usage de ces savoirs probabilistes statistiques à des fins d'anticipation des comportements individuels, *datamining* [169]. Cette étape est naturellement la plus préoccupante et traduit les risques que font encourir les procédés algorithmiques.

En effet, le *data mining* permet d'agréger des connaissances sur les individus et de les profiler, pour conditionner par exemple l'obtention d'un la tarification d'un contrat d'assurance, la suggestion d'achats sur des sites de vente en ligne, etc.

Ce type de profilage des individus risque de porter atteinte aux droits fondamentaux, d'être source de discriminations. Dans notre vie quotidienne, de plus en plus, la machine décide à la place de l'homme. Mais

comment s'assurer de sa pertinence ? Une grande partie de nos comportements sont déjà captés, analysés. Même si on pense que les algorithmes sont utilisés simplement pour aider l'application de la loi, il faut s'interroger sur la manière dont les contrôles sur les individus sont ainsi réalisés. Les moyens sont tout aussi importants que les fins.

Les algorithmes sont de puissants moyens de contrôler tout particulièrement l'argent et l'information[170].

La collecte massive de données relatives aux individus permet leur profilage détaillé pour une personnalisation des services proposés. Le partage se limitera à un cercle social, au travers d'échanges via les réseaux sociaux au sein de groupes limités. L'information personnalisée nous confine dans des bulles réconfortantes d'un horizon connu et compris. De nouvelles communautés se créent par ces nouvelles « liaisons numériques »[20 ; 55]. Le service individualisé n'est pas seulement le produit correspondant aux besoins individuels, mais aussi le produit qui va informer et aider à forger une opinion.

On sait que la distinction traditionnellement faite entre les données anonymes et les données personnelles n'est plus tellement performante. De nombreuses études ont en effet montré les possibilités de réidentifier les personnes à partir de plusieurs jeux de données anonymisées. Dès lors, les techniques d'anonymat ne sont plus suffisamment fiables, en présence de techniques de croisement de données par lesquelles on cherche précisément des corrélations et cumuls d'informations, de nature à obtenir la réidentification les personnes.

Il faut relever une autre faiblesse de la législation. La norme est plus confortable s'il s'agit d'obtenir des informations à des fins de sécurité nationale. Par exemple, l'affaire Snowden. Cette proximité entre les responsables de traitement et les services publics de renseignement affaiblit les personnes concernées. La recherche d'un nouvel accord, le *Privacy Shield*, va interdire la surveillance massive des citoyens européens et leur octroyer un droit de recours par la saisine d'un médiateur (*Ombusdman*), membre du Département d'État[165].

Des entreprises dont les politiques reposent sur l'utilisation d'algorithmes peuvent avoir leur responsabilité engagée en lien avec d'éventuels abus des règles de marché. Dans le secteur financier, des abus de marché ont pu être réalisés dans le cadre d'opérations de trading à haute fréquence [144 ; 88-92].

Dans le cas, un algorithme a été inventé pour réaliser une manipulation de marché certes classique mais réalisée à une échelle jusqu'alors inenvisageable techniquement. Il s'agissait de la stratégie du *marking the close*. Pratique consistant à poster puis annuler de nombreux ordres portant sur des quantités importantes dans le carnet, obligeant ainsi les autres négociateurs à perdre du temps à traiter et interpréter ces ordres. Ce type de tactique est rendu possible par le trading algorithmique.

Des algorithmes peuvent également être les instruments de pratiques anticoncurrentielles pour des ententes entre concurrents.

Il existe aussi le cas d'abus d'exploitation. Dans cette situation, l'algorithme sert de base à l'imposition de conditions tarifaires différenciées si ce n'est discriminatoires entre les utilisateurs de la plateforme. Par exemple, une plateforme, ayant de grandes masses de données sur ses utilisateurs et un algorithme de prix pourrait proposer à chacun de ses consommateur un prix strictement égal à sa propension marginale. Ainsi, la plateforme pourrait maximiser son profit en utilisant son pouvoir de marché.

Les algorithmes peuvent être utilisés pour des pratiques anticoncurrentielles. Il s'agit d'une situation dans laquelle les firmes coordonnent leurs comportements pour augmenter leur profit.

11.2.1. Usages différenciés des algorithmes

Un premier type d'entente fonctionnant au travers d'un algorithme nous est donné par un cas américain : Topkins. Il s'agit d'un vendeur de posters sur Amazon Market Place qui a utilisé avec ses concurrents un algorithme de prix leur permettant de s'ajuster instantanément à tout facteur conduisant à des différences entre eux. L'entente montée par Topkins procédait certes d'un agrément entre les firmes

concernées mais reposait exclusivement pour son fonctionnement sur un algorithme de prix. Si tous les « concurrents » augmentent leurs prix, la stratégie optimale est de réduire les siens de façon la plus discrète possible.

L'utilisation de données massives/Big Data et les algorithmes utilisant l'IA garantissent une meilleure stabilité des résultats. En économie, le Big Data se caractérise par la notion des 4V : Volume des données traitées ; Variété ;Vitesse de traitement ;Valeur .

On pourrait prendre en considération la capacité croissante des algorithmes à prévoir des évènements futurs à partir des données actuelles. Il s'agit par exemple de la notion de *now-casting*. Par exemple, une recherche en ligne sur la grippe annonce une épidémie avant même que les médecins ne soient consultés et donc que le système de santé ne soit informé du phénomène [99].

Au travers du *machine learning*, l'algorithme modifie de lui-même son code et ses paramètres. Le *machine learning* désigne la capacité de l'algorithme à se modifier de lui-même dans le cadre d'un processus d'apprentissage. La spécificité de ces algorithmes est la capacité d être autonome dans leur codage initial via l'expérience. Cette expérience est accumulée au travers des interactions de marché.

Les algorithmes sont programmés pour maximiser le profit individuel. Le *deep learning* permet d'analyser de très grandes quantités de données et donne la possibilité à une machine de corriger d'elle-même ses paramètres internes pour améliorer sa performance[144 ; 3-8].

Selon les recommandations de la Cnil, le principe de la loyauté doit être appliqué à tous les algorithmes. **Tout algorithme, qu'il traite ou non des données personnelles, doit être loyal envers ses utilisateurs, non pas seulement en tant que consommateurs, mais également en tant que citoyens**. Questions rhétoriques : peut-on parler d'« éthique des algorithmes » et comment appréhender ces robots humanisés ?

Les algorithmes reposant sur l'intelligence artificielle seront particulièrement difficiles à analyser par les autorités de concurrence. Ils reposent sur des architectures de nombreuses interconnexions. L'utilisation des algorithmes par les industries culturelles contribue à la diversité en facilitant la découverte d'œuvres audiovisuelles. Mais ils peuvent également conduire à des effets inverses, à savoir enfermer les individus dans une personnalisation des services en fonction de leurs goûts et opinions. Les algorithmes sémantiques sont vraisemblablement les plus favorables à la diversité culturelle mais ils sont aussi les plus coûteux. Les algorithmes statistiques créent un risque d'enfermement du consommateur dans une bulle culturelle.

« L'économie de l'algorithme sera à l'origine du prochain grand saut de l'évolution du *machine to machine* vers l'Internet des objets. Les produits et services seront déterminés selon la sophistication de leurs algorithmes et de ce qu'ils offriront. Les organisations ne seront pas seulement évaluées en fonction de leurs gros volumes de données mais par leurs algorithmes qui transformeront ces données en actions pour finalement impacter le consommateur »[17].

L'utilisation des algorithmes par les industries créatives peut avoir des effets plus ou moins importants sur le développement d'une offre riche et diversifiée. Pour préserver le libre choix de l'individu et de lui permettre de contextualiser les recommandations personnalisées, il est nécessaire d'assurer un certain degré d'information du consommateur sur les mécanismes directeurs des algorithmes.

Quelques systèmes, comme IBM Watson avec le jeu Jeopardy, ont médiatisé les avancées de l'intelligence artificielle (IA). Ces grands systèmes sont complexes, associant de multiples algorithmes, selon différentes technologies. Pour leur développement, surtout depuis deux ans, les grands du numérique américains investissent des milliards dans des capacités de calculs et de stockage.

Les algorithmes de personnalisation visent principalement à respecter un principe général de non-discrimination et à rendre plus transparents les modes de collecte, de traitement des données et de restitution de l'information. La loyauté des algorithmes participe de fait à créer davantage de confiance.

L'algorithmique statistique, comme moyen de profilage, crée les conditions d'un dialogue homme-machine simulant un dialogue réel entre un utilisateur et un expert. L'algorithmique statistique ne fait que recycler une information à la sphère de l'utilisateur. Les entreprises cherchent à créer des écosystèmes

autour d'algorithmes propriétaires aux performances inégalées, s'appuyant sur des communautés de développeurs et chercheurs en IA. La division spécialisée d'IBM dans le domaine de la santé, le Watson Developer Cloud, est une plateforme qui associe 400 Watson Ecosystem partners développant des produits. En janvier 2016, par exemple, Sopra Steria a annoncé la création d'un centre de compétences cognitives IBM Watson [73].

11.2.2. Conséquences de l'IA sur le travail de l'avenir

Pour imaginer les conséquences de l'IA sur le travail de l'avenir, il faut étudier l'historique du développement technologique. Les résultats des recherches sont différents. **Les chercheurs de l'Université d'Oxford Carl Frey et Michael Osborne ont publié une étude portant sur différents types d'emplois pour calculer d'entre eux la probabilité d'automatisation. Cette étude concluait que** 47 % des emplois américains étaient menacés par l'automatisation dans les 20 années à venir**.**

Des travaux plus récents réalisés par les chercheurs Melanie Arntz, Terry Gregory et Ulrich Zierahn estiment que l'approche par métiers de Frey et Osborne ne donne pas la possibilité de restituer une image réelle. **Elle estime qu'environ 9 % des emplois pourraient disparaître du fait de la robotisation et l'adoption d'outils d'IA remplaçant le travail humain [146]**.

Une autre étude de France Stratégie estime pour la France que le **nombre d'emplois facilement automatisables à l'horizon 2025 serait d'environ 3,5 millions soit 15 % de l'emploi total**, tandis que ceux qui ne sont pas du tout automatisables s'élèvent à plus de 9 millions.

Selon la dernière publication de *l'International Federation of Robotics,* en France, il y une densité de robots industriels plus faible que dans ses voisins européens. On comptait ainsi 154 robots pour 10 000 employés dans l'industrie française, contre respectivement 200 en Italie, 188 en Belgique et 168 en Espagne [121 ; 13-16].

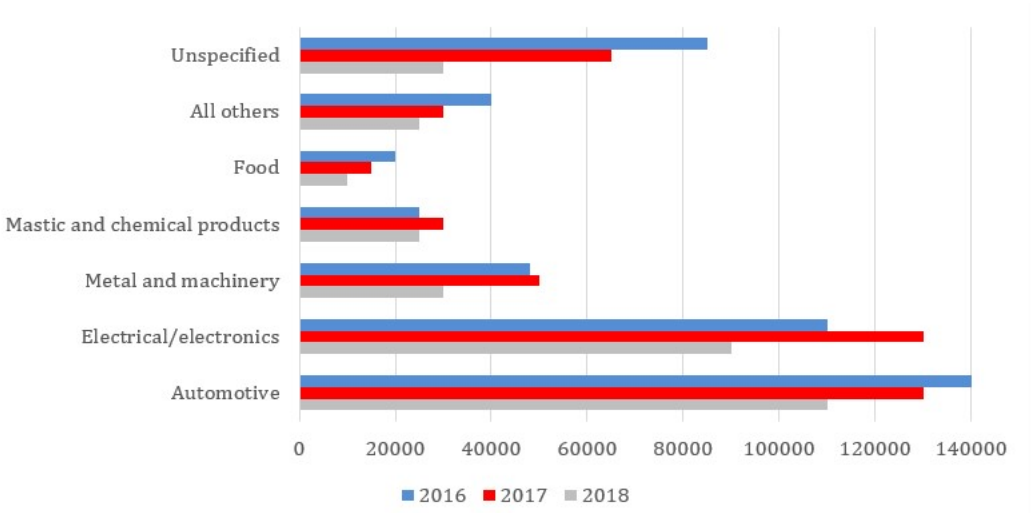
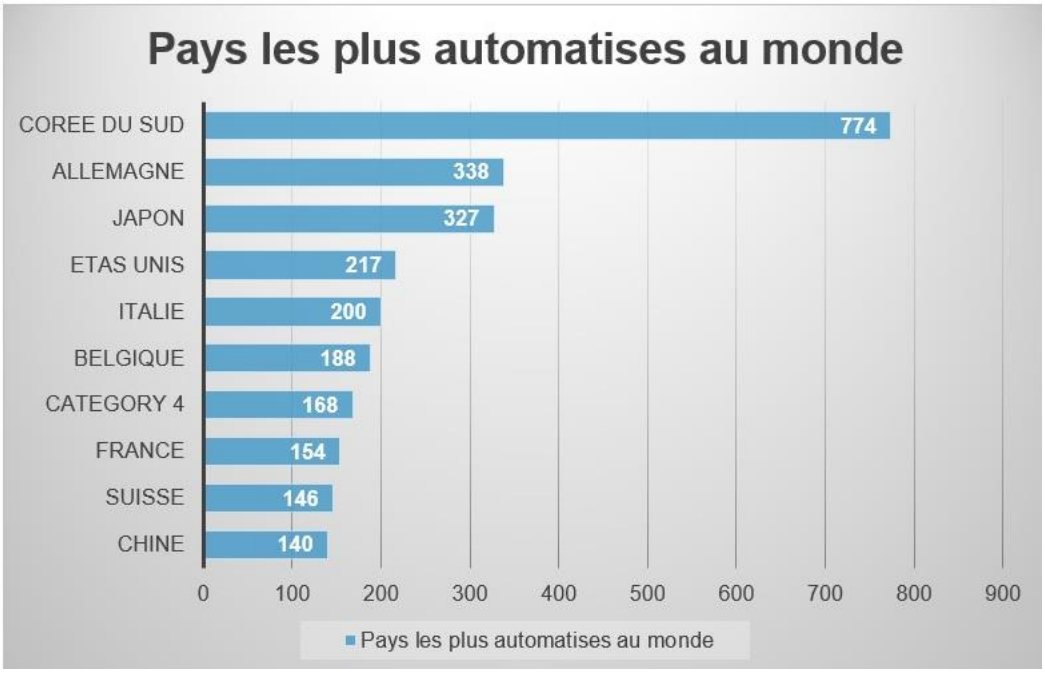


Fig. 26: *Sommaire executif robotics, 2019, Source International federation robotics*

Fig. 27 : *Pays les plus automatisés, Source : GAUDIAUT Tristan, « Les pays les plus robotisés au monde », 21 novembre 2021, [104]*



11.3 Algorithmes et vérification des données

L'utilisation algorithmes dans le système de vérification pose des défis non seulement pour le secteur dans lequel ils sont exploités, mais aussi pour la société. Surtout, l'impact des algorithmes sur le développement de la technologie et du droit de l'homme est particulièrement intéressant. Des nombreuses définitions, nous pouvons choisir la plus marquante : l'IA est une discipline (processus) scientifique visant à exécuter des processus cognitifs par des machines (ordinateurs et programmes informatiques). Les systèmes d'IA ne peuvent être que logiciels, (reconnaissance faciale) ou être intégrés dans des dispositifs matériels (voitures autonomes). Le système de l'IA a beaucoup d'avantages : rapidité d'exécution, exactitude, coûts… mais il porte en soi un effet négatif et risqué pour non-respect de la vie privée.

Selon 1000 dirigeants d'entreprise américains interrogés, plus de 20% des entreprises utilisent l'IA et leur organisation prévoit d'améliorer ce système. La plupart des dirigeants savent que l'intelligence artificielle (IA) a le pouvoir de changer presque tout dans le business et pourrait contribuer jusqu'à 15,7 billions de dollars à l'économie mondiale d'ici 2030. Mais ce que de nombreux chefs d'entreprise ne savent pas, c'est comment déployer l'IA, dans toute l'organisation, pour créer une valeur maximale [8].

Ces systèmes d'IA peuvent configurer et optimiser la réalisation de l'objectif global sur une échelle globale qui était impossible avant internet. Par exemple, un système de navigation par IA peut permettre à chaque conducteur de gagner sa destination le plus rapidement possible [190 ; 25].

L'un des défis important posés par l'IA est sa capacité à fonctionner de manière très ciblée à l'échelle d'une population très grande. Pour mesurer le niveau d'intelligence d'une machine, il faut définir une tâche

que l'on considère comme complexe à accomplir. D'autre part, il existe l'expérience **« test de Turing »** (Alan Turing en 1950) pour tester l'intelligence de la machine. Celui-ci consiste à faire discuter une machine avec un être humain. Si l'être humain n'arrive pas à conclure si c'est une machine ou un humain, c'est que la machine a suffisamment « d'intelligence ».

Il faut souligner qu'une tâche difficile pour une machine n'est pas aussi difficile à effectuer pour un être humain et au contraire, une machine peut accomplir telle tâche que l'être humain n'aurait jamais imaginé faire (il s'agit du paradoxe de Moravec).

Nous savons que depuis 1997, avec la victoire de Deep Blue sur le champion du monde Gary Kasparov, une étape importante a été marquée. « Lorsque Deep Blue m'a battu, il a été clair que les machines allaient supplanter les êtres humains dans tous les environnements comparables, c'est-à-dire les systèmes fermés où il s'agit d'atteindre un but spécifique en respectant des règles données. J'ai commencé à mesurer la largeur du panel d'activités qui allaient pouvoir être assistées par la technologie » déclare Garry kasparov [127].

Nous pouvons imaginer l'effet à l'inverse. Un chatbot Tay « bien intelligent » sur Twitter a été retiré au bout de 24h car il avait « appris » des propos racistes sous l'action de certains utilisateurs.

Dans notre vision, la question de la cohabitation de l'IA avec la protection des données est intéressante. La loi pour une République numérique prévoit que les administrations mettent en œuvre un traitement algorithmique qui aboutit à une décision individuelle. Les algorithmes occupent une place importante dans notre vie quotidienne : résultats sur un moteur de recherche, actualité sur les réseaux sociaux, recommandations sur des sites de e-commerce, démarches financières effectuées par des robots sur les marchés, diagnostics médicaux automatiques… des algorithmes sont présents dans tous ces domaines.

Les décisions individuelles ne doivent pas être prises sur la seule base d'un algorithme. En revanche, les algorithmes peuvent être utilisés comme un outil d'aide à la décision.

Aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité [139 : article 10].

Bien évidemment, l'avis de la société française sur ce sujet est intéressant. Une enquête a été menée auprès d'un échantillon de 1001 personnes, représentatif de la population française âgée de 18 ans et plus (par la Cnil) : pour 72 %, l'IA est un enjeux pour la société [36].

Fig. 28 : *L'intelligence artificielle et ses enjeux. Source : Sondage Ifop pour la CNIL, 2017*

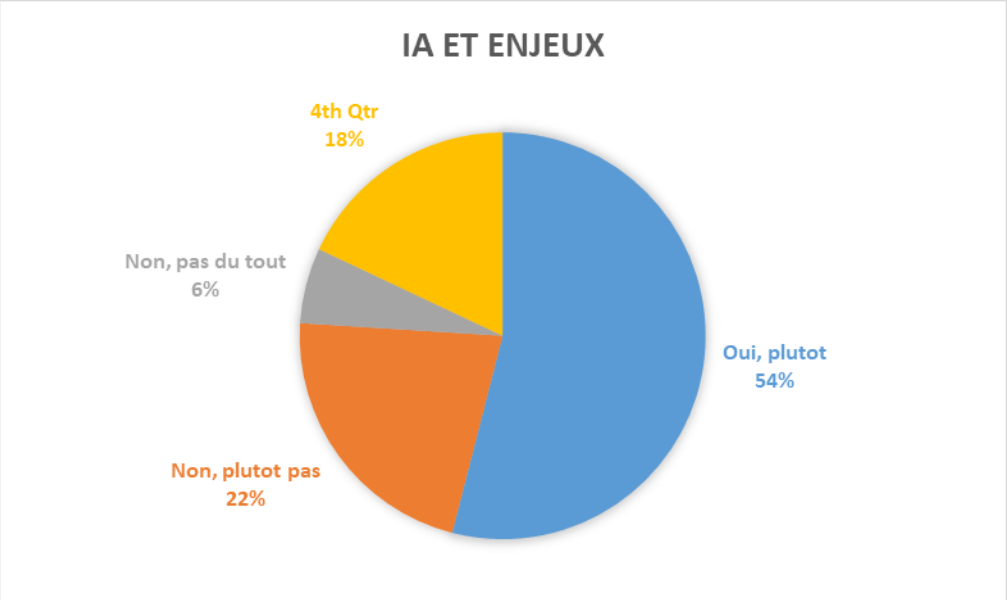
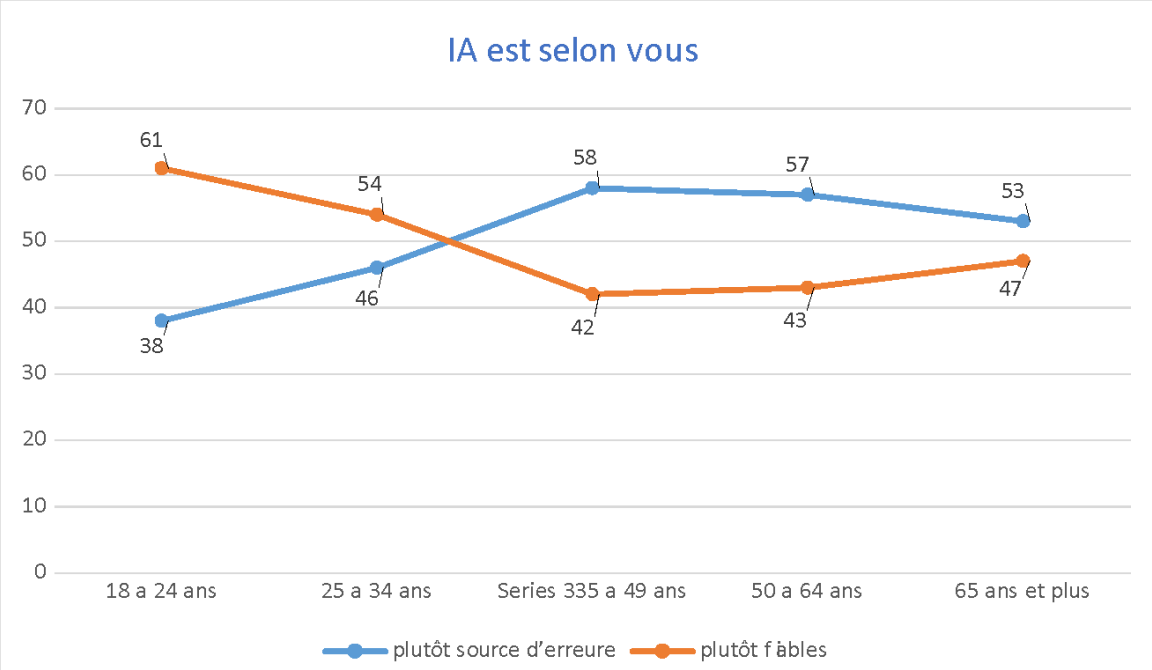


Fig. 29 : *L'IA et la perception des consommateurs. Source : Sondage Ifop pour la CNIL, 2017*



Les algorithmes sont un sujet connu des Français mais de façon assez ambiguë. 83% des Français ont déjà entendu parler des algorithmes, mais presque la moitié ne sait pas précisément de quoi il s'agit (52%) [36].

11.4 Utilisation des algorithmes dans des différents secteurs

Au niveaux des pays - On définit l'échange automatique de renseignements comme la transmission systématique et régulière d'un gros volume d'informations concernant des contribuables, qui sont

communiquées au pays de résidence par le pays de la source et concernent diverses catégories de revenus (par exemple les dividendes, intérêts, redevances, salaires, pensions, etc [153].

La notion de l'échangé automatique de renseignements repose généralement sur la clause d'échange de renseignements d'une convention de double imposition [152]. L'échange automatique de renseignements est largement utilisé, tant au sein de l'Union europeenne (UE) qu'en dehors de celle-ci. Les 38 pays (100%) reçoivent tous automatiquement des renseignements des partenaires conventionnels. Par ex. : Le Danemark, pays qui a le plus de relations d'échanges automatiques de renseignements, envoie des renseignements automatiquement à 70 pays. **Certains pays demandent un mémorandum d'accord (MOU) stipulant les conditions de l'échange automatique proposé.** Ce mémorandum contient une description détaillée des procédures d'envoi et de réception des informations.

L'OCDE a rédigé un Modèle de Mémorandum d'accord sur l'échange automatique de renseignements qui peut servir de base à un accord. L'échange automatique offre l'avantage de lutter contre l'indiscipline fiscale offshore. Il peut livrer en temps des informations sur l'absence de déclaration fiscale.

Le cas du Danemark et de la Norvège a montré le risque de dissimulation de revenus de source étrangère. En 2009, la Norvège a reçu des informations de plusieurs pays. Au-dessus d'un certain seuil, les fichiers ont été comparés avec les déclarations de revenu déposées par les contribuables**. On constate de l'enquête que, dans 38.7 % des cas, des revenus imposables en Norvège n'avaient pas été déclarés**.

L'OCDE travaille régulièrement à l'élaboration de normes juridiques et techniques de contrôle automatisée. Le procès est assez difficile car les informations doivent être échangées et traitées sous les standards de la protection de la vie privée. Le Conseil de l'Union européenne a adopté des formats standard pour la mise en œuvre de la Directive de l'Union Européenne sur les revenus de l'épargne. Il a également adopté en 2011 une nouvelle Directive sur l'entraide administrative qui prévoit l'élaboration de nouveaux formats pour quelques types de revenus : revenus d'activité, revenus immobiliers, pensions et produits d'assurance vie non couverts par un autre texte de l'UE sur l'entraide administrative. Pour concevoir ces formats, l'Union européenne collabore étroitement avec l'OCDE dans le but de l'échange automatique de renseignements. Dans le cas de **la France, pour mettre en place un traitement automatisé d'informations nominatives, on doit informer la CNIL.**

Si dans une organisation, le système d'évaluation est informatisé, l'employeur doit effectuer une déclaration auprèss de la CNIL. Si le support d'entretien annuel est un document manuscrit, ils doivent être constitués et utilisées conformément aux principes et exigences de la CNIL.
Le système de vérification automatisée est assez répandu dans les entreprises. L'employeur peut mettre en place des logiciels permettant de surveiller les connexions des salariés à internet (sites visités, messages envoyés). Il peut en limiter l'accès, ce qui ne constitue une atteinte à la liberté des salariés. L'employeur qui souhaite introduire des nouvelles technologies dans l'entreprise doit informer et consulter les représentants du personnel et informer les salariés. L'employeur doit communiquer les éléments d'information au moins un mois avant la réunion [60], quels que soient les moyens de contrôle mis en place dans l'entreprise, la direction doit **obligatoirement en informer au préalable les salariés**. Aucune information concernant personnellement un salarié ne peut être collectée par un **dispositif** qui n'a pas été **porté préalablement à sa connaissance [59].**

Les nouvelles méthodes de collecte et de traitement des données présentent certains risques pour les travailleurs. Différentes lois nationales et normes internationales assujettissent le traitement des données personnelles à des règles différentes. Toute personne ayant accès aux données personnelles des travailleurs devraient être tenue à l'obligation de confidentialité.

En principe, toutes les données devraient être obtenues du travailleur lui-même. S'il s'avère nécessaire de se procurer des données personnelles auprès de tiers, le travailleur devrait en être informé à l'avance et donner son consentement explicite**.** L'employeur ne devrait pas collecter de données personnelles concernant :

- La vie privée
- Les opinions politiques, religieuses
- Les condamnations pénales des travailleurs

L'employeur peut, dans des circonstances exceptionnelles, collecter des données personnelles mentionnés ci-dessus, à condition que ces données soient directement liées à une décision en matière d'emploi [124].

Des données médicales personnelles ne devraient être collectées que d'une manière conforme à la législation nationale, à la confidentialité médicale.

Le traitement automatisé de données à caractère personnel est un moyen irremplaçable pour la presse. Les journalistes travaillent en direct, avec les bases de données publiques, les archives informatisées des grandes institutions. La diffusion des documents publics sur les différents réseaux permet le libre accès aux documents. Les rapports publics, les textes juridiques, deviennent accessibles directement, en ligne. L'automatisation des procédures garantit :

- L'objectivité du traitement des administrés ;
- L'accélération du traitement des dossiers ;

Les informations automatisées sont indispensables à la lutte contre le terrorisme et la grande délinquance financière. Au niveau de la santé, la Carte Sésame/ Vital permettra au praticien de disposer des informations de base sur le patient et de transmettre directement sa feuille de soins aux caisses d'assurance-maladie. Comme les informations sur la santé sont les données très sensibles, le réseau santé-social s'appuiera sur un système de cryptologie, qui ne donnera l'accès à l'information qu'à un destinataire déterminé.

C'est la facilité de transfert et d'analyse des données d'un opérateur à un autre qui comporte de nombreux risques liées à la protection de la vie privée. La nature de l'information traitée n'est pas l'atteinte à la vie privée. L'abus de droit consiste en collecte de données sans le consentement de l'intéressé.

Les internautes s'intéressent souvent aux moyens de protection lorsque les informations les concernant font l'objet de flux transfrontaliers. **Lorsque le traitement automatisé de données à caractère personnel met son produit dans différents pays (d'une banque de données dans un pays relié à des terminaux dans d'autres pays), il était difficile de déterminer quel Etat a juridiction et quelle loi nationale est applicable avant RGPD.**

Des personnes résidant dans un pays pouvaient avoir des difficultés lorsqu'elles voulaient exercer leurs droits par rapport aux fichiers automatisés situés dans d'autres pays. Des moyens spécifiques de sécurité devraient être pris pour chaque fichier. Les moyens de sécurité doivent être définis selon le caractère des données. Pour garantir l'efficacité de ces droits, la Convention exige que le nom ou la raison sociale du maître de chaque fichier soit indiqué. Dans certains Etats, le nom du maître du fichier est inscrit dans un répertoire public. Dans la convention [78], il n'est pas précisé de la part de qui une personne concernée peut obtenir les informations sur la confirmation, rectification, etc. Dans certains des Etats, ils sont maîtres (responsables) du fichier, mais dans d'autres, ce droit peut être réalisé par l'autorité de surveillance. Afin que cette Convention puisse garantir une protection des données plus efficace, les buts des utilisateurs et les droits des personnes concernées devraient entrer en corrélation dans la législation nationale des Etats membres.

Le traitement automatisé sans contrôle permanent porte le risque d'un abus du droit de la vie privée. Par exemple, le recensement de la population et les nouvelles techniques de collecte, de conservation et d'utilisation des données sont susceptibles de porter atteinte au respect de droits de l''homme. De plus, un stockage illimité des données risque leurs réutilisations, sans que la personne puisse réellement les

contrôler. La technologie permet aujourd'hui de collecter des informations sur les personnes sans passer par des tiers. Par exemple, la RFID rend possible une telle collecte de données. Même l'identification par radiofréquence (RFID) permet de connaître la localisation des personnes.

Un autre type d'abus peut être la dépossession des personnes des données et leur traitement par des moyens divers. Par exemple, les autotests génétiques via Internet. Les entreprises proposant de tels tests recueillent, lors de l'analyse, des caractéristiques génétiques des personnes. Plusieurs centaines des données peuvent être utilisée à des fins diverses. Une fois les informations obtenues, elles ne peuvent s'opposer à leur utilisation à des fins de recherche. Un grand risque est apparu lors du lancement du projet de banque de données médicales et génétiques de la population. Il est vrai que la recherche génétique, pour l'établissement des corrélations entre gènes et une maladie, peut nécessiter de recourir à une grande quantité de données. La recherche génétique « recouvre un domaine très sensible." Ce n'est pas l'accumulation de tissus humains obtenus dans des circonstances diversifiées qui est le problème le plus crucial, mais bien l'accumulation d'informations sur une même personne. "[183]

La CNIL a mis en place une procédure simplifiée de déclaration en homologuant une méthodologie de référence pour les traitements de données personnelles mis en œuvre dans le cadre des recherches biomédicales, traduisant ainsi, dans le secteur de la recherche, la volonté de simplifier les formalités pour des applications conduites dans le cadre d'exigences législatives et réglementaires strictes [38]. L'information génétique et son traitement automatisé sont des sujets très importants pour les organisations connues. L'information génétique, considérée comme propre à l'humanité toute entière, est l'objet de la défense de UNESCO. Dans sa Déclaration universelle sur le génome humain, elle recommande de prendre des mesures pour que « les résultats de la recherche génétique ne servent pas à des fins non pacifiques. »

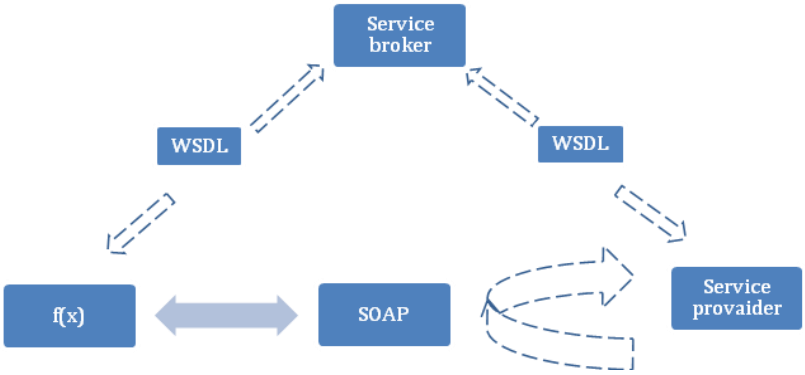
La CNIL considère que « une prise de sang effectuée dans le cadre de la conduite d'un essai de pharmacogénétique destiné à évaluer l'efficacité d'un médicament au regard du profil génétique ne devrait pas pouvoir être utilisée ultérieurement pour déterminer l'empreinte génétique de la personne dans le cadre d'une recherche de paternité. » [28 ; 210] Une recherche de l'INSERM sur les liens entre comportements et délinquance à l'adolescence pose questions [122 ; 133-159]. Un lien a été établi entre le fait d'être turbulent à trois ans et le fait de commettre des actes antisociaux à l'adolescence. Les associations de défense de l'enfance ont rejeté de telles recherches. Si on généralise les décisions des recherches, elles peuvent être définies comme un abus des droits des personnes.

11.5 Service Web et Protocole de sécurité

Service Web est un système logiciel pour permettre l'interaction entre les machines à l'aide d'un réseau. Un service Web possède une interface décrite dans un langage qu'une machine peut lire et traiter.

WSDL C'est le format standard pour décrire un service Web. WSDL a été développé conjointement par Microsoft et IBM. WSDL est souvent utilisé en combinaison avec SOAP et XML Schéma pour fournir des services Web sur Internet. Un programme client se connectant à un service Web peut lire le WSDL pour déterminer quelles fonctions sont disponibles sur le serveur.

Fig. 30 : *Protocole de sécurité*



Un document WSDL comporte divers éléments, mais ils sont contenus dans les trois éléments principaux : Types, Operations, Obligations. Code d'Exemple WSDL message

Fig. 31 : *Code d'Exemple WSDL message, Source : Message Sets: WSDL generation, IBM*

<message name = "SayBonjourRequest">

<part name = "firstName" type = "xsd:string"/>

</message> <message name = "SayBonjourResponse">

<part name = "greeting" type = "xsd:string"/>

</message>

L'élément « service » définit les ports pris en charge par le service Web. Pour chacun des il existe un élément de port. L'élément de service est un ensemble de ports. Les clients du service Web peuvent apprendre ce qui suit.

Fig. 32 : *Code des éléments*

```
<service name = "Bonjour_Service">
  <documentation>WSDL File for BonjourService</documentation>
  <port binding = "tns:Bonjour_Binding" name = "Bonjour Port">
    <soap:address
      location = "http://www.examples.com/SayBonjour/">
  </port>
</service>
```

Les attributs de liaison de l'élément port associent l'adresse du service à un élément de liaison défini dans le service Web. Dans cet exemple, il s'agit de Bonjour_Binding

Fig. 33 : *Intégration des modèles*

```
<binding name =" BONJOUR_Binding" type = "tns:BONJOUR_PortType">
  <soap:binding style = "rpc"
    transport = "http://schemas.xmlsoap.org/soap/http"/>
  <operation name = "sayBONJOUR">
    <soap:operation soapAction = "sayBONJOUR"/>

    <input>
      <soap:body
        encodingStyle = "http://schemas.xmlsoap.org/soap/encoding/"
        namespace = "urn:examples:BONJOURservice" use = "encoded"/>
    </input>

    <output>
      <soap:body
        encodingStyle = "http://schemas.xmlsoap.org/soap/encoding/"
        namespace = "urn:examples:BONJOURservice" use = "encoded"/>
    </output>
  </operation>
</binding>
```

11.6 *Privacy by design* et modèle de belge de transfert des données

Pour respect de la vie privée on utilise le système de la décentralisation des données ainsi on diminue les risques d'atteinte a la vie privee. Dans ce contexte il est très intéressant *Privacy by design*. Selon ces concepts les moyens législatifs ne sont pas suffisants pour garantir la protection de la vie privée. D'après le commissaire européen de la concurrence « Ce que nous voyons en Europe c'est qu'il y a une grande proportion de citoyens qui trouvent qu'ils n'ont pas le contrôle. Ils ne font pas confiance dans les entreprises pour protéger leurs données, et je pense que c'est néfaste, parce qu'il y a alors un risque qu'ils se retirent de tous les bénéfices de notre économie numérique. Et pour construire la confiance, je pense qu'il est très important que nous fassions respecter les règles de protection de la vie privée, que nous ayons le " privacy by design" dans de nouveaux services, pour que la vie privée ne soit pas juste un add-on, mais qu'elle soit vraiment à la base » [23]

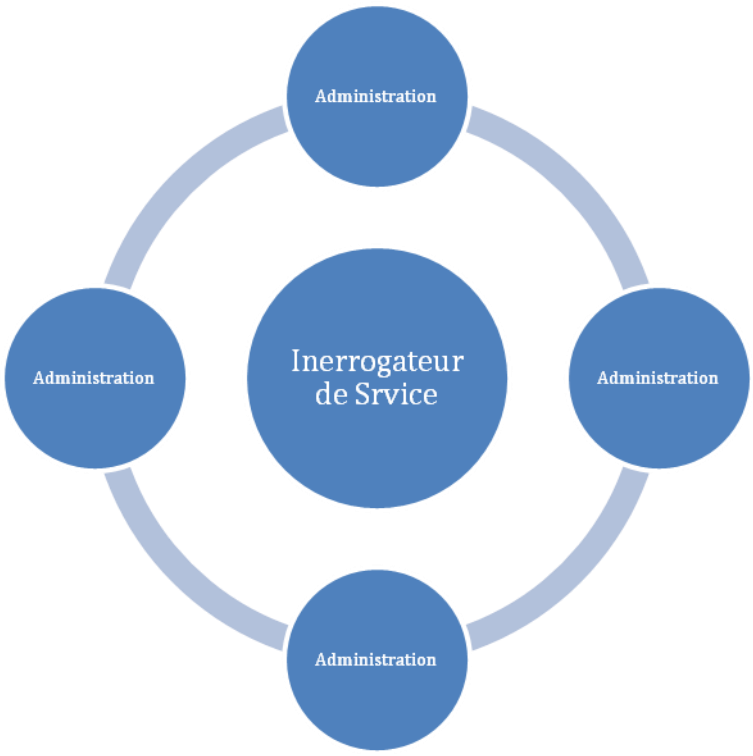
En 2010, ce concept a fait l'objet d'une résolution adoptée par les commissaires à la protection des données et de la vie privée. Dans ce document le commissaire souligne la nécessite de l'incorporation de la privacy dans la politique de confidentialité et de la législation. Commissaire s'exprime également pour ajouter Privacy by Design à l'ordre du jour des événements qui se déroulent à Journée internationale de la confidentialité des données (28 janvier) [1].

Pour le respect de la vie privée et en même temps pour l'échange des informations entre administrations, certains pays utilisent un modèle administratif d'après lequel un intégrateur de services assure l'échange des données entre les administrations concernées. Donc, les données sont enregistrées de manière décentralisée au sein de l'administration et sont échangées par un intégrateur de services. Le premier réseau du genre est le réseau de la sécurité sociale, qui regroupe les institutions de sécurité sociale [87 ; 71-86]

Utilisant ce système Il est pratiquement impossible pour un tiers d'accéder aux données centralisées en un seul accès. il n'existe pas aucun numéro d'identification global mis en place. Ce fait renforce le niveau de sécurité. Chaque citoyen possède un numéro d'identification propre à chaque réseau ce qui empêche les références croisées d'un réseau à l'autre. Dans l'hypothèse pour accéder aux données d'un citoyen devrait mener une tentative d'accès à chaque source authentique de données, ce qui réduit les risques d'accès. Par contre Chaque source de données se doit fournir le niveau de sécurité pour assurer le bon fonctionnement de sécurité entière. **Il faut souligner que même les usagers ne possèdent pas d'accès central à leurs propres données. Un tel portail serait une garantie pour la protection de la vie privée conservant le droit à l'information et à la transparence**.

Le modèle belge d'e-gouvernement est un bon exemple de l'administration qui est à la fois efficace et garant de la protection de la vie privée. L'automatisation de certains droits, l'informatisation de la lutte contre la fraude, l'accès à des formulaires en ligne sont les pas avancées dans relation entre l'administration et citoyens. C'est un Schéma illustrant un réseau d'administrations composé d'un intégrateur de services auquel sont reliées plusieurs administrations.

Fig. 34 : *Le modèle belge de l'interrogateur de services*



D'après le gouvernement belge la multiplication d'intégrateurs de services verticaux crée une difficulté pour les administrations. Par exemple les administrations doivent s'adresser à différents intégrateurs de services en fonction du type de donnée et chaque fois doivent attendre des procédures particulières. Pour améliorer le service et gagner le temps on a créé des intégrateurs de services dits » horizontaux » qui regroupent des administrations en fonction de leur appartenance à l'entité fédérale. Ils comprennent un intégrateur de services chargé d'assurer la circulation des données entre les administrations concernées.

11. 7 Méthodologies de contrôles des fichiers automatisées

En ingénierie logistique Zave et Jackson [191] définissent les exigences de logiciels souhaitables et distinguent les systèmes par leur capacité à exercer un contrôle sur l'environnement . De plus, ils identifient le défi auquel les ingénieurs sont confrontés en distinguant les descriptions du domaine et les descriptions des systèmes. Ce dernier comprend les exigences et les spécifications du système.

Pour faire valoir que les logiciels sont conformes à une réglementation, les ingénieurs doivent utiliser la traçabilité des descriptions réglementaires du mode aux exigences et aux spécifications du système. Les ingénieurs doivent encore justifier que leur interprétation des règlements soit valide et conforme à leurs spécifications et que les comportements du système ne contredisent pas ces interprétations.

Dans les exigences et l'ingénierie logicielle, les chercheurs ont étudié les méthodes d'analyse des exigences de sécurité en utilisant les aspects ' les objectifs, les cadres des problèmes [129] argumentations.

Les travaux plus récents se concentrent sur des exigences des règlements de la sécurité [145]. Cette approche est semblable au logique déontique qui est formalisation les rapports entre les quatre caractéristiques d'une loi : **l'obligation, l'interdiction, la permission et le facultatif.**

Au Etas Unis la méthodologie d'accès et de contrôle au système des soins est assez structuré et défendue. La méthodologie a été validée dans une étude pilote qui utilise une fiche d'information sur le patient qui résume la règle de confidentialité HIPAA « Le Health Insurance Portability and Accountability Act « (HIPAA)et dans une plus grande étude de cas qui utilise quatre sections de la règle de confidentialité [171].

La méthodologie d'ingénierie des exigences pour les règles de codage à partir des règlements examinés a été développée à l'aide de Grounded Theory.[110] Bien que la méthodologie ait été validée uniquement en utilisant des documents liés à HIPAA, en fonction des certaines expériences dans le développement de méthodologies, un grand nombre des scientifiques pensent que cette methodologie est generalizable au-delà de HIPAA [6].

La méthodologie requiert des exigences pour analyser chaque déclaration dans un texte de règlement et identifie l'énoncé comme définition, droit, obligation ou contrainte. Comme mentionné précédemment, les déclarations de droit et d'obligation peuvent contenir des contraintes sur diverses propriétés, telles que le sujet ou le destinataire dans une divulgation d'information.

La méthodologie a été appliquée pour extraire les droits et les obligations [13].

Dans le but de construire le tableau des règles, nous pouvons définir quelques propriétés dans les activités liées à l'accès à l'information :

- Le sujet est l'acteur qui effectue une action sur un objet ;
- L'action est un verbe qui affecte des informations telles (l'accès, l'utilisation) ;
- La modalité modifie l'action en désignant l'action comme un droit ;
- L'objet est limité à l'information (le nom ou la date de naissance d'un patient) ;
- L'objectif est le destinataire dans une transaction telle que le destinataire d'une divulgation ;
- Le but est l'objectif d'une activité (les informations sur le patient peuvent être utilisées à des fins de facturation).

En décembre 2000, le Conseil de conformité des États-Unis (la Commission d'accès) a publié « Électronique normes d'accessibilité en technologie de l'information ». Ces normes exigent que les entreprises de technologie demandent des contrats de passation afin d'aligner les normes sur leurs

produits de technologie de l'information. Les normes d'accessibilité contiennent les sous-parties. La sous-partie intitulée « Généralités », comprend le but, la compétence, les exceptions et les définitions juridiques. La sous-partie B est « Normes techniques ». Une méthode de développement de systèmes multi-agents est constituée d'un processus, de notations et d'outils pour prendre en charge ce processus. L'objectif d'une méthode est de guider un utilisateur tout au long du processus de développement. Les phases principales d'une méthode sont les suivantes :

- L'analyse des besoins ;
- L'analyse, appelée conception de l'architecture. Elle décrit le problème à résoudre par le système ;
- La conception détaillée, (les mécanismes à utiliser) ;
- Le développement (codage et d'intégration d'un logiciel) ;
- La phase de maintenance (corriger d'éventuelles erreurs);

L'Open Data permet l'ouverture et le partage de données gratuitement par toute personne intéressée (organisme public ou privé). Il existe déjà plusieurs bases publiques de données en accès libre et gratuites.

L'ouverture des données de santé est une **facilitation de l'accès anonymisé aux données individuelles de l'Assurance Maladie regroupées dans le SNIIRAM** (Système national d'informations inter-régimes de l'Assurance Maladie). Outre la facilitation de l'accès au SNIIRAM et aux PMSI et leur enrichissement avec de nouvelles données, la Commission Open-Data demande sur la nécessaire anonymisation des données des patients (protection de la vie privée). Les données détaillées ayant un risque de ré identification pourront aussi ouvertes, **après avis d'**un **comité technique** (experts et scientifiques indépendants) et d'un **comité d'orientation** s'il ne s'agit que d'une recherche académique. **Ces comités pourraient se situer au sein de l'institut de santé.** Cet organisme gère déjà l'accès aux données disponibles, comme celles du SNIIRAM pour éviter une utilisation abusive ces informations. Selon leur recommandation toutes Ces données doivent être anonymisées et leur utilisation contrôlée.

Malgré la création d'un système national des données de santé (SNDS) il reste encore beaucoup à faire pour que l'*Open data* en santé devienne une réalité. Organisme COTSAM, regroupant non plus seulement des professionnels de santé et des experts mais aussi d'autres acteurs (Etat, régimes d'assurances). Créé par une loi d'août 2004, l'Institut des données de santé (IDS) a pour mission « d'assurer la cohérence et de veiller la qualité des systèmes d'information utilisés pour la gestion du risque maladie. L'accès aux données de santé doit être réservé uniquement aux personnes désignées.

En France, malheureusement certains hôpitaux n'ayant pas des logiciels d'anonymisation des données pour ce genre d'analyses met en danger la protection de notre vie privée. La CNIL a participé aux nombreux chantiers de la e-santé aux côtés de l'ASIP Santé Le but de contrôle est d'amener les acteurs de la santé au plus haut niveau de sécurité. "Les données concernant les personnes physiques ne peuvent être communi quées que sous forme de statistiques agrégées et d'informations constituées de sorte que ces personnes ne puissent être identifiées » [12]

La loi « études en santé publique » a prévu autorisation de l'accès aux données du SNIIRAM pour des études de vigilance et d'épidémiologie impliquant notamment des médicaments. Laboratoires pharmaceutiques sont intéressées à utiliser le SNIIRAM pour réaliser leur propre études afin de vérifier des paramètres de leurs produits. Ainsi que elle peut favoriser le développement d'une recherche publique ou privée en santé. **Si les données Présentent un risque de l'identification, il serait légitime de restreindre les accès et renforcer le contrôle. Au contraire si les données ne sont pas Indirectement nominatives elles doivent être communicables**.

Une autre approche de la modélisation des réglementations utilise techniques de contrôle d'accès pour identifier les informations relatives aux éléments de textes juridiques. La mise en œuvre du système de

confidentialité vérifiable remplit certaines tâches d'ingénierie des exigences, mais il ne peut pas soutenir adéquatement les besoins complexes des exigences travaillant avec les textes légaux. May et lee. utiliser un langage de modélisation pour représentent des textes juridiques et des politiques de confidentialité, permettant ainsi opérations de contrôle et de vérification des modèles [145]. Les politiques réglementaires diffèrent de nombreuses politiques classiques de confidentialité et de contrôle d'accès dans leur utilisation.

Transfert Quel est le droit d'un agent de transférer une information à un autre ?

Action Quel est le droit d'un agent d'accomplir une action qui peut affecter la vie privée ?

Création de données Quels agents sont autorisés à créer un objet ?

Notification Lorsqu'un agent a effectué une action sur ou transfère un objet qui doit en être informé ?

11.8 Le cloud et les fichiers automatisés

La CNIL constate que le Cloud computing pose des difficultés au regard du respect de la législation relative à la protection des données personnelles. Ces difficultés sont nombreuses dans le cas des offres standardisées avec des contrats d'adhésion ne laissant pas aux clients la possibilité de les négocier. En générale, les clients n'ont pas l'information suffisante sur la sécurité et sur la destination du transfert des données vers pays étrangers.

La CNIL conseille aux entreprises françaises qui envisage de recourir à un service de Cloud computing réalise une analyse de risques et soit très rigoureuse dans le choix de son prestataire [45].

L'entreprise devra soigneusement analyser les garanties offertes par un prestataire en matière de protection des données personnelles et s'assurer qu'il lui fournira les garanties nécessaires au niveaux respect de ses données au regard de la loi Informatique et Libertés. En cas d'impossibilité de négocier un contrat, une comparaison des conditions contractuelles proposées par les différents prestataires est indispensable. Dans ce cas l'entreprise aura la possibilité d'effectuer un choix considérant les aspects économiques juridiques et techniques.

La CNIL a établi les recommandations pour aider les entreprises françaises, notamment les PME, à effectuer une prise de décision éclairée lorsqu'elles envisagent d'avoir recours à des prestations de services de Cloud computing. Ces recommandations doivent être formalisés dans les contrats de prestation de services.

Certains types de données sont soumis à une réglementation spécifique, il est obligatoire de vérifier si les données qui pourraient être transférées dans le Cloud sont soumises à de telles obligations. Par exemple, les données de santé ne peuvent être stockées que par un hébergeur de données de santé agréé par le ministère de la santé [45].

11.8.1 Recommandation de la CNIL

La commission recommande d'identifier le type de cloud. Il existe différentes offres de services de Cloud computing, qui peuvent être distinguées selon des modèles de services et modèles de déploiement. Les modèles de services sont les suivants :

- SaaS : Software as a Service, la fourniture de logiciel en ligne ;

Le contrat SaaS permet de commercialiser un logiciel, développé pour être utilisé via le web, non pas en l'installant sur un serveur interne ou un poste de travail dans l'entreprise, mais **en tant qu'application accessible à distance par d'Internet**, comme un service en ligne. Les obligations des parties pourront éventuellement être modifiées et adaptées. Ce model laisse la faculté de choisir les conditions de résiliation pour qu'elles s'adaptent aux exigences du prestataire et/ou du client.

Les avantages du SaaS présentent un impact budgétaire et la rapidité de déploiement lorsque le logiciel SaaS correspond exactement au besoin (et qu'il ne nécessite aucune adaptation)

Le niveau de confidentialité des données ou des documents dépend de la législation du pays de l'hébergeur. La délocalisation des serveurs de la solution SaaS permet également un accès nomade aux données de l'entreprise. Cet accès entraîne un souci de sécurité de l'information lors du départ de collaborateurs. Il est indispensable d'avoir mis en place des procédures permettant, lors d'un départ, de supprimer l'habilitation de l'ancien collaborateur à accéder aux données de l'entreprise**.** En termes de contrôles internes, il est recommandé que le prestataire de service fournisse un certificat de type SSAE16 à son client afin de garantir de la bonne qualité de son propre système de contrôles internes. Le cas échéant, le client doit prendre des mesures compensatoires.

- PaaS : « Platform as a Service », c'est-à-dire la fourniture d'une plateforme de développement d'applications en ligne ;

En général, la stratégie PaaS ne remplace pas l'intégralité des ressources internes d'une entreprise. Les utilisateurs accèdent à une ressource PaaS via un navigateur et une console Web. Les fournisseurs PaaS facturent cet accès « à l'usage ».

- IaaS (type cloud) fournit un socle d'infrastructure informatique virtualisé et capable de répondre aux mises en production des applications de l'entreprise. Ce socle d'infrastructure est composé d'un ensemble de ressources (serveurs, réseaux, stockage) accessibles de façon granulaire.

  La cnil fait la différence entre le cloud public et le cloud privée. On Distingue « Cloud public », pour un service partagé et mutualisé entre de nombreux clients, le « Cloud privé », pour un service dédié à un client et le « Cloud hybride », quand les deux modèles précédents sont combinés. De nombreuses contributions ont rappelé l'importance de ces distinctions [30].

La commission conseille aux entreprises de contrôler le niveau de sécurité et mettre en œuvre certains obligations :

- Garantie que le prestataire n'a pas accès aux données qui lui sont confiées (chiffrement côté client, avec un algorithme reconnu et une gestion des clés adéquates, avant tout transfert)
- Sureté physique sur le site d'hébergement
- Protection du terminal, sécurité des développements applicatifs

La CNIL constate que dans certains cas » les clients de Paas et Saas, ne sont pas en mesure de contrôler l'effectivité des garanties de sécurité et de confidentialité apportées par les prestataires. Cette absence de moyens de contrôle est due à des offres standards, non modifiables par les clients [45]. Le cloud est devenu nécessaire pour les entreprises. Il est destiné à la fois aux entreprises et aux utilisateurs particuliers. Les employés et managers en situation de mobilité l'adopteront naturellement. Le Cloud Computing était compatible avec des systèmes d'exploitation comme Windows, Linux ou encore Apple. Par ailleurs, les services de stockage utilisant la technologie du Cloud Computing peuvent stocker n'importe quel type de fichiers.

Dans ces dernières années plusieurs sociétés ont été créé qui aides aux entreprises de déployer les meilleures technologies du Cloud professionnel pour optimiser et sécuriser patrimoine numérique. Cloud permet une protection contre les catastrophes naturelles ou politiques ; aussi la résilience des données des utilisateurs en cas de panne matérielle ou de catastrophe (inondation, incendie etc.) [117]

Pour Microsoft, le cloud computing désigne l'ensemble des disciplines, technologies utilisés pour délivrer des capacités informatiques (logiciels, plates-formes, matériels), comme un service. Si on cite des inconvénients de Cloud ils sont assez nombreux :

- **Aucun accès physique** à ces données ;
- **Sécurité du stockage** : si les données sont conservées dans un seul disque ;
- **Confidentialité ;**
- **Sécurité des locaux** : sont-ils inaccessibles pour des tiers

Les données transférées dans le cloud ne sont pas forcément présentes sur le territoire national : elles peuvent l'être, elles peuvent être dans un autre pays. Par conséquent on ne sait pas précisément à quel endroit sont stockées les données.

L'externalisation par les entreprises de certaines de leurs activités par le recours à la sous- traitance est aujourd'hui de plus en plus fréquente. Elle est dite « offshore », si elle concerne la création ou l'utilisation d'une entité juridique dans un autre pays : elle a souvent pour but la recherche d'une réduction des coûts, notamment fiscaux, financiers ou salariaux. De plus en plus souvent, les activités sont externalisées dès l'origine dans un pays tiers. Dans les deux cas, lorsqu'elle porte sur des services, elle correspond à la consommation en France de prestations réalisées à l'étranger [46].

Il existe Le terme « nearshore » qui désigne l'externalisation vers des pays utilisant la même langue et situés dans un fuseau horaire identique. Pour la France, le « Near shore » concerne les pays d'Europe de l'Est. Les centres d'appels correspondent d'ailleurs à cette définition, puisqu'il s'agit de confier à un spécialiste un processus de support après-vente des produits, ou un processus de prospection de clients. Depuis quelques années, l'externalisation est très souvent associée au Cloud Computing [46]

Pour traitement légitime des données personnelles, l'organisation doit informer les personnes concernées, avant tout transfert, de ce que leurs données feront l'objet d'un transfert vers un pays tiers. Les personnes concernées doivent être informées de la finalité du transfert, ou des pays destinataires. Ces personnes ont le droit de savoir le niveau de protection offert par le pays destinataires, ainsi que le droit d'opposition d'accès et de rectification.

En général, les traitements automatisés de données à caractère personnel doivent faire l'objet d'une déclaration préalable auprès de la Commission nationale de l'informatique et des libertés [130]. Cette obligation concerne tous les fichiers automatisés de données à caractère personnel, à l'exception de ceux bénéficiant d'une dispense ou ceux soumis à une procédure spéciale d'autorisation.

En 2012 La CNIL a édicté une norme simplifiée concernant exclusivement les traitements de données relatifs à la gestion des clients et de prospects [31].

- Gestion des clients ;
- Contrats ;
- Factures ;
- Service après-vente ;
- Enquêtes ;
- Statistiques commerciales ;

Toute utilisation non expressément prévus par la norme simplifiée n°48 doit faire l'objet d'une déclaration classique ou bien d'une autorisation (suivant les cas, notamment en raison du caractère sensible de la donnée collectée).

11.9. Conclusion

L'utilisation algorithmes dans le système de vérification pose des défis non seulement pour le secteur dans lequel ils sont exploités, mais aussi pour la société. Surtout, l'impact des algorithmes sur le développement de la technologie et du droit de l'homme est particulièrement intéressant. Des nombreuses définitions, nous pouvons choisir la plus marquante : l'IA est une discipline (processus) scientifique visant à exécuter des processus cognitifs par des machines (ordinateurs et programmes informatiques). Les systèmes d'IA ne peuvent être que logiciels, (reconnaissance faciale) ou être intégrés dans des dispositifs matériels (voitures autonomes). Le système de l'IA a beaucoup d'avantages : rapidité d'exécution, exactitude, coûts… mais il porte en soi un effet négatif et risqué pour non-respect de la vie privée.

A notre époque de haute technologie, personne n'est protégée contre le piratage de données. Non seulement les cartes bancaires portent en elles le risque d'être usurpées, mais aussi les comptes bancaires peuvent être piratés par les hackers. Même les grandes institutions avec leur *cloud computing* sont impuissantes face à ces problématiques.

Un exemple de fuite de données massives est celui de « Capital One », une attaque informatique qui s'est conclue par un vol de données de plus de 100 millions de clients américains et canadiens [161]. Après cette fuite, la question se pose sur la fiabilité du *cloud computing*. Ces données ont été reportées sur des serveurs à distance qui était « plus protégés » contre les attaques. Cette pratique n'est pas courante en France, mais quelques banques pensent à transférer leurs données vers un cloud privé, c'est à dire dans leurs propres centres de données.

Chapitre 12

Protocole de sécurité de transfert des données

Ce chapitre présente le protocole de sécurité de transfert des données, les types de chiffrement, les serveurs mandataires et le réseau privé virtuel, ou **VPN** (pour Virtual Private Network), et la solution technique permettant de chiffrer l'intégralité des activités réseau de l'usager.

12.1 Protocole de sécurité de transfert des données

Le protocole SSL (*Secure Socket Layer*), remplacé par le protocole TLS (*Transport Layer Security*) est considéré comme le standard de chiffrement des communications HTTP. Il sécurise la communication des usagers en rendant la communication incompréhensible aux attaquants. Il consiste en un chiffrement symétrique de tous les messages échangés entre le terminal de l'usager et le serveur distant. L'utilisation de ce protocole permet l'authentification du serveur, la confidentialité des données échangées et leur intégrité (comme par exemple en France pour la déclaration des revenus en ligne). Il est important de comprendre ce qui est sécurisé. La communication entre client et serveur est bien chiffrée, mais le serveur aura accès aux informations en clair. D'autre part, les adresses IP ne sont nullement masquées et un attaquant à l'écoute peut déterminer qu'il y a eu un échange important entre le client et le serveur.

Cet outil de protection de la vie privée peut être considéré comme passif. L'utilisateur peut parfois choisir d'accéder à certains services en utilisant TLS ou SSL, mais il faut que cette option lui soit proposée. La technologie fournit une certaine protection à l'utilisateur sans qu'il ait besoin de rien faire. Cela devrait être une habitude pour l'utilisateur de vérifier que le site qu'il visite est bien celui qu'il pense. C'est le meilleur moyen pour éviter un site de phishing.

Les serveurs mandataires, ou proxies, sont des serveurs agissant comme des intermédiaires entre l'utilisateur et le service auquel il souhaite accéder (un site web, par exemple). L'utilisateur envoie sa requête au proxy, qui la transmet au service. Les données (adresses IP) sont modifiées par le proxy pour faire disparaître l'adresse de l'utilisateur et la remplacer par celle du proxy. Donc, le fournisseur de service a l'impression d'avoir affaire au proxy et non à l'utilisateur.

Cependant, seules certaines informations sont modifiées par le proxy, et le contenu du message peut contenir des informations identifiants. Les proxies ont le pouvoir d'anonymiser les informations qui lui sont spécifiques. D'autre part, il faut rester conscient du fait que les administrateurs du proxy sont en mesure d'accéder à l'intégralité des messages. Il faut donc, pour utiliser un proxy, avoir confiance dans ses administrateurs.

Un réseau privé virtuel, ou **VPN** (pour Virtual Private Network), est une solution technique permettant de chiffrer l'intégralité des activités réseau de l'usager. Le VPN est un service auquel l'utilisateur doit souscrire. Il peut être fourni par son employeur. L'utilisateur devra lancer un logiciel sur son poste (un client VPN), s'authentifier auprès d'un serveur VPN, et le logiciel fera passer toutes ses connexions futures, de manière chiffrée, via le serveur VPN. Ainsi, un observateur local aura l'impression que l'utilisateur ne communique

qu'avec le serveur VPN (et non avec des sites web par exemple). De plus, les connexions avec le serveur sont chiffrées.

Toutefois, le fournisseur de service VPN pourra toujours identifier le service distant, et pourra lire le contenu des messages. Le VPN est une technologie efficace. Souscrire à un accès VPN avant un déplacement dans un pays où on peut surveiller Internet est une stratégie pour protéger des activités susceptibles d'être censurées.

TOR (The Onion Router) est un réseau interconnecté, comprenant des nœuds d'entrée et des nœuds de sortie. Les techniques de chiffrement sont faites par couches. D'une part, l'adresse de l'utilisateur est masquée à tous, sauf au nœud d'entrée. Le destinataire ne peut pas l'identifier, même s'il peut renvoyer une réponse. Pour utiliser Tor, l'usager doit installer un logiciel de proxy spécial sur sa machine et configurer ses logiciels. Ce réseau peut être bloqué dans les pays, comme la Chine.

La technologie Open ID propose un moyen d'éviter à l'utilisateur de créer des comptes sur les sites web qu'il visite. L'utilisateur ouvre un compte uniquement chez un fournisseur OpenID. Cette technologie est utilisée par les comptes Google, Yahoo ou Windows.

12.2 Chiffrement de données sur disque

Un des sujets importants de la protection de la vie privée est la capacité à chiffrer les documents sensibles stockés sur un poste de travail. Un mot de passe est un moyen de protéger mais insuffisant. Si l'on fait démarrer un autre système d'exploitation avec un accès au disque considéré, il pourrait accéder aux données sans aucune restriction. C'est ainsi que sur un ordinateur en double boot Windows/Linux, Linux peut accéder à votre système de fichier (NTFS). Pour mieux protéger les informations, il faut chiffrer les données. Les systèmes d'exploitation proposent les méthodes de chiffrement du système de fichiers suivants : EFS (Encrypted File System) sous Windows, FileVault sous Mac OS X, des paquetages du type cryptés ou dm-crypté sous Linux. Dans tous les cas, c'est un chiffrement symétrique.

Pour une sécurisation supplémentaire, les messages envoyés peuvent être chiffrés au point que seuls les destinataires pourront les lire. C'est le cas de méthodes de chiffrement asymétrique. En effet, un X veut que seul un Y lise son message, il devra le chiffrer avec la clé publique de ce dernier, pour qu'il puisse la déchiffrer avec sa clé privée. S'il veut signer son message, il ajoutera à son envoi un résumé cryptographique du message (le condensat) qu'il aura chiffré avec sa clé privée. Différents scénarios de divulgation sont envisageables :

- Divulgation d'identité (identity disclosure) : un individu statistique (entreprise ou personne) peut être retrouvé dans un fichier. Par ex. pour identifier l'entreprise d'un secteur avec son chiffre d'affaires.
- Divulgation d'attributs (attribut disclosure) : l'information sensible sur un individu est révélée suite à la publication d'un fichier. Il est possible qu'il y ait divulgation d'attributs sans qu'il y ait divulgation d'identité.
- Divulgation inférentielle (inferential disclosure) : grâce à la publication d'un fichier de données, on peut prédire les caractéristiques d'un individu avec plus de précision que cela aurait été possible autrement [98]. On distingue généralement trois types de variables dans un fichier de données :

- Les variables directement identifiants (par exemple Nir pour un individu, Siren pour une entreprise) ;
- Les quasi-identifiants dont la combinaison peut permettre la ré-identification (âge, lieu de naissance ; pour les organismes, la localisation géographique, le domaine d'activité) .

- Les autres variables non identifiants. En pratique, un utilisateur malveillant peut utiliser les quasi-identifiants pour ré-identifier un individu.

Pour estimer le risque, il convient de dresser la liste des variables quasi-identifiants. Cette étape est difficile à mener en pratique, car elle dépend des hypothèses faites sur l'information disponible. Dans les études méthodologiques effectuées en pratique concernant des données, l'approche générale consiste à comparer différents types de recodage possible. Certains algorithmes de recodage local ont également été développés, par exemple l'algorithme de Mondrian. Avec ce type d'algorithmes, le niveau de détail diffusé pour les variables quasi-identifiantes dépend de l'unité considérée et de son potentiel risque de ré-identification. La diffusion de données avec différents degrés de précision pour les variables quasi-identifiantes peut complexifier leur utilisation.

12.3 Anonymisation

Dans la technique d'anonymisation, on peut distinguer deux catégories : la première catégorie représente les données qui sont vraies mais qui peuvent manquer de détails, alors que les données de la deuxième catégorie sont inexactes, ce qui n'empêche pas leur usage à des fins de statistique par exemple.

La technique de recodage global (« global recoding ») s'applique à toutes les valeurs d'un attribut afin de diminuer le risque de ré-identification. Ainsi, on peut remplacer l'âge d'un individu par un intervalle.

La technique de généralisation consiste à remplacer des valeurs par des valeurs plus générales [172] : les données sont vraies, mais pas précises. La généralisation est appliquée à un ensemble d'attributs formant un quasi-identifiant (QI). Généraliser consiste à remplacer une valeur par son ancêtre direct dans la hiérarchie de généralisation, à chaque étape de la généralisation.

La micro-agrégation [173] répartit les données originales en groupes homogènes. Elle fonctionne en ajoutant chaque valeur de l'attribut à anonymiser par une variable aléatoire.

Chacune de ces techniques a donné lieu à plusieurs algorithmes. Ainsi, il existe une grande variété de techniques d'anonymisation et encore plus d'algorithmes qui les mettent en œuvre.

Les exigences d'anonymisation sont exprimées en terme de chaînage et de sûreté. Le chaînage permet d'associer un ou plusieurs identifiants anonymes à une même personne physique. Un chaînage peut être temporel (toujours, jamais) ; géographique local ou spatio-temporel (par exemple, "toujours et partout"). Des objectifs d'anonymisation :

- Réversibilité : cacher les données par un simple chiffrement des données. Dans ce cas, il y a possibilité de remonter depuis les données chiffrées jusqu'aux données nominatives originelles ;
- Irréversibilité : une fois remplacés par des identifiants anonymes, les identifiants nominatifs originels ne sont plus recouvrables, la technique utilisée est une fonction de hachage ;
- Insensibilité : c'est le cas où il est impossible en pratique de remonter aux données nominatives, sauf en appliquant une procédure exceptionnelle sous surveillance d'une instance ;

L'objet de l'anonymisation est de détecter ces données personnelles, de les éliminer afin d'empêcher toute personne extérieure d'identifier les acteurs, de les localiser ou d'entrer en contact avec eux. Ce brouillage est nécessaire lorsque l'on rend les données accessibles à des tiers [163].

« Ce brouillage » doit être opéré avec suffisamment de précision pour conserver certaines marques culturelles ou maintenir la cohérence du contenu. Les finalités de l'anonymisation de données devraient être définies, quand elles jouent un rôle dans l'identification. Les attributs quasi-identifiants devraient être supprimés de l'ensemble de données. Dans le cas des interactions médiées par ordinateur, l'anonymisation des identifiants des auteurs est souvent automatisée.

Le problème le plus délicat à traiter est celui de l'anonymisation à l'intérieur des messages. En effet, il est très fréquent que les acteurs de la formation utilisent des éléments qui permettent de les identifier facilement. Par exemple des noms, prénoms, sites web personnels, adresses postales, lieux de résidence, institutions de rattachement, espaces fréquentés, etc. Le choix des éléments à repérer est une étape préliminaire. Par exemple « Bonjour, je m'appelle Patricia. J'ai 23 ans, je suis une étudiante à la Sorbonne Paris 1, pas très loin de Panthéon. » Dans ce cas précis, il faut masquer au moins le nom de l'institution et le nom de la ville.

Certaines analyses peuvent nécessiter des informations telles que le prénom, la localisation, ou la nationalité, à ce titre, les informations doivent être conservées sous une forme intelligible pour le chercheur [162]. Pour l'anonymisation de corpus d'interactions potentiellement multilingues, il est convenable de construire un outil adapté à ce type de données textuelles répondant aux exigences de l'analyse.

L'utilisateur peut manuellement décider des données qu'il veut partager avec le serveur, en cochant des cases ou utiliser le paramétrage des données selon trois niveaux de confidentialité :

- Low
- Medium
- High

Un tel système de paramétrage ressemble à la gestion des cookies où l'utilisateur peut définir ses préférences.

Les marques d'identification laissées par les acteurs peuvent prendre des formes très variées. Par ex. le traitement des dossiers médicaux : il s'agit d'anonymiser des retranscriptions d'entretiens avec les patients. Les données de santé pouvant être particulièrement sensibles, ces données personnelles sont à masquer impérativement avant toute diffusion [182].

Pendant la validation de la technique d'anonymisation, il faut tenir compte du facteur de risque et évaluer la gravité et la probabilité de ce risque. Les données à caractère personnel doivent être collectées et traitées dans le respect de la législation applicable en matière de conservation des données sous une forme identifiable.

Le processus d'anonymisation doit satisfaire au critère de compatibilité conformément aux lignes directrices proposées par le groupe de travail «Article 29» [66]. Quand des tiers traitent un ensemble de données auquel une technique d'anonymisation a été appliquée, ils ne sont pas tenus d'observer les exigences de protection des données. Les tiers doivent prendre en compte les facteurs contextuels et circonstanciels pour décider comment ils comptent combiner ces données anonymisées pour leur propre usage.

Les données pseudonymisées ne peuvent être assimilées à des informations anonymisées puisqu'elles continuent à permettre l'individualisation d'une personne concernée et la corrélation entre différents ensembles de données. Le pseudonymat n'est pas de nature à empêcher qu'une personne concernée soit identifiable et reste donc dans le champ d'application du régime juridique de la protection des données. Cela vaut en particulier dans le contexte des recherches scientifiques, statistiques ou historiques [113 : 19-21].

La pseudonymisation n'est pas reconnue comme un moyen d'anonymisation. Elle ne peut pas donner un niveau de protection élevé. Par la combinaison des éléments, on peut retrouver l'individu. Par ex., croiser deux bases de données, une base de données médicale pseudonymisée et une liste électorale avec des données nominatives. Le résultat de la pseudonymisation peut être indépendant de la valeur initiale ou il peut être dérivé des valeurs originales d'un attribut, par exemple de hachage ou d'un système de chiffrement.

Hachage par clé enregistrée. On utilise une clé secrète comme entrée supplémentaire. Un responsable du traitement peut ré-exécuter la fonction sur l'attribut en se servant de la clé secrète. Dans ce cas, on sélectionne un nombre aléatoire comme pseudonyme pour chaque attribut de la base de données et supprime la table de correspondance. Cette solution permet de réduire le risque de corrélation entre les

données à caractère personnel figurant dans l'ensemble de données et celles qui se rapportent au même individu dans un autre registre de données.

Tokenization. Cette technique est appliquée dans le secteur financier pour remplacer les numéros d'identification de cartes. On utilise des fonction d'index, ou d'un nombre produit de manière aléatoire.

Parfois les responsables du traitement des données supposent qu'il suffit de supprimer ou de remplacer un ou plusieurs attributs pour rendre l'ensemble des données anonyme. Le simple fait de modifier l'identité n'empêche pas quelqu'un d'identifier une personne concernée s'il subsiste des quasi-identifiants dans l'ensemble de données. Il est important d'éviter d'utiliser la même clé dans des bases de données différentes pour pouvoir réduire la corrélation. Si la clé secrète est conservée avec les données pseudonymisées, l'attaquant peut relier les données pseudonymisées avec leur attribut.

Les chercheurs du Massachusetts Institute of Technology ont analysé un ensemble de données pseudonymisé couvrant des coordonnées mobiles spatiales de 1,5 million de personnes sur un territoire d'un rayon de 100 km. Ils ont démontré que quatre points de localisation permettaient d'isoler 95 % de cette population, ce qui montre le danger pour la protection des données personnelles [149].

12.4 Conclusion

L'innovation est inévitable dans notre vie numérique et il faut bien trouver un équilibre entre les risques et les avantages et tirer profit des résultats. Quand on parle de l'automatisation des tâches, il est indispensable d'étudier les facteurs importants pendant l'utilisation de l'intelligence artificielle. Un manque de recherches scientifiques a provoqué des attentes irréelles. Mais il faut souligner que dans certains secteurs (tels la banque, la santé), l'avancement de la numérisation a déjà apporté des résultats tangibles. Une grande partie des clients se disent satisfaits de ces innovations. Le côté négatif est la perte d'emplois et le risque élevé d'usage non convenables des données.

Chapitre 13

Automatisation des documents : atouts et inconvénients

Ce chapitre présente les atouts et inconvénients de l'automatisation des documents sur les exemples des cas du registre public de la Géorgie. Par des manipulations sur les sites internet, des inconnus parviennent à obtenir des informations sensibles sur autrui. L'information n'est pas anonymisée et en passant par la caisse du commerce (magasin, pharmacie...), une carte de fidélité ou un numéro personnel est habituellement demandé pour, par ex. cumuler des bonus.

13.1 Exemple de la Géorgie : le cas du registre public

En Géorgie, il existe un site qui rassemble les informations à partir des documents officiels d'achat/vente de biens, d'enregistrement de business, d'organisations, d'adresses. Ce site a été créé en 2004, après l'adoption d'un règlement sur les biens. Le site dans sa globalité est un pas en avant dans notre vie numérique, mais nous supposons que, en termes de respect des données à caractère personnel, il reste encore des éléments à renforcer.

Ce site est le Registre Public, et d'après l'étymologie du mot, l'information doit y être publique, mais nous supposons que les personnes intéressées peuvent obtenir les informations sensibles sur les autres [150].

Par exemple, si je cherche des informations sur la personne X/ Nino, je tape son nom et son prénom, et le système me propose des dizaines de X/ Nino :

Fig. 35 : *Page d'accueil du Registre public de Géorgie. Source : Registre public de Géorgie*

Pour rechercher cette information, il nous est proposé différents moyens :

- Numéro de demande
- Période d'enregistrement de demande
- Nom, prénom ou NP de la personne recherchée
- Le nom de l'organisation
- Adresse du bien
- Code de plan de cadastre

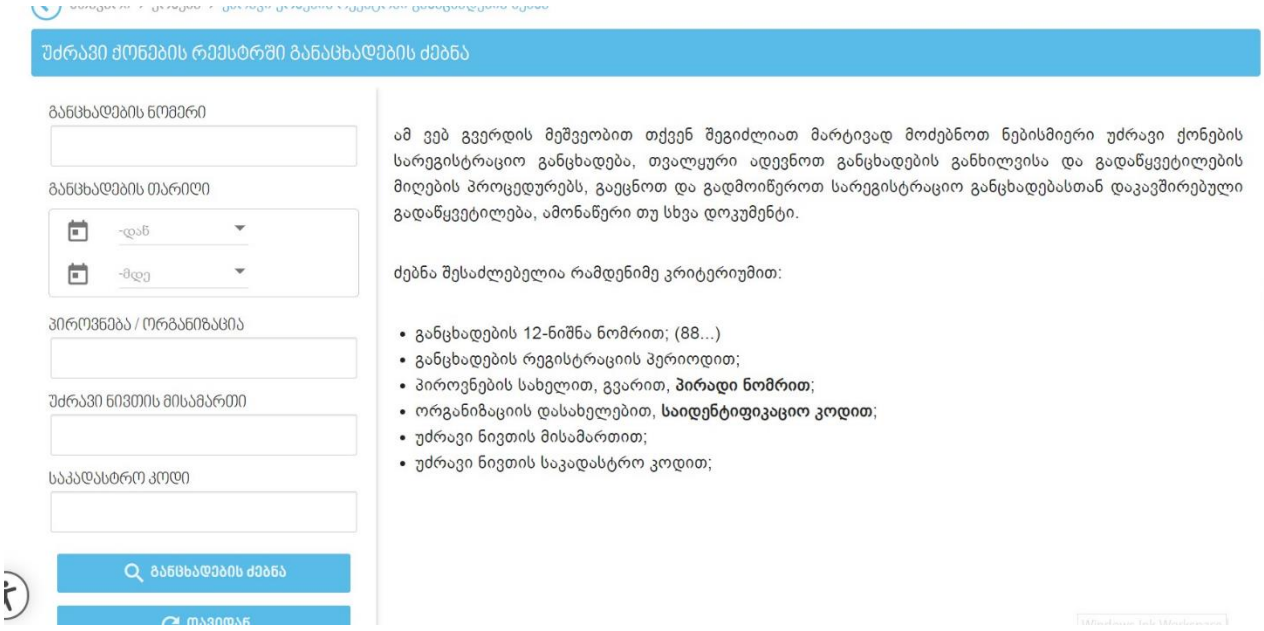


Fig. 36 : *Registre public,. Fichier pour les recherches des informations sur les biens.*

En cherchant des informations sur Nino/X en octobre 2020, nous trouvons 155 ordonnances :

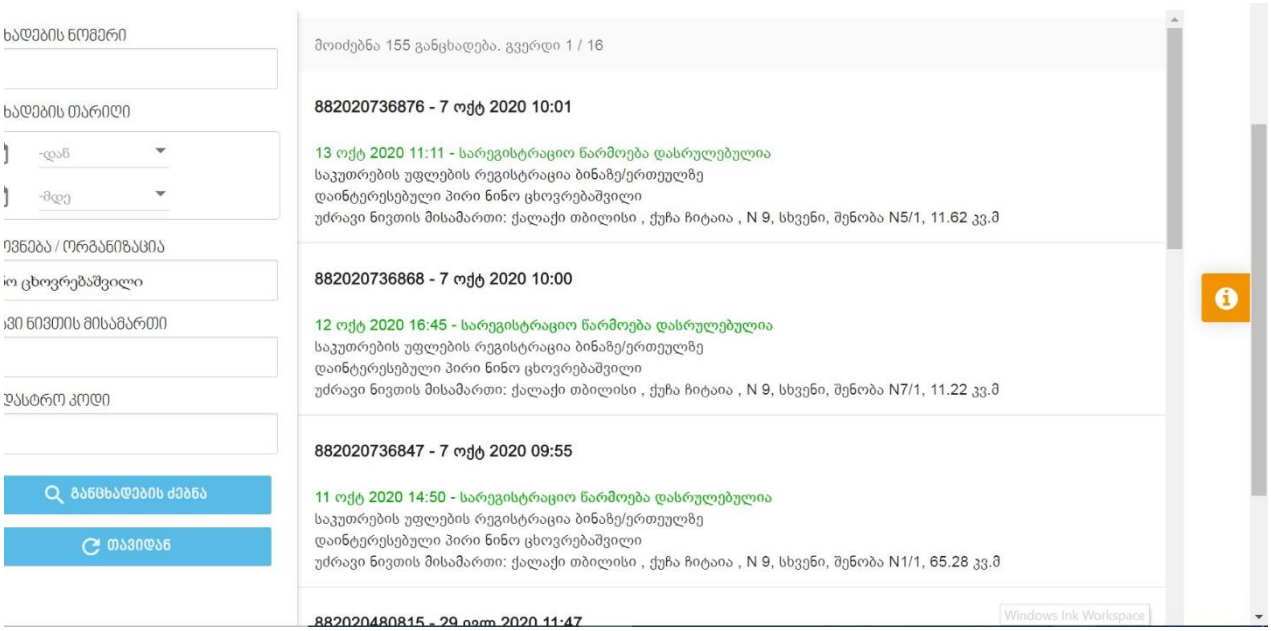


Fig. 37 : *Exemple de recherches d'informations sur le bien de la personne concernée. Source : Registre public*

Dans cette ordonnance, tout est détaillé. Qui a demandé de préparer cette ordonnance, quand, prix du service, date de préparation des demandes. Par exemple, nous avons dans cet exemple une demande datant de 2012 :

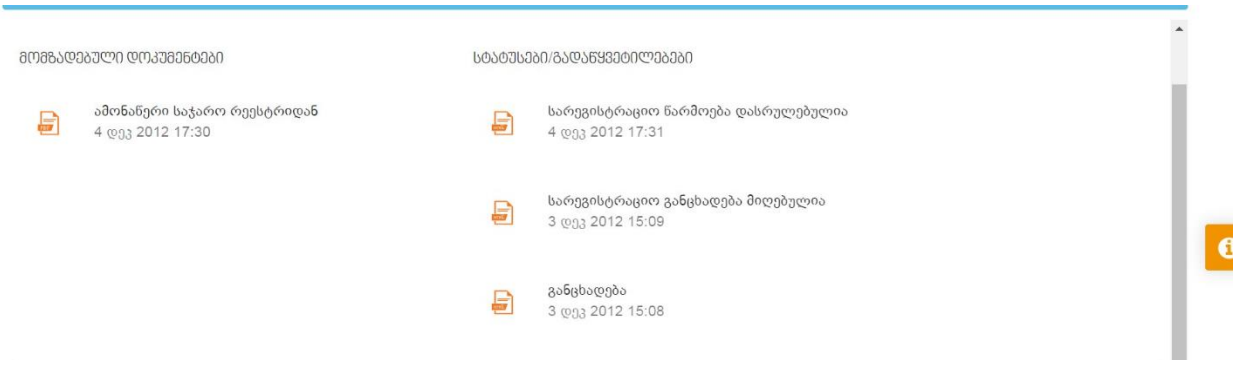


Fig. 38 : *Annonces en format PDf sur le bien de la personne concernée. Source : Registre public*

Le plus sensible selon moi dans ce système est de voir que les numéros personnels comme les NIR sont rendus publics :

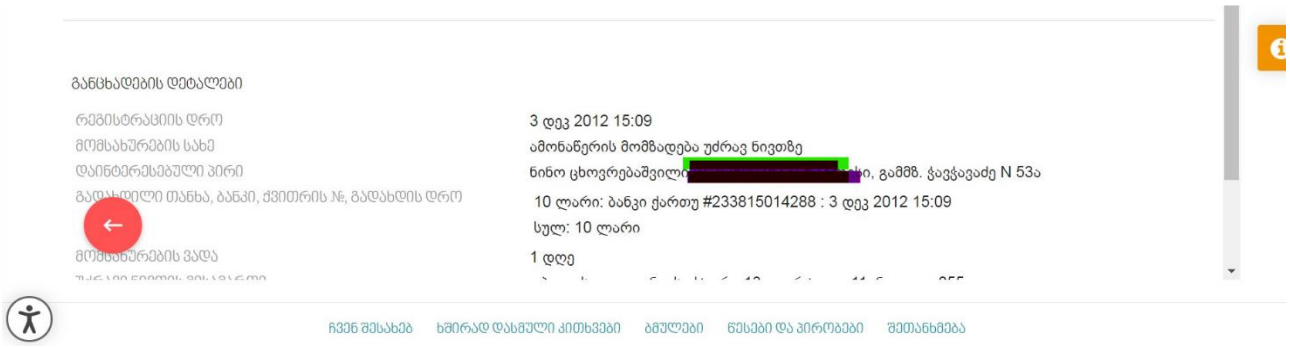


Fig. 39 : *Résultat de recherche sur les démarches d'enregistrement du bien par la personne concernée, Source Registre public.*

En trouvant le numéro personnel de la personne recherchée, les internautes qui le souhaitent peuvent aussi trouver son adresse via le site des élections, sur lequel nous pouvons aussi trouver les photos d'identité de la personne.

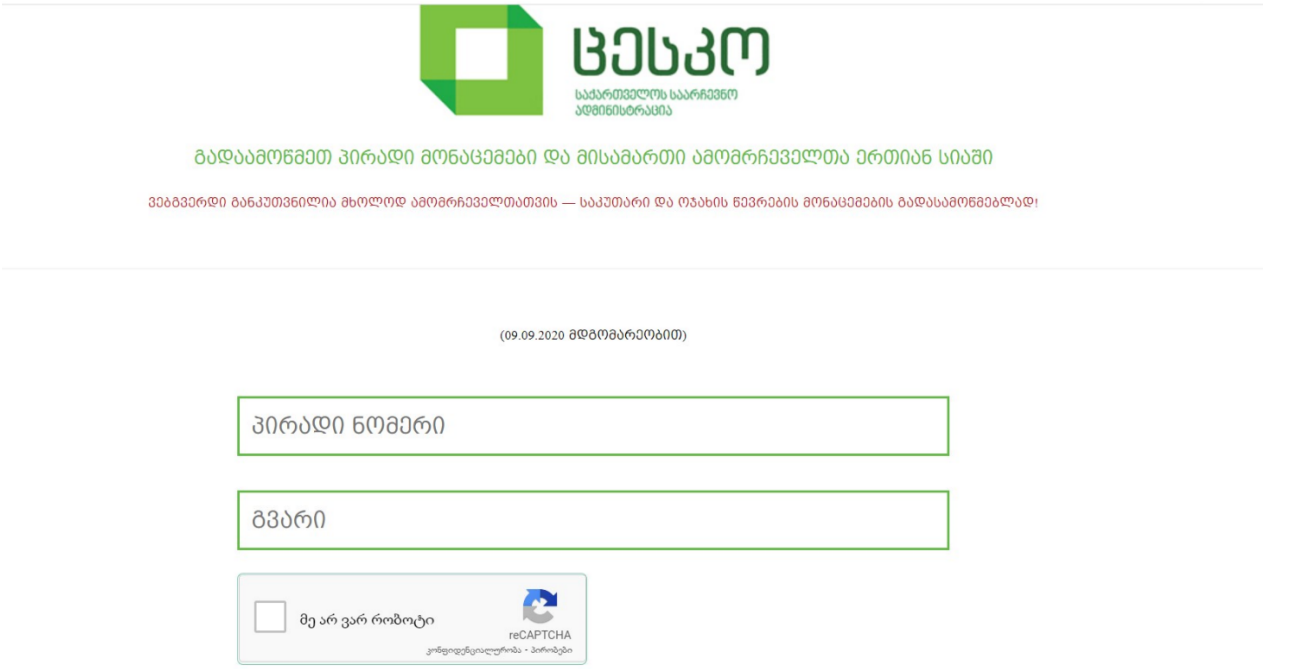


Fig. 40 : *Site Web de la Commission électorale centrale, Source : commission électorale centrale*

Voici ci-dessus la capture d'écran du site de l'administration des élections. Pour l'identification, il nous est demandé le numéro d'identification de la personne (NINO) et son nom. Comme nous l'avons déjà souligné, il n'est pas difficile de trouver le numéro personnel sur le site du registre public de la personne souhaitée.

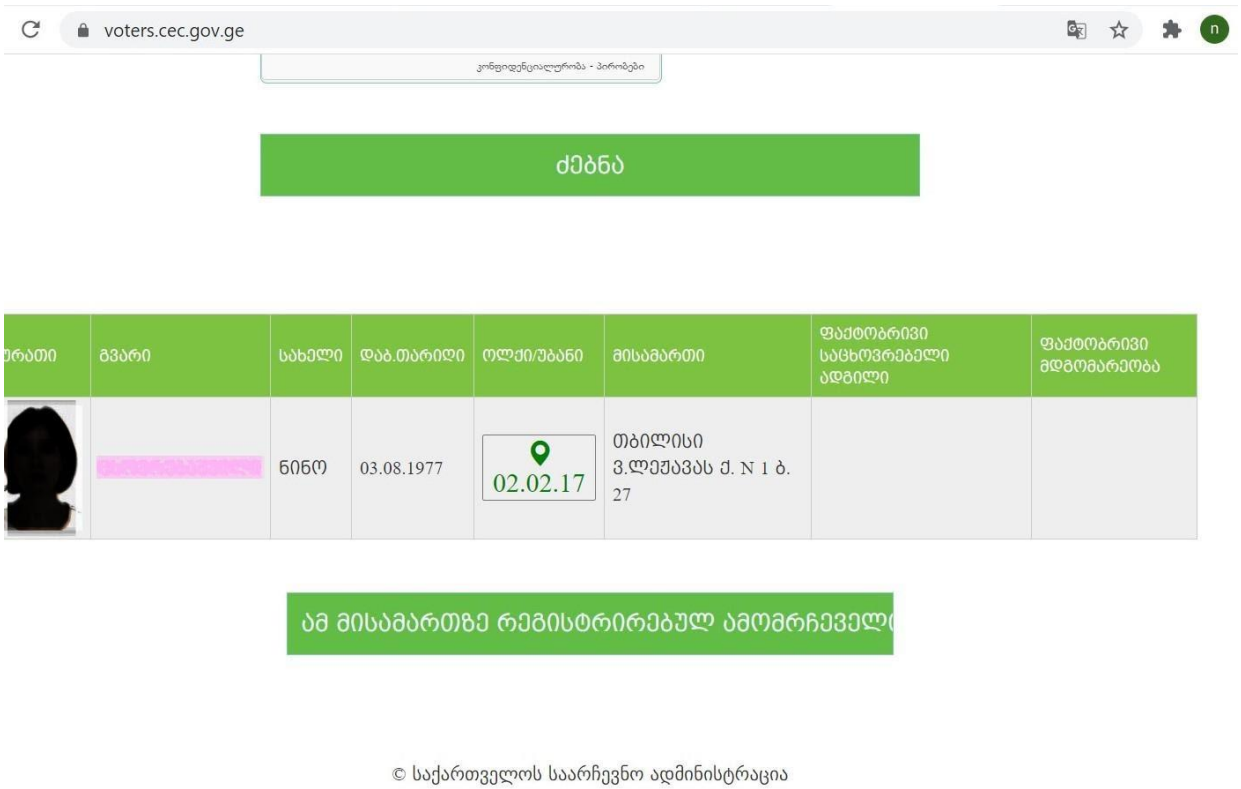
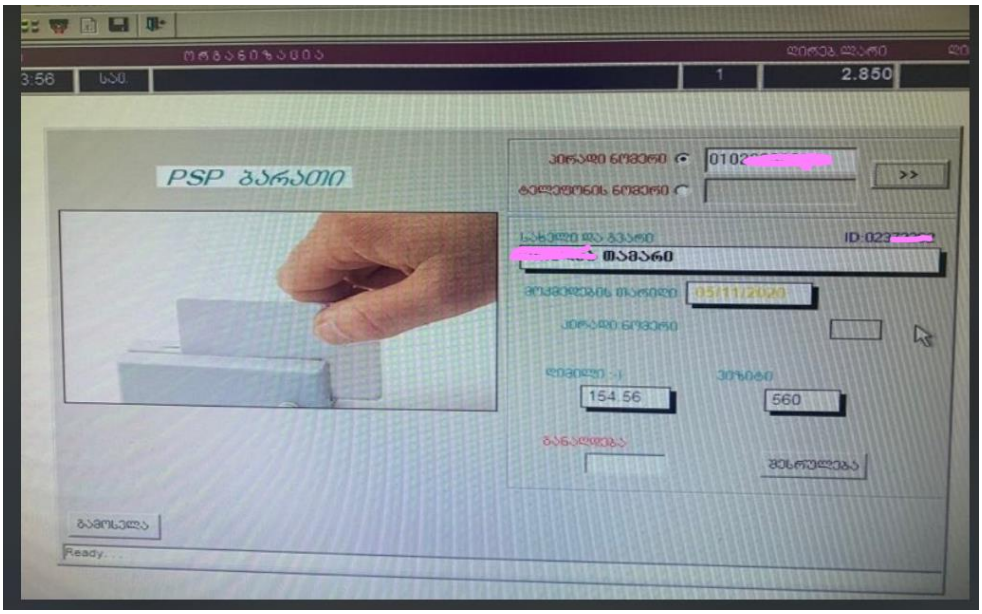


Fig. 41 : *Résultat de recherche de la personne concernée, Source : commission électorale centrale*

Nous estimons que la situation s'aggrave quand tout commerce (quelle que soit leur taille) demande le numéro personnel pour l'activation de bonus système. Plus grave, chaque vendeur de caisse a accès à ces informations. L'information n'est pas anonymisée et en passant par la caisse, une carte de fidélité ou un numéro personnel est demandé. En tapant le NP, la caissière « prononce » le prénom du client (pour vérifier l'identité du client). Il apparaît ainsi évident que les informations sensibles sont rendues publiques dans le programme des commerces et des pharmacies. Ces informations sont délivrées par les clients eux-mêmes en faveur de bonus système.



13.2 Risques de l'utilisation des données sensibles comme « Nir » dans les documents automatisés

Le numéro d'inscription des personnes (NIR) au répertoire national d'identification des personnes physiques (RNIPP), appelé numéro de sécurité sociale, est créé à partir de l'état civil et est géré par l'INSEE. Il est attribué à chaque personne à sa naissance sur la base d'éléments d'état civil transmis par les mairies à l'INSEE.

La CNIL recommande que l'emploi du NIR comme identifiant des personnes dans les fichiers soit justifié et en aucun cas systématique. Ce numéro à 13 chiffres permet de déterminer le sexe, le mois et l'année de naissance, ainsi que le département de naissance en France. Ou il indique que la personne est née à l'étranger.

L'enregistrement du numéro de sécurité sociale dans un traitement est autorisé :

- dans les fichiers de paie et différentes déclarations sociales obligatoires [84]
- dans la prise en charge des frais de maladie [125]

Le numéro de sécurité sociale ne peut pas être utilisé comme numéro de matricule de l'employé.

Pour l'identifier ans tous les fichiers de gestion, **au niveau de transferts de ces données vers un organisme dans un pays n'appartenant pas à l'Union européenne, il faut absolument demander l'autorisation à la CNIL.**

Le transfert est autorisé :

- Vers un pays reconnu comme "adéquat" par la Commission européenne
- Vers des entreprises si des Clauses contractuelles types sont approuvées par la Commission européenne, et signées entre deux entreprises
- Vers les entreprises ou (BCR) si elles sont adoptées au sein d'un groupe
- Vers les États-Unis, si l'entreprise destinataire a adhéré au Privacy

Des exceptions peuvent être faites pour :

- Sauvegarde de la vie de cette personne ;
- Sauvegarde de l'intérêt public ;
- Obligations d'assurer la défense d'un droit en justice ;
- A la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers.

En cas d'exercice du droit d'accès ou de rectification, les données relatives aux pièces d'identité peuvent être conservées pendant le délai prévu à l'article 9 du code de procédure pénale, soit un an. En cas d'exercice du droit d'opposition, ces données peuvent être archivées pendant le délai de prescription prévu à l'article 8 du code de procédure pénale, soit trois ans [34].

En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes. » [26 ; 4]. Après la loi de 2004, les données relatives à la santé figurent au rang des données sensibles.

Selon La CNIL, il est strictement interdit, sauf accord exprès de l'intéressé, de mettre ou conserver en mémoire informatisée des données nominatives qui, directement ou indirectement, renseignent sur ces données sensibles.

La nationalité peut être considérée comme une donnée sensible. L'information relative à la nationalité d'une personne est de nature à faire apparaître son origine, ce qui a conduit à la considérer, dans certaines hypothèses, comme une donnée sensible [140].

13. 3 Recherches menées auprès d'universités française et géorgienne

Nous avons organisé une étude auprès d'universités française et géorgienne dans les années 2018- 2021. L'objet de ces recherches était découvrir le niveau de protection et des attitudes envers les données personnelles dans les universités. Dans le Focus groupe se trouvaient des étudiants et professeurs de l'institution. Tranche d'âge : 20- 68 ans. Ces études étaient quantitatives et les méthodes déductives.

Questions :

- LA protection des données est-elle importante pour vous ?
- Délivrez-vous vos données facilement ?
- Avez-vous l'expérience de demander au responsable du traitement de ne plus traiter vos données ?
- Avez-vous modifié vos attitudes envers les réseaux sociaux après la sanction de Facebook de 5 milliards d'euros ?
- Connaissez-vous les institutions responsables en matière de protection des données à caractère personnel ?
- Etes-vous usagers des réseaux sociaux ?
- Comment appréciez-vous le rôle de CNIL dans la défense de vos droits ?
- Vous adressez-vous aux organisations compétentes pour la défense de vos droits en cas d'abus ?
- Les enfants sont-ils bien protégés dans notre ère numérique ?
- Connaissez-vous le RGPD ?

- Quel est pour vous le droit à l'oubli ?
  - Une défense renforcée où
  - Rien de particulier

- Avez-vous entendu parler de cyber attaques en Géorgie en 2019 ?

- Comment qualifierez-vous niveau de cyber sécurité en France/ Géorgie ?

- Avant le scandale de Snowden, pensez-vous que les dirigeants étaient mieux protégés ?

- Jugez-vous légitime dans certains cas particuliers de divulguer les images de la vie privée ?

- Novac a échoué en tant qu'expert-comptable stagiaire irlandais, à un examen de comptabilité. A la suite de cet échec, il a introduit une réclamation visant à contester le résultat de cet examen. Sa réclamation ayant été rejetée, il a présenté une demande d'accès visant l'ensemble des données à caractère personnel le concernant détenu par l'ordre irlandais des experts comptables. Ce dernier lui a communiqué des documents mais a refusé de lui transmettre sa copie d'examen au motif que celle-ci ne contenait pas de données à caractère personnel. La copie d'examen contenait-elle pour vous des données à caractère personnel ?
- L'arrêté du 23 novembre de 2018 portant création de traitement automatisées des données à caractère personnel dénommé "Système d'information sur l'orientation dans le supérieur" (ORISUP). Qu'est-ce que c'est pour vous ?
  - Un traitement à des fins statistiques
  - Un danger pour la protection des données ?
    - Intelligence artificielle et RGDP peuvent-ils cohabiter ?

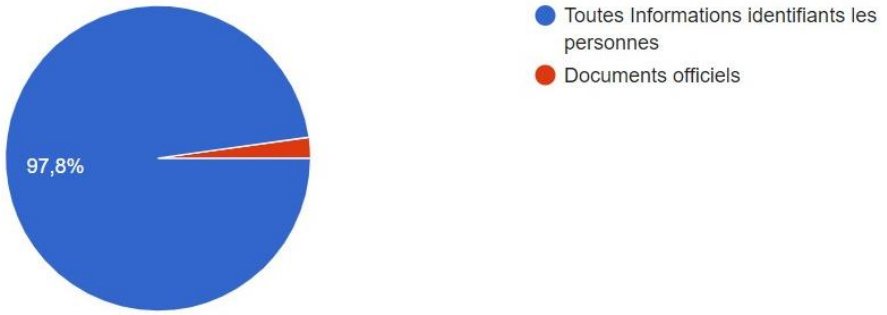
    - Avez-vous déjà suivi des cours sur la protection des données ?

13.4 Résultats des études

Ci-après, nous avons publié les captures d'écran des résultats de cette étude menée en France et en Géorgie : les graphiques permettent d'apprécier les réponses d'un coup d'oeil.

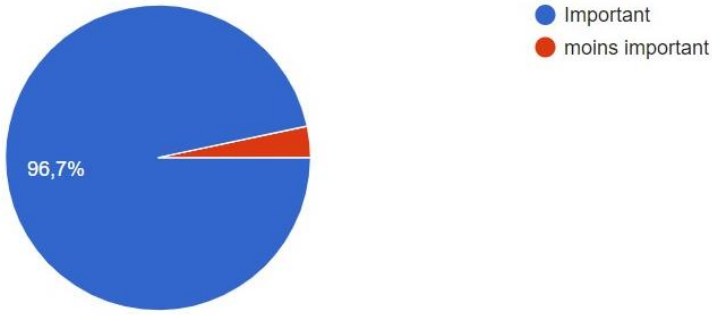
Qu' est ce que c'est pour vous les données à caractère personnel ?

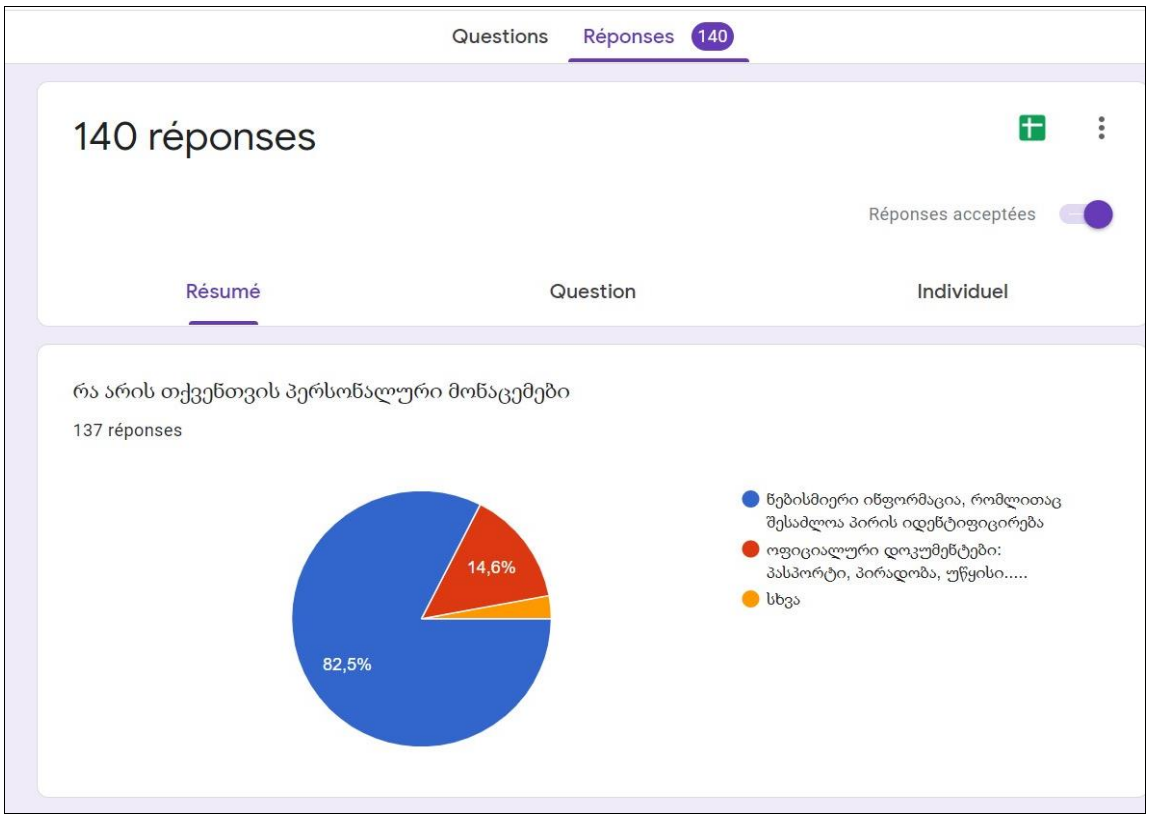
90 réponses

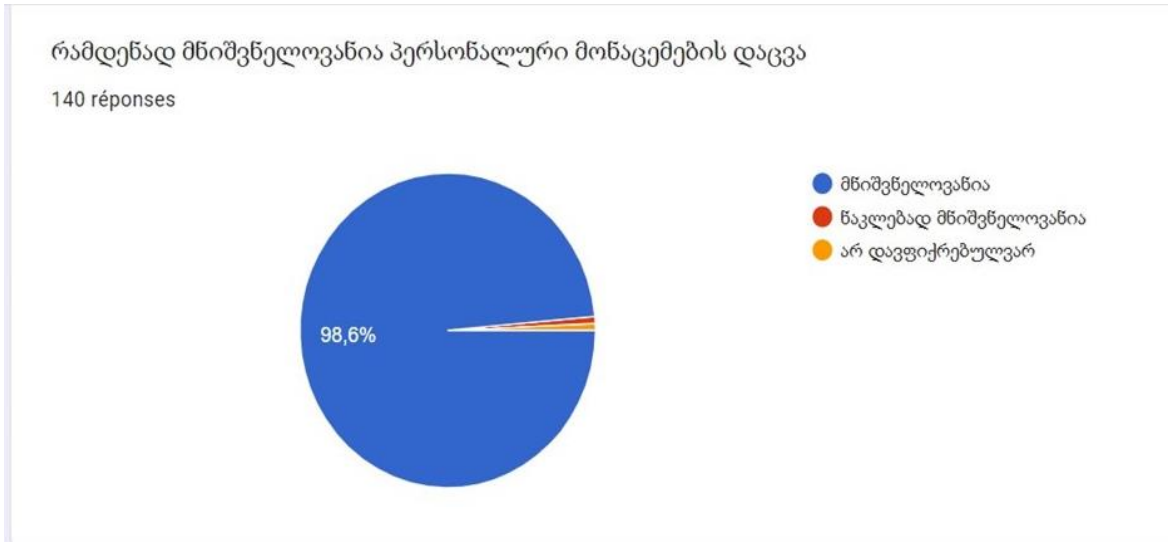


Protection des données est elle importante pour vous ?

90 réponses

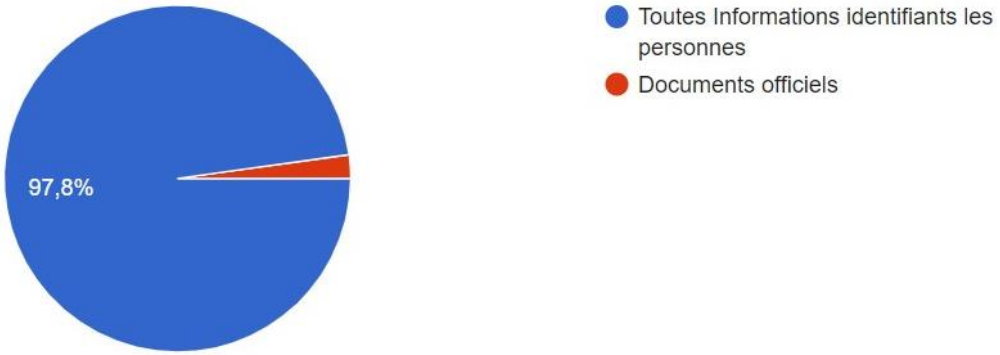



Questions
Réponses 140
140 réponses
Réponses acceptées
Résumé
Question
Individuel
რა არის თქვენთვის პერსონალური მონაცემები
137 réponses
14,6%
82,5%
წებისმიერი იწფორმაცია, რომლითაც შესაძლოა პირის იდენტიფიცირება
ოფიციალური დოკუმენტები: პასპორტი, პირადობა, უწყისი.....
სხვა


რამდენად მნიშვნელოვანია პერსონალური მონაცემების დაცვა
140 réponses
98,6%
მნიშვნელოვანია
წაკლებად მნიშვნელოვანია
არ დავფიქრებულვარ

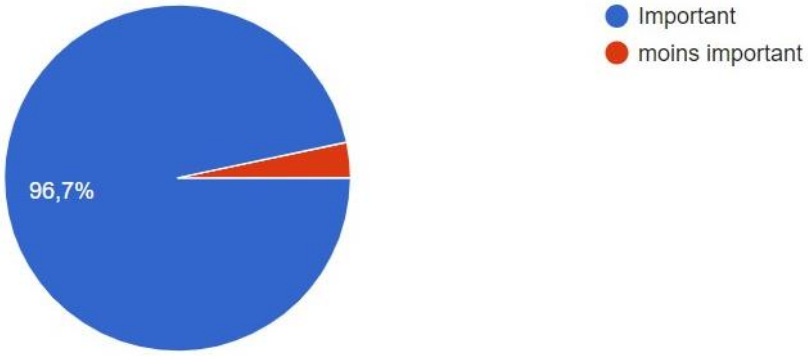
Qu' est ce que c'est pour vous les données à caractère personnel ?

90 réponses



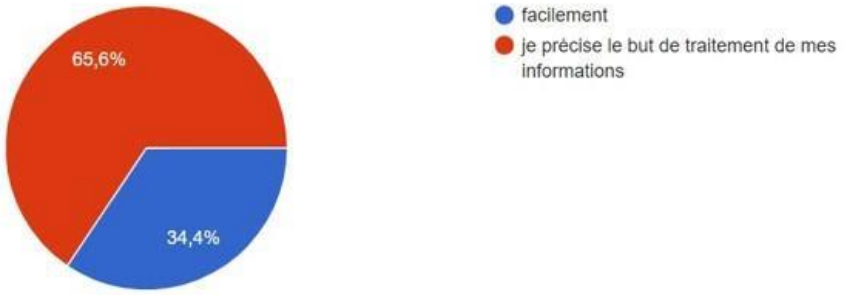
Protection des données est elle importante pour vous ?

90 réponses



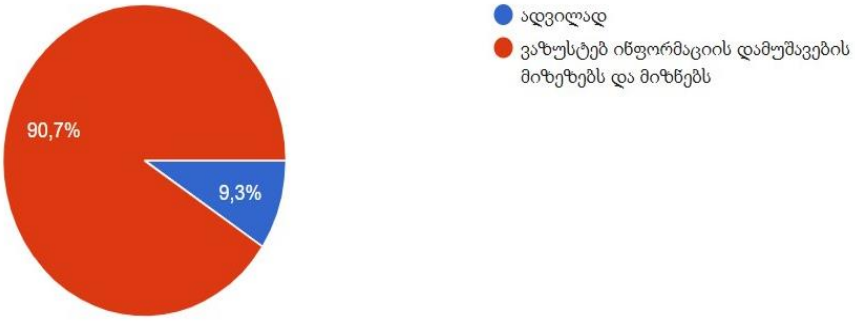
Délivrez vous vos données facilement ?

90 réponses



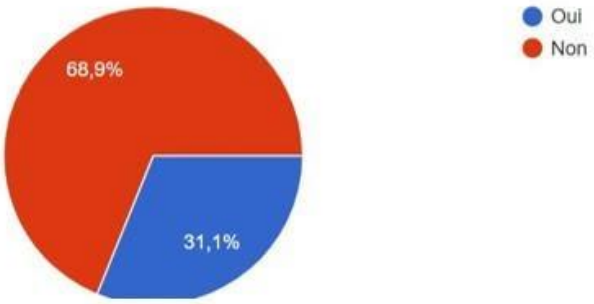
რამდენად ადვილად გასცემთ თქვენს მონაცემებს

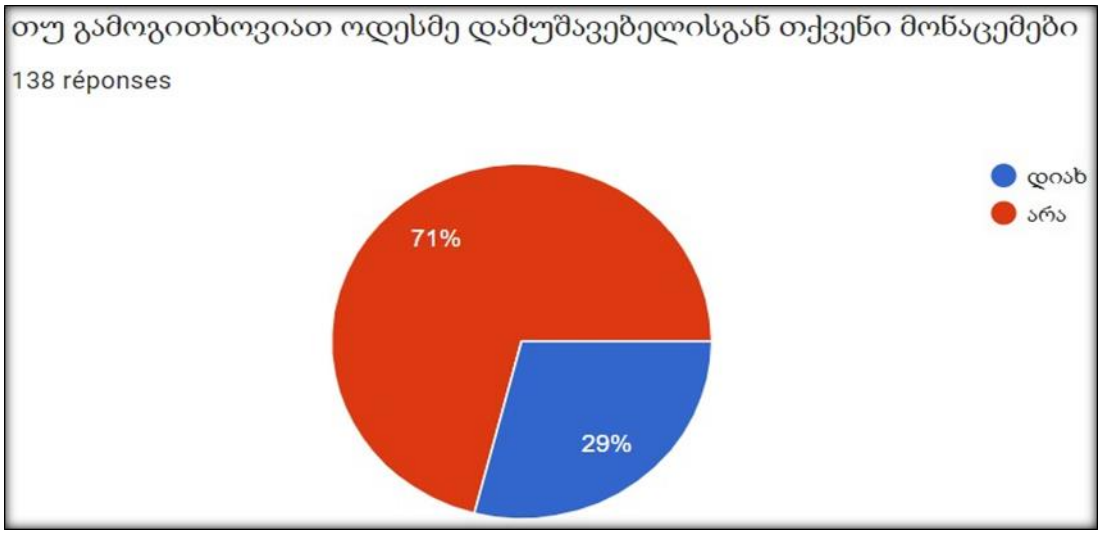
140 réponses



avez vous l'expérience de demander aux responsables de traitement des données de ne plus traiter vos données?

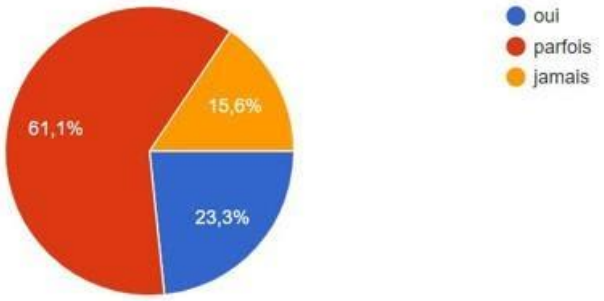
90 réponses





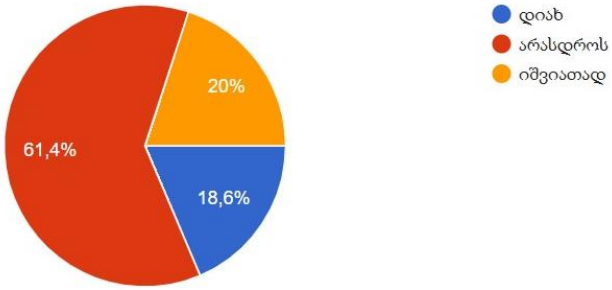
avez vous jamais regretté d'avoir délivré vos informations?

90 réponses



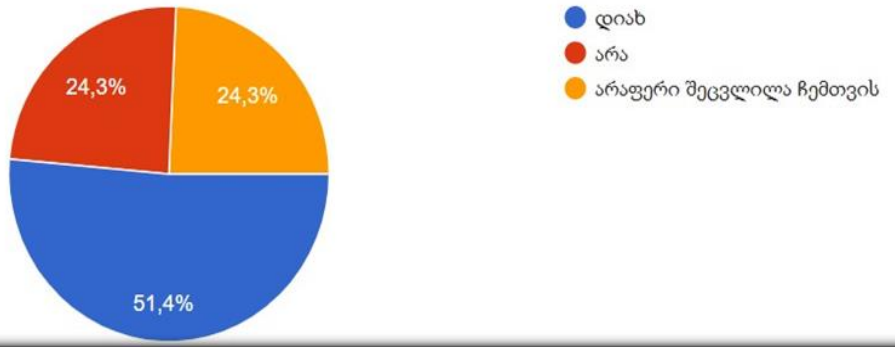
თუ გქონიათ შემთხვევა, როცა პირადი ინფორმაციის გამოაშკარავების შემდეგ გინანიათ, რომ ეს ინფორმაცია საჯარო გახადეთ

140 réponses



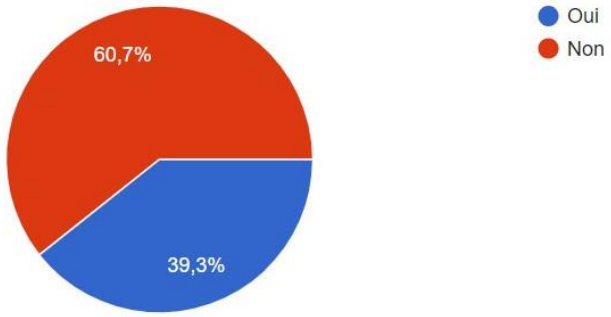
თუ შეგეცვალათ დამოკიდებულება სოციალური ქსელების მიმართ მას შემდეგ, რაც მომხმარებელთა მონაცემების არასათანადო შენახვის გამო ფეისბუქი რეკორდული თანხით, 5 მილიარდი დოლარით, დაჯარიმდა,https://www.france24.com/fr/20190724-facebook-accepte-amende-milliards-dollars-ftc-record-critiques

140 réponses



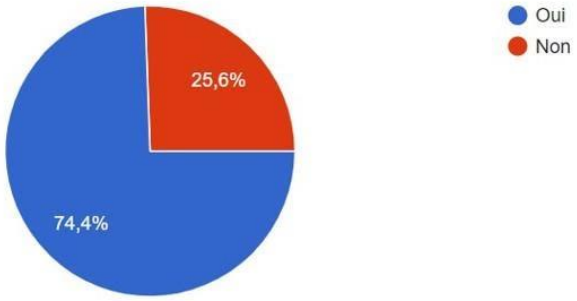
Avez vous modifié votre attitude envers les réseaux sociaux après la sanction de Facebook de 5 milliard d' euros https://www.france24.com/fr/20190724-facebook-accepte-amende-milliards-dollars-ftc-record-critiques

89 réponses



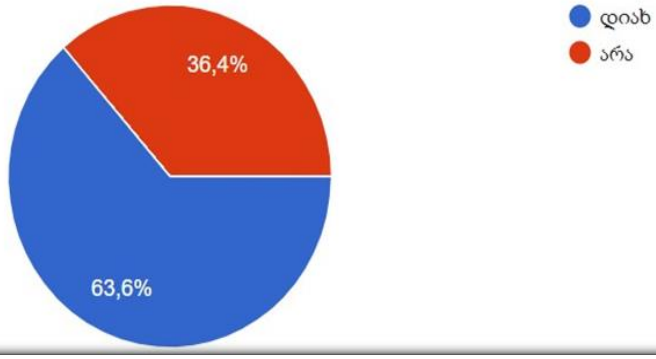
Connaissez vous l' institution responsable en matière de protection des données à caractère personnel?

90 réponses



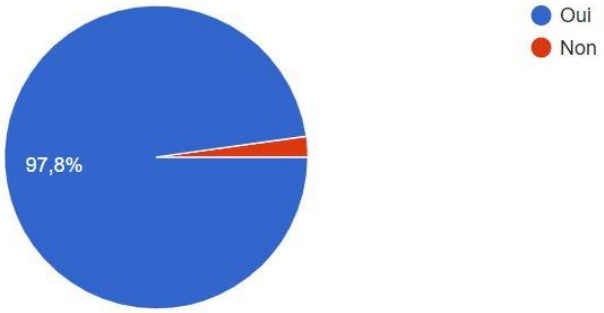
თუ იცით რომელ ინსტიტუციას ევალება პეროსნალურ მონაცემთა დაცვის საკითხების კონტროლი საქართველოში

140 réponses



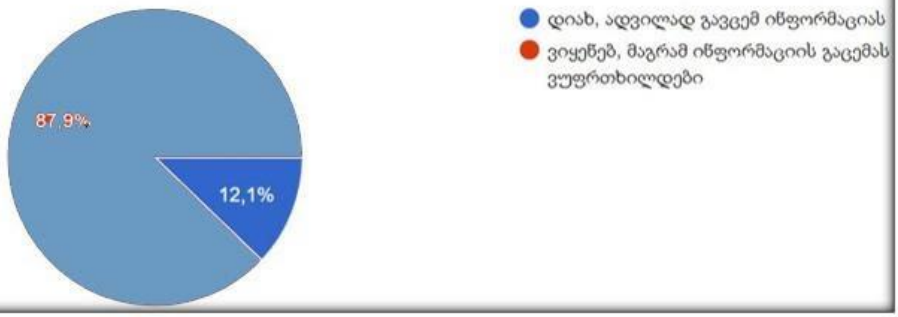
Etes vous usager des réseaux sociaux ?

90 réponses



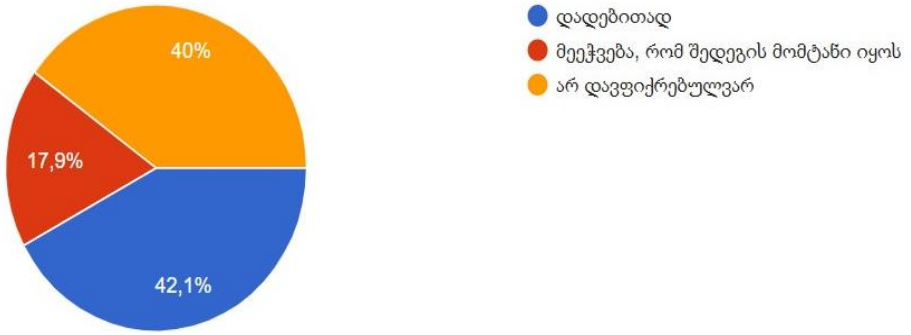
თუ იყენებთ სოციალურ ქსელს და რამდენად ადვილად გასცემთ თქვენს მონაცემებს

140 réponses



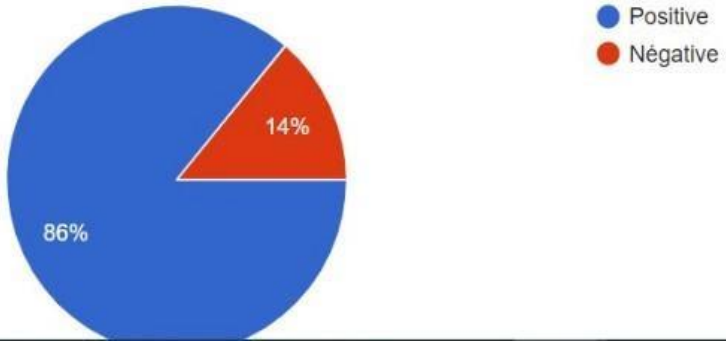
როგორ აფასებთ სახელწიფო ინსპექტორის აპარატის დაფუძნებას და რამდენად დროული იყო მისი დაარსება

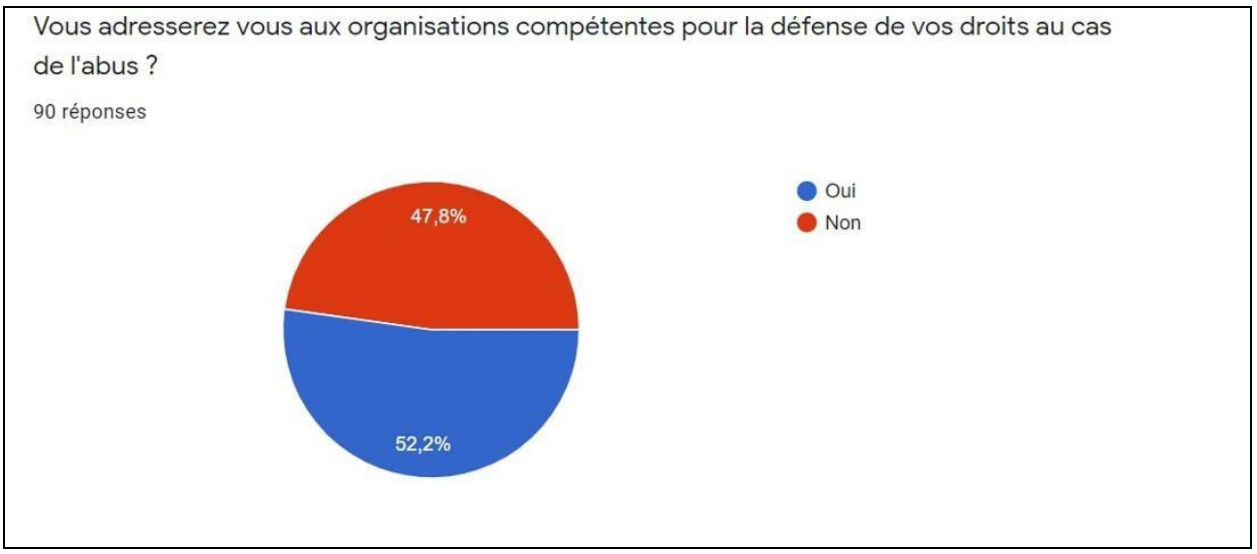
140 réponses

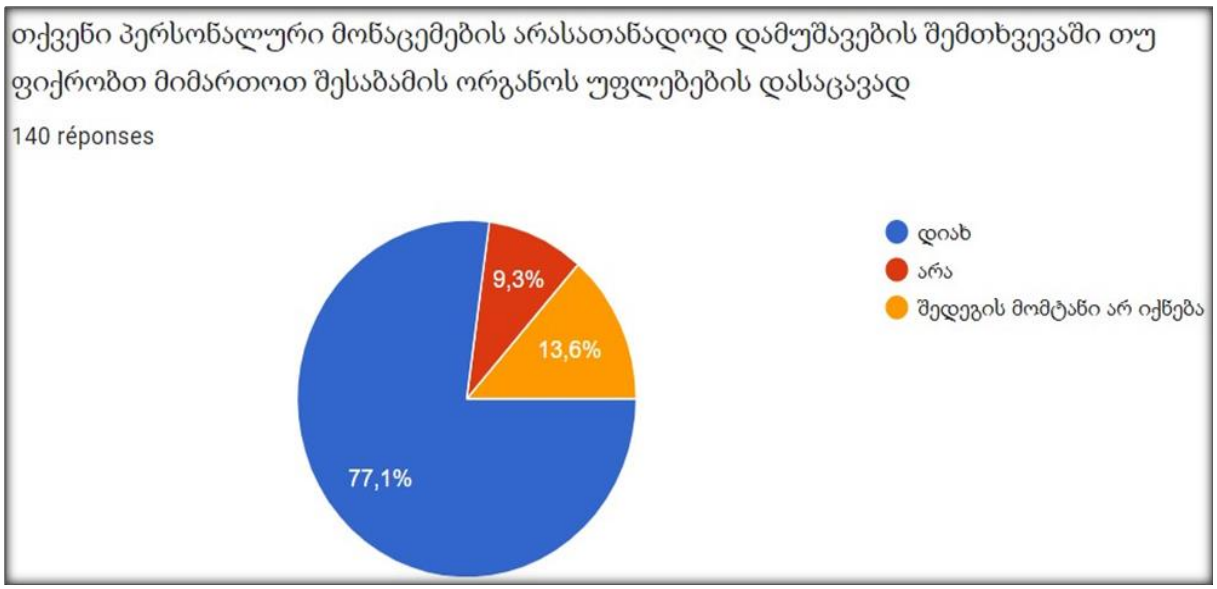


Comment appréciez vous le rôle de la CNIL dans la défense de nos droits

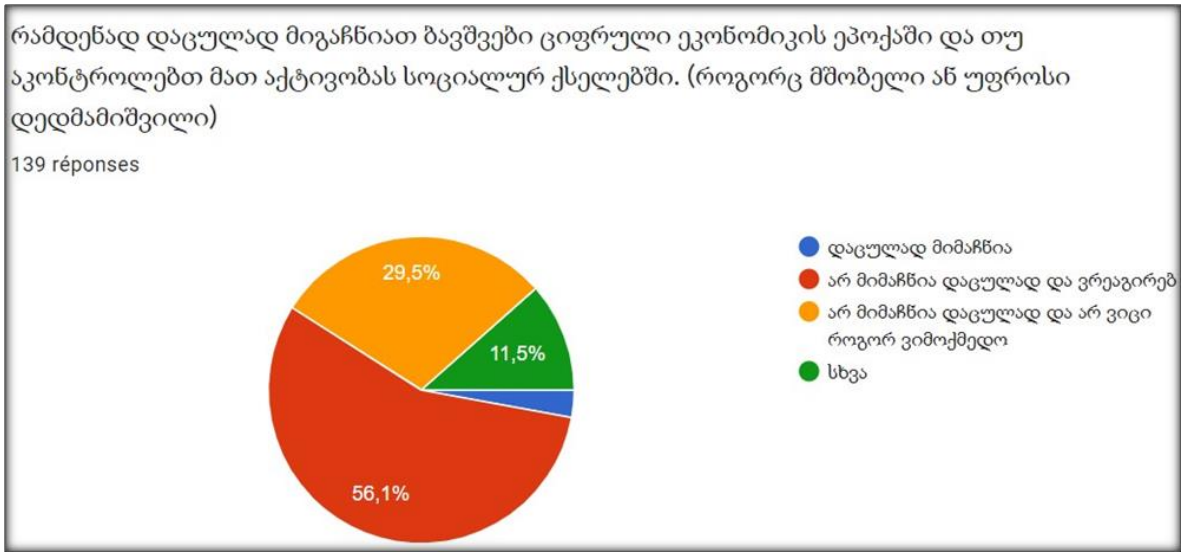
86 réponses

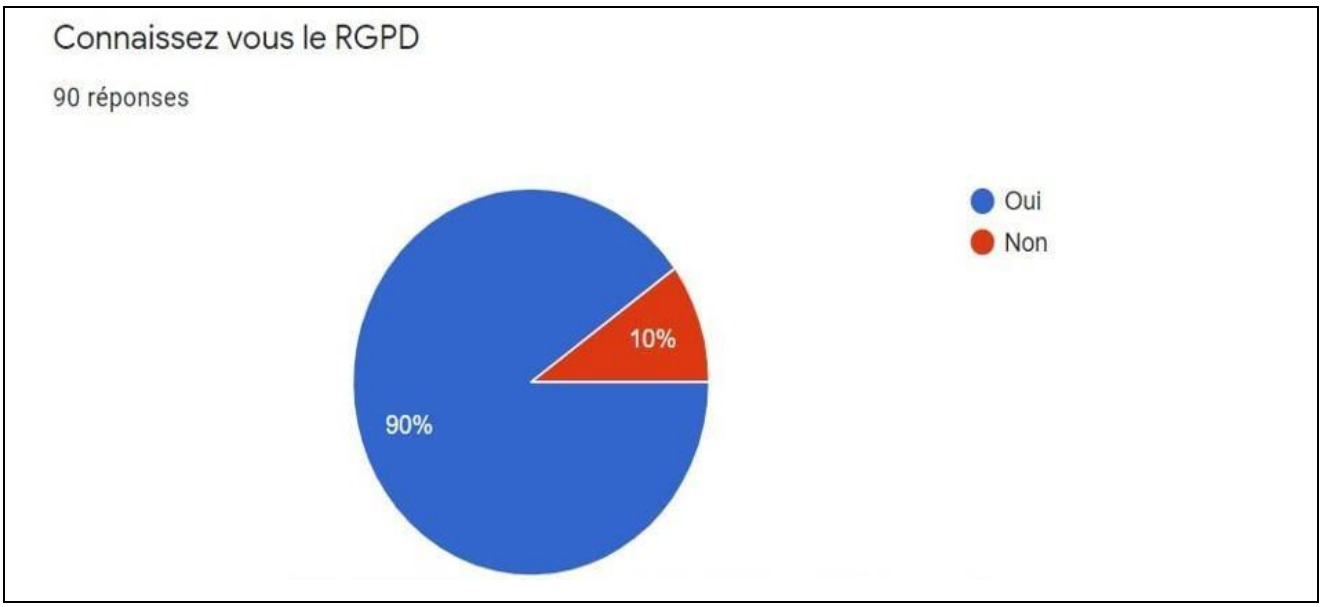


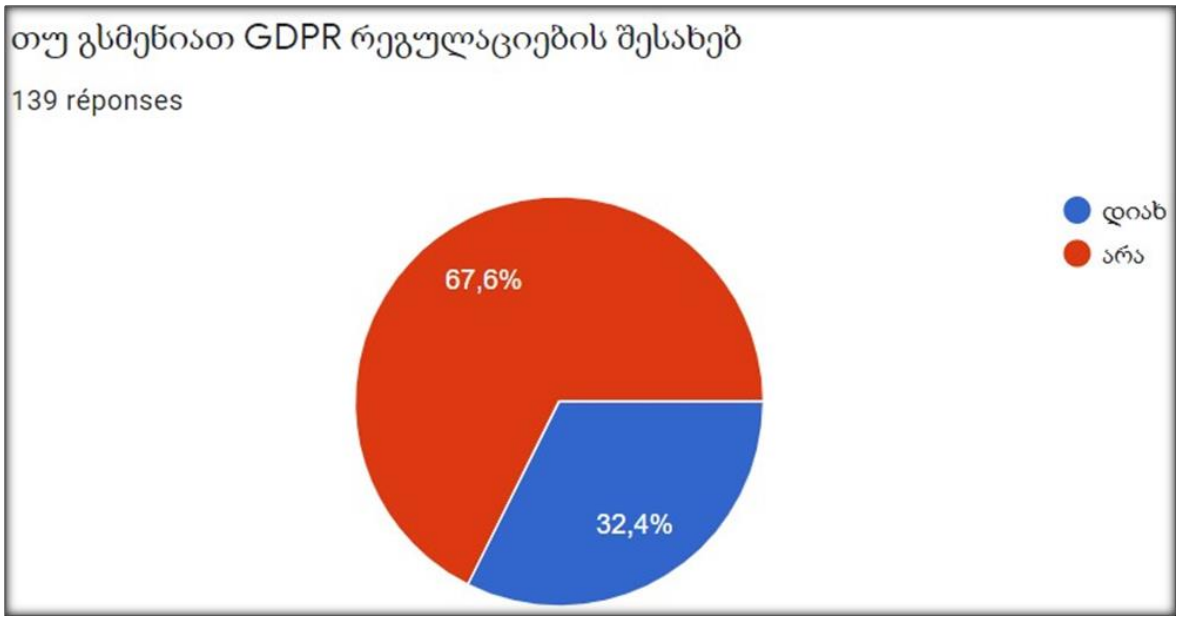

Vous adresserez vous aux organisations compétentes pour la défense de vos droits au cas de l'abus ?
90 réponses
47,8%
52,2%
Oui
Non

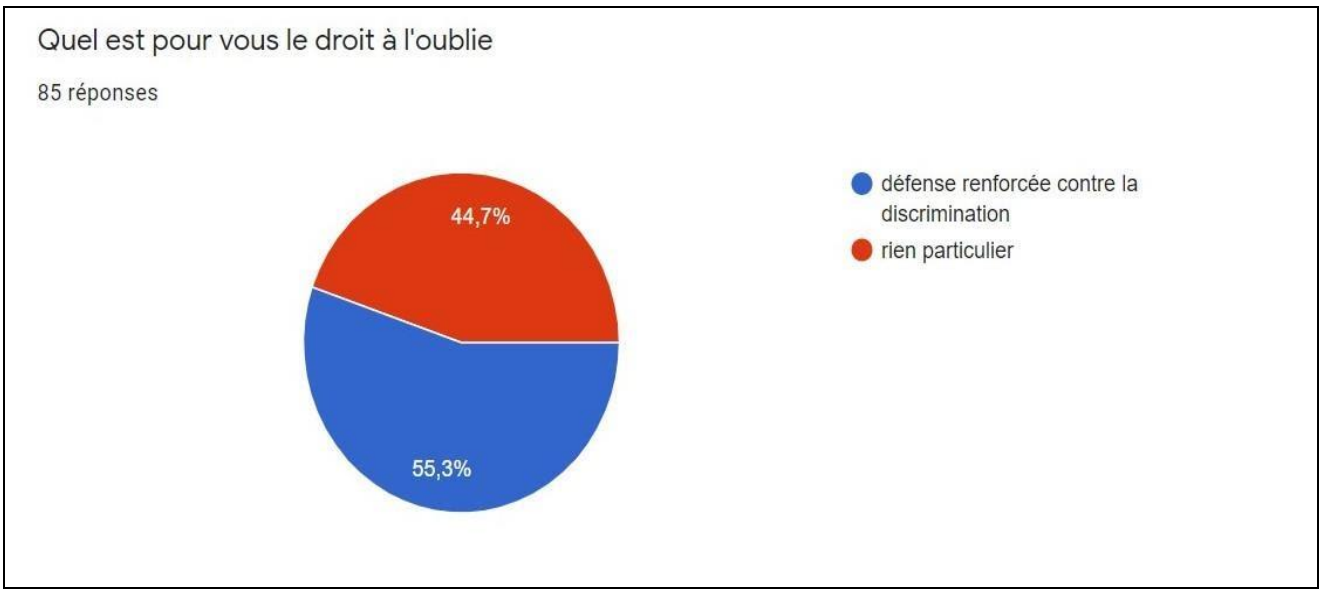

თქვენი პერსონალური მონაცემების არასათანადოდ დამუშავების შემთხვევაში თუ ფიქრობთ მიმართოთ შესაბამის ორგანოს უფლებების დასაცავად
140 réponses
9,3%
13,6%
77,1%
დიახ
არა
შედეგის მომტანი არ იქნება

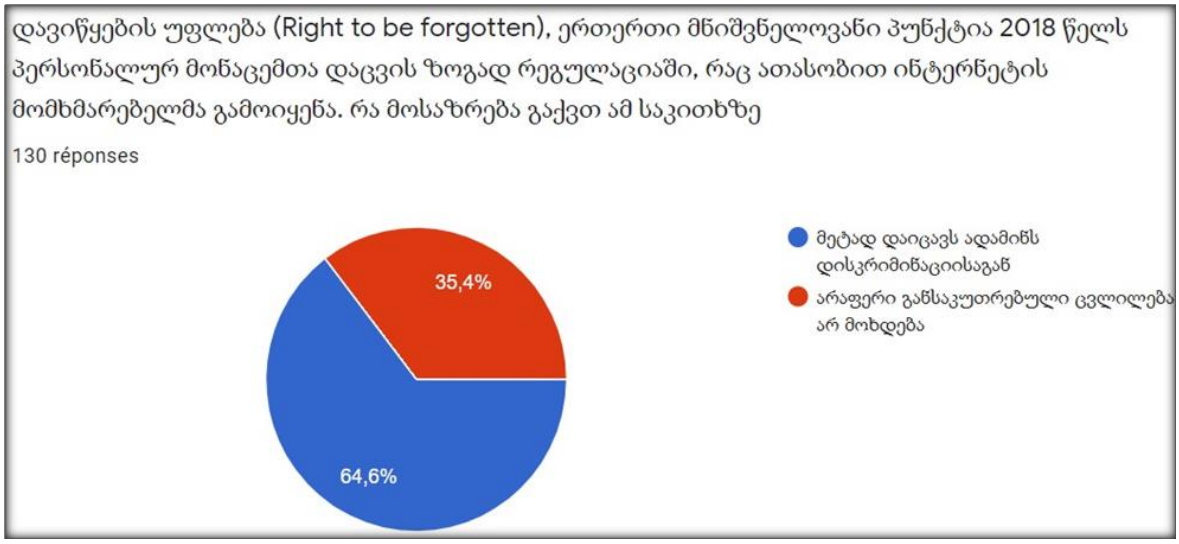

Les enfants sont ils bien protégés dans notre ère numérique ?
90 réponses
92,2%
7,8%
Oui
Non


რამდენად დაცულად მიგაჩნიათ ბავშვები ციფრული ეკონომიკის ეპოქაში და თუ აკონტროლებთ მათ აქტივობას სოციალურ ქსელებში. (როგორც მშობელი ან უფროსი დედმამიშვილი)
139 réponses
29,5%
11,5%
56,1%
დაცულად მიმაჩნია
არ მიმაჩნია დაცულად და ვრეაგირებ
არ მიმაჩნია დაცულად და არ ვიცი როგორ ვიმოქმედო
სხვა


Connaissez vous le RGPD
90 réponses
Oui
Non
10%
90%

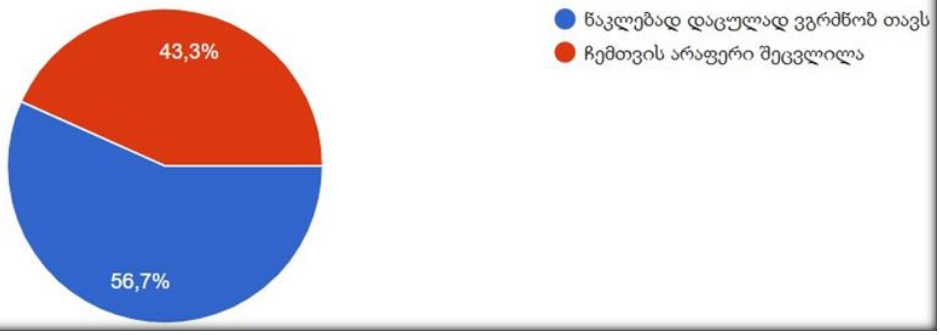

თუ გსმენიათ GDPR რეგულაციების შესახებ
139 réponses
დიახ
არა
67,6%
32,4%


Quel est pour vous le droit à l'oublie
85 réponses
44,7%
55,3%
défense renforcée contre la discrimination
rien particulier


დავიწყების უფლება (Right to be forgotten), ერთერთი მნიშვნელოვანი პუნქტია 2018 წელს პერსონალურ მონაცემთა დაცვის ზოგად რეგულაციაში, რაც ათასობით ინტერნეტის მომხმარებელმა გამოიყენა. რა მოსაზრება გაქვთ ამ საკითხზე
130 réponses
35,4%
64,6%
მეტად დაიცავს ადამიწს დისკრიმიწაციისაგაწ
არაფერი გაწსაკუთრებული ცვლილება არ მოხდება

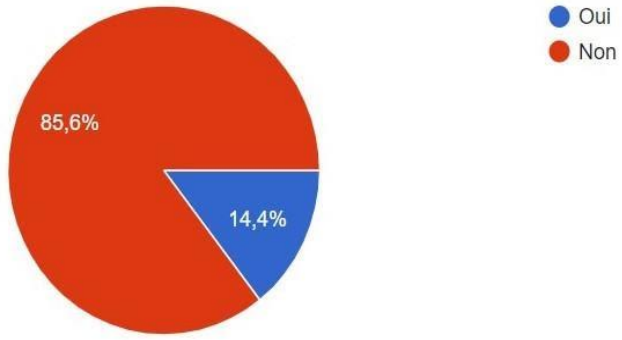
2019 წლის 28 ოქტომბერს საქართველოში განხორციელდა ფართომასშტაბიანი კიბერშეტევა საქართველოს პრეზიდენტის ადმინისტრაციის,სხვადასხვა მუნიციპალიტეტის საკრებულოების, სახელმწიფო, კომერციული და მედია ორგანიზაციების ვებ-გვერდებზე, სერვერებსა და სხვა მართვით სისტემებზე. ამ მოვლენის მერე ნაკლებად დაცული გგონიათ თქვენი მონაცემები?

134 réponses



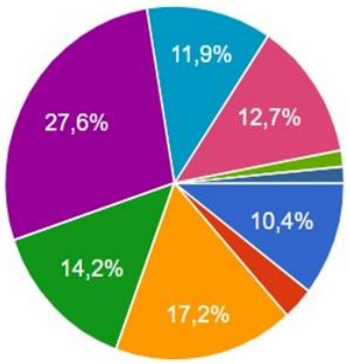
Avez vous entendu parler des cyberattaques de Géorgie de 2019 ?
https://www.lemonde.fr/international/article/2019/10/30/l-etrange-cyberattaque-qui-affole-la-georgie_6017435_3210.html

90 réponses



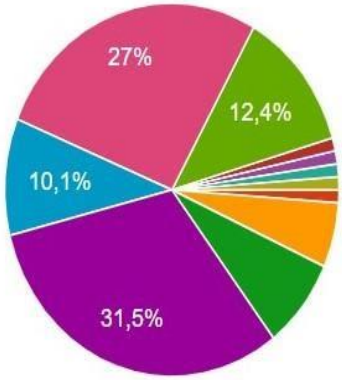
როგორ შეფასებთ კიბერ უსაფრთხოების დონეს საქართველოში? 1 დან 10 ქულამდე

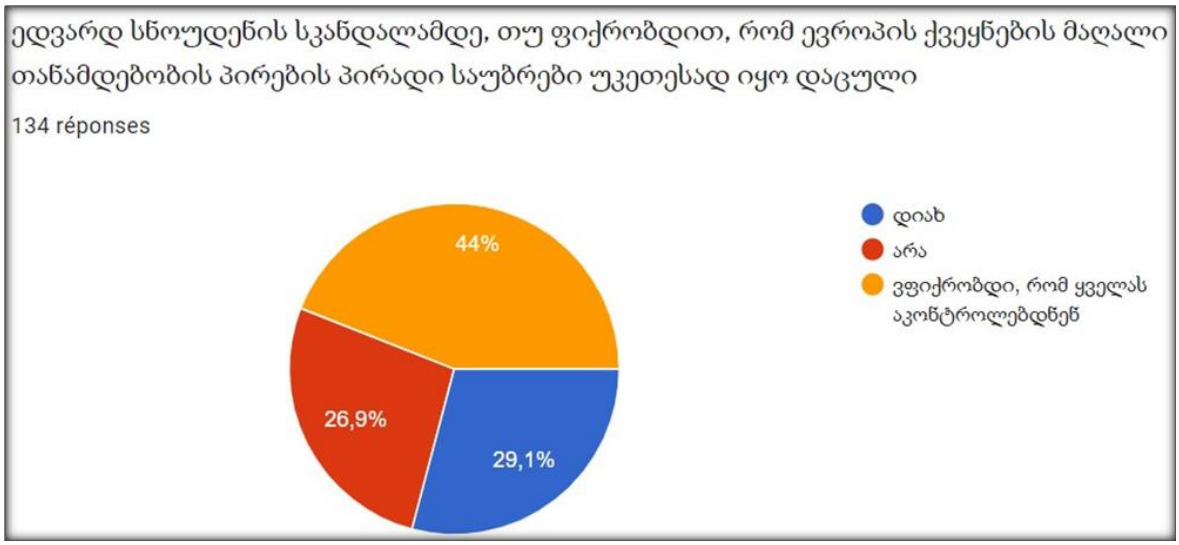
134 réponses

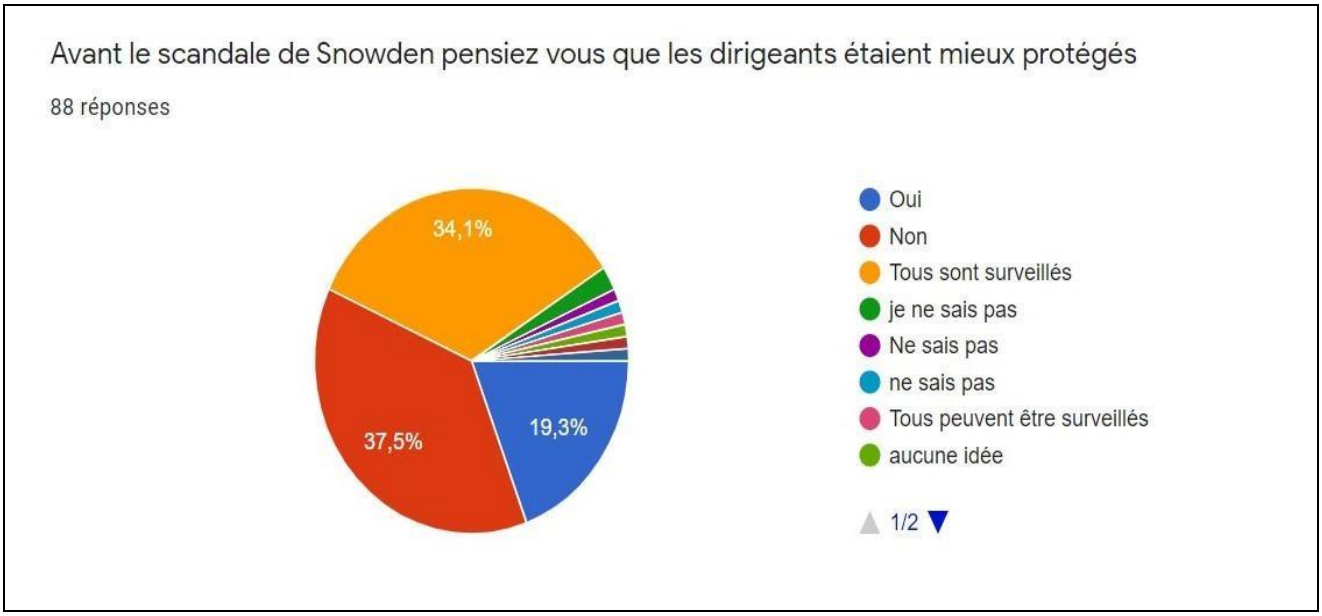


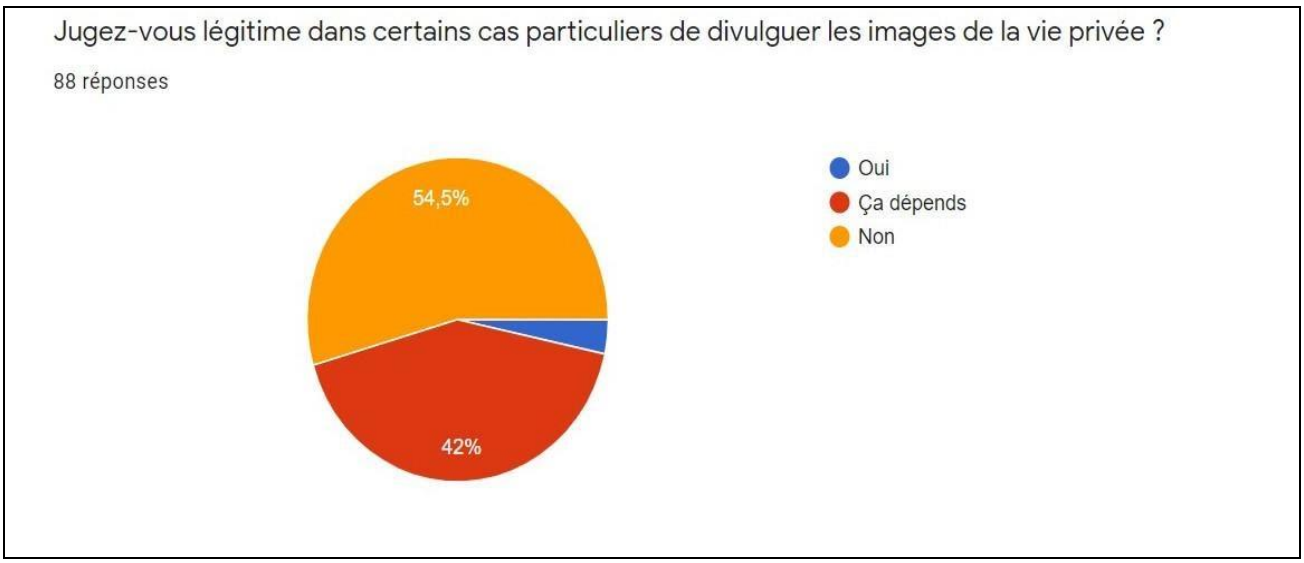
Comment qualifieriez-vous le niveau de cybersécurité en France?

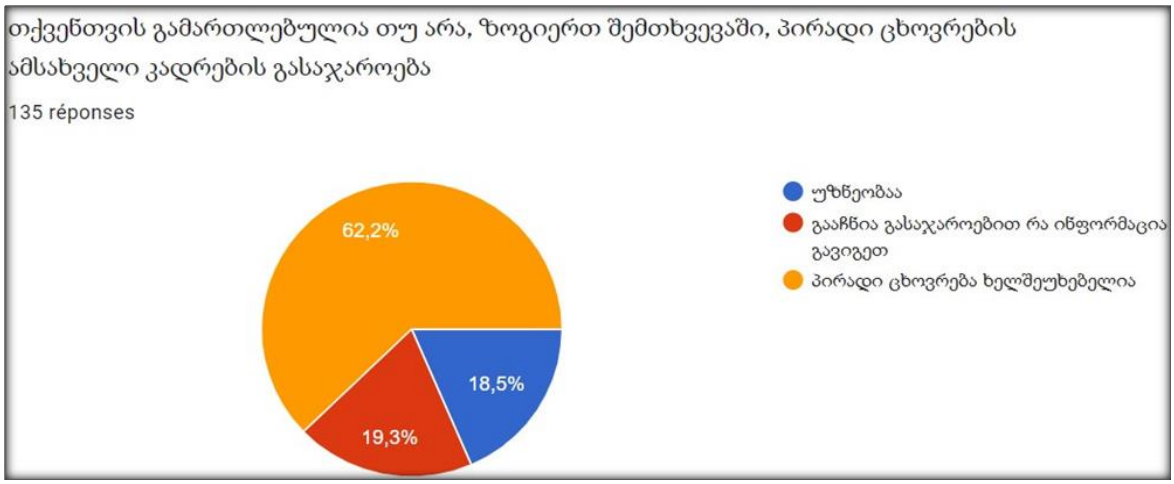
89 réponses




ედვარდ სნოუდენის სკანდალამდე, თუ ფიქრობდით, რომ ევროპის ქვეყნების მაღალი თანამდებობის პირების პირადი საუბრები უკეთესად იყო დაცული
134 réponses
44%
26,9%
29,1%
დიახ
არა
ვფიქრობდი, რომ ყველას აკონტროლებდნენ

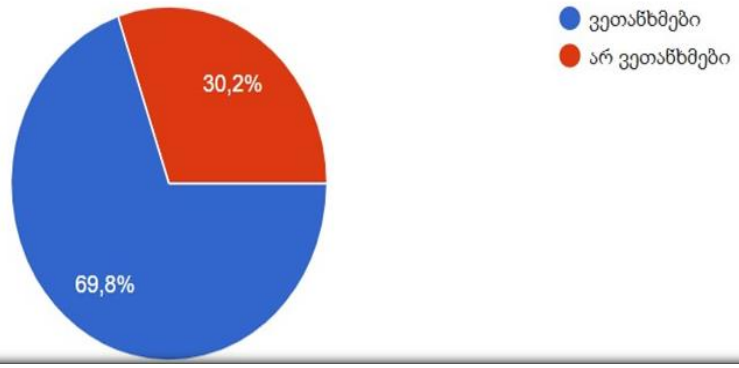

Avant le scandale de Snowden pensiez vous que les dirigeants étaient mieux protégés
88 réponses
34,1%
37,5%
19,3%
Oui
Non
Tous sont surveillés
je ne sais pas
Ne sais pas
ne sais pas
Tous peuvent être surveillés
aucune idée
1/2


Jugez-vous légitime dans certains cas particuliers de divulguer les images de la vie privée ?
88 réponses
54,5%
42%
Oui
Ça dépends
Non


თქვენთვის გამართლებულია თუ არა, ზოგიერთ შემთხვევაში, პირადი ცხოვრების ამსახველი კადრების გასაჯაროება
135 réponses
62,2%
18,5%
19,3%
უზნეობაა
გააჩნია გასაჯაროებით რა ინფორმაცია გავიგეთ
პირადი ცხოვრება ხელშეუხებელია

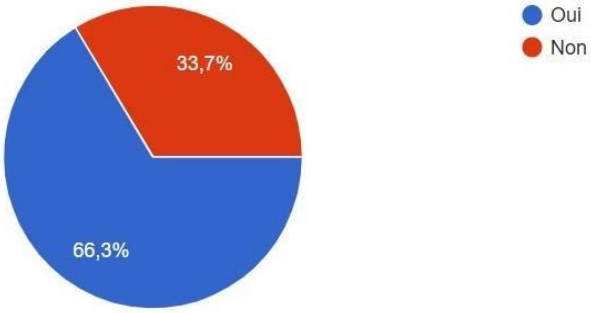
ნოვაკის შემთხვევის შემდეგ ევროპის სასამართლო სისტემამ პირად მონაცემად აღიარა საგამოცდო ნაშრომები, ნიშნები, ანოტაციები საგამოცდო ფურცელზე. თუ ეთანხმებით ამ მოსაზრებას (Affaire Novak, C 434/16, arrêt du 20 décembre 2017)

129 réponses



M. Nowak a échoué, en tant qu'expert-comptable stagiaire irlandais, à un examen de comptabilité. A la suite de cet échec, il a introduit une réclamation visant à contester le résultat de cet examen. Sa réclamation ayant été rejetée, il a présenté une demande d'accès visant l'ensemble des données à caractère personnel le concernant, détenues par l'ordre irlandais des experts-comptables.Ce dernier lui a communiqué des documents, mais a refusé de lui transmettre sa copie d'examen, au motif que celle-ci ne contenait pas de données à caractère personnel. la copie d'examen contient elle pour vous de données à caractère personnel ?

89 réponses

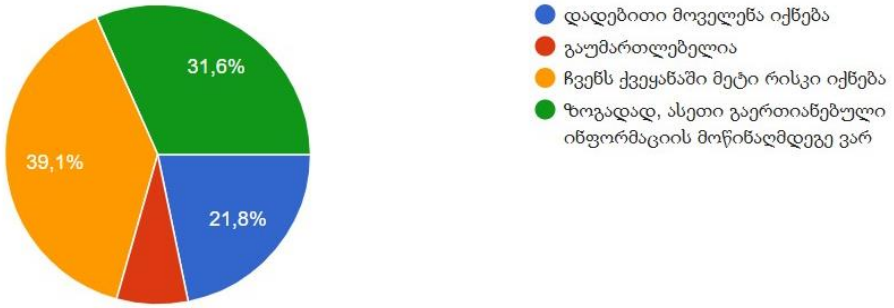


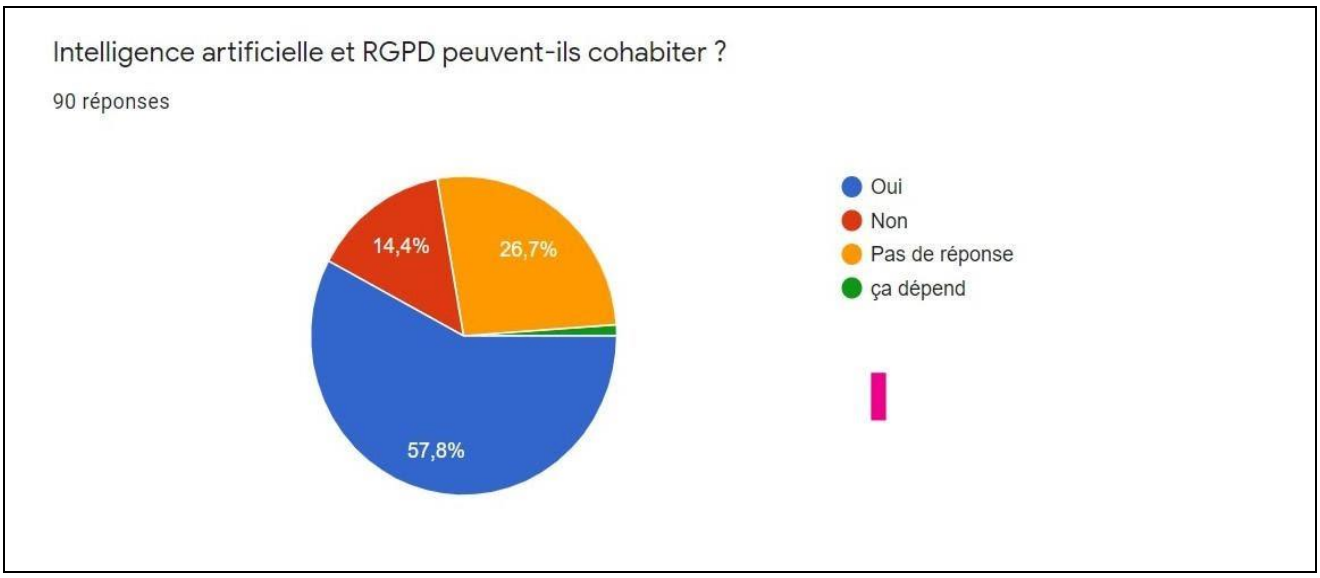
Arrêté du 23 novembre 2018 portant création d'un traitement automatisé de données à caractère personnel dénommé « Système d'information sur l'orientation dans le supérieur » (ORISUP) Qu' es ce que c' est pour vous ?

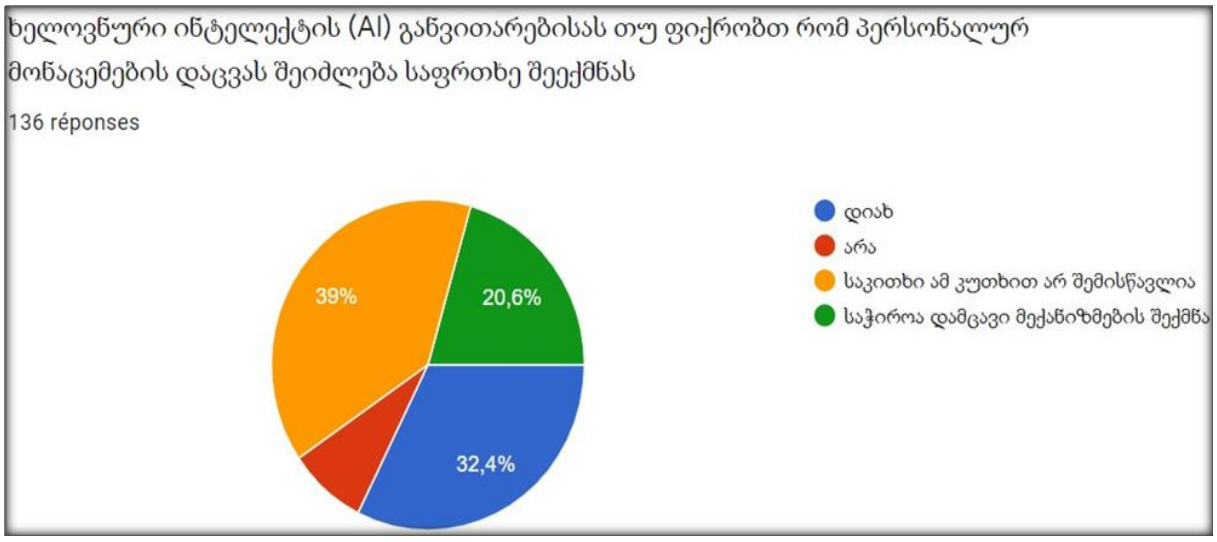
86 réponses

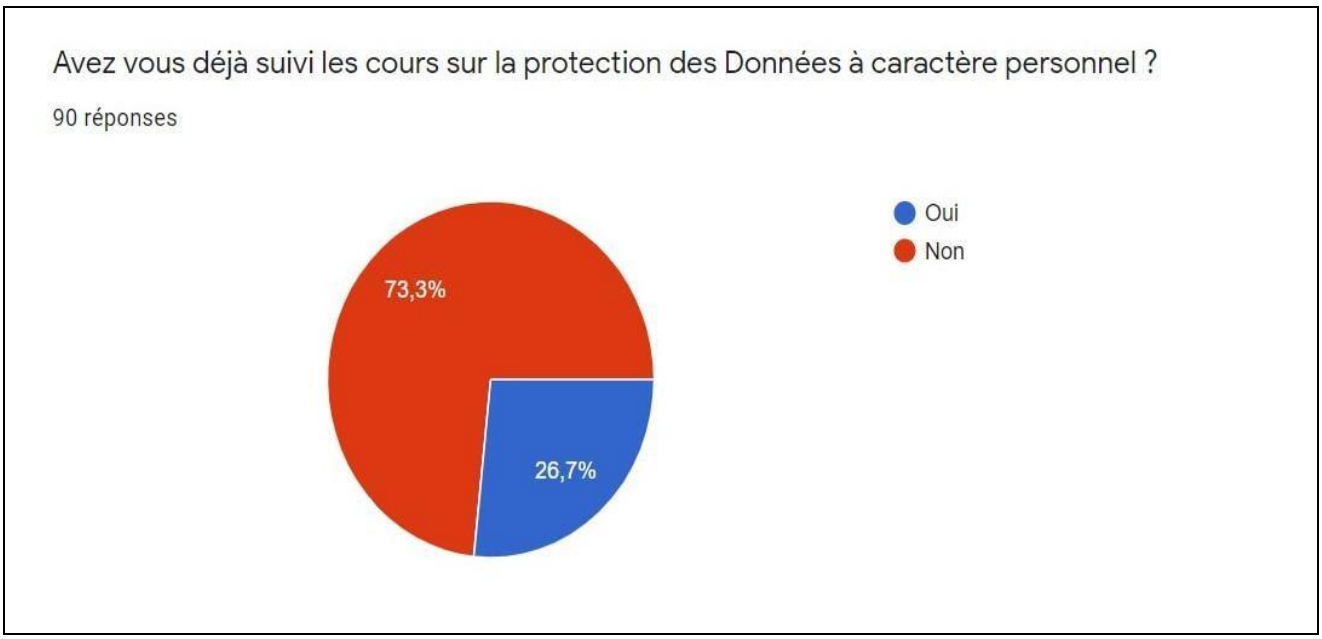
საფრანგეთში 2018 წლიდან არსებობს ინფორმაციული სიტემა უმაღლეს სასწავლებლებში ორიენტაციის შესახებ « système d'information sur l'orientation dans le supérieur ». შემქმნელების მოსაზრებით, ეს სიტემა ხელს უწყობს არსებული პრობლემატიკის და ინტერესების დანახვას, მომავლში მათი სრულყოფის მიზნით. თითოეულ მოსწავლეზე და სტუდენტზე თავმოყრილია სრული ინფორმაცია სკოლიდან უნივერსიტეტამდე. ანონიმიზირებული ინფორმაცია მიეწოდება მკვლევარებსაც. რამდენად გამართლებულად მიაგაჩნიათ მსგავსი სისტემის არსებობა, და იგივე პრაქტიკის გამოყენება საქართველოში

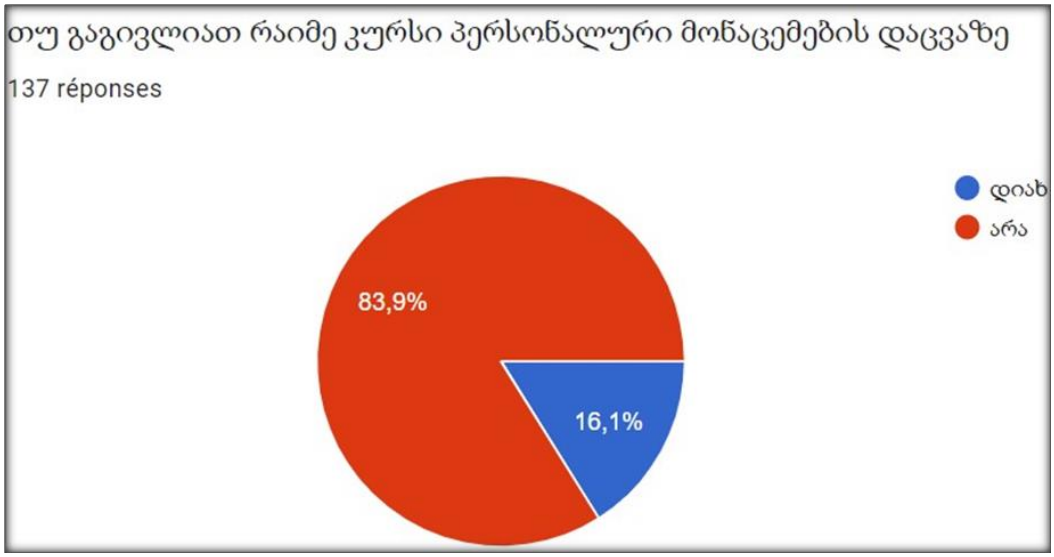
133 réponses




Intelligence artificielle et RGPD peuvent-ils cohabiter ?
90 réponses
14,4%
26,7%
57,8%
Oui
Non
Pas de réponse
ça dépend


ხელოვნური ინტელექტის (AI) განვითარებისას თუ ფიქრობთ რომ პერსონალურ მონაცემების დაცვას შეიძლება საფრთხე შეექმნას
136 réponses
39%
20,6%
32,4%
დიახ
არა
საკითხი ამ კუთხით არ შემისწავლია
საჭიროა დამცავი მექანიზმების შექმნა


Avez vous déjà suivi les cours sur la protection des Données à caractère personnel ?
90 réponses
Oui
Non
73,3%
26,7%


თუ გაგივლიათ რაიმე კურსი პერსონალური მონაცემების დაცვაზე
137 réponses
დიახ
არა
83,9%
16,1%

13.5 Conclusion

Dans les années 1990, les entreprises se contentaient de rassembler des informations liées au marché (parts de marché, caractéristiques des clients...). Actuellement, elles ciblent des données spécifiques pour chaque consommateur, ses caractéristiques, ses préférences de consommation. A l'époque, la collecte se faisait face-à-face ou par téléphone, ou par courrier. Aujourd'hui, la nouvelle technologie a complètement changé la situation.

Récolte, stockage et transmission des données s'effectuent à grande vitesse à travers le monde. D'une part, la technologie a évolué, mais d'autre part cela a posé le problème de la protection de la vie privée. Pour les entreprises, la collecte et le traitement de données sont une affaire stratégique qui doit être traitée d'une part par les lois et d'autre part par l'éthique personnelle.

En étudiant la protection des données personnelles, on remarque rapidement que plusieurs sciences s'intéressent à ce sujet. Citons notamment l'intérêt des « marketologues » pour la collecte des données des clients. Tout aussi grand est l'intérêt et les avis des sociologues, psychologues et informaticiens sur ce thème.

En sociologie, on parle d'un contrat social, forme d'échange dans lequel les individus s'engagent en contrepartie de bénéfices économiques ou sociaux. La notion de « contrat social » implique de comprendre que les individus sont prêts à fournir des informations personnelles s'ils y trouvent une contrepartie convenable.
En psychologie, il a été constaté que donner des informations sur sa personnalité était un phénomène lié au développement de l'intimité. La vie privée serait alors une base sur laquelle l'intimité pourrait se construire.

La variété des réponses que ce sujet suscite pose la question : **en quoi consiste le respect de la vie privée, et où se trouve la frontière entre les données personnelles et les intérêt commerciaux et sécuritaires ?**
Il existe plusieurs ouvrages sur le dévoilement de soi qui se définit comme le processus par lequel on donne des informations personnelles aux autres. Les théories de la personnalité ont centré leur attention sur les facteurs qui expliquent pourquoi un individu est ce qu'il est. L'individu habite dans la société et il a des échanges réguliers avec les autres individus, membres de ce groupe.

On peut distinguer deux types d'échanges dans nos sociétés :

- Échange économique (quand « les biens » peuvent être échangés contre leur équivalent monétaire) ;
- Échange social, qui peut être défini comme un échange dans lequel l'un des deux partenaires peut s'engager sans connaître exactement la contrepartie qui lui sera proposée [11].

La satisfaction commerciale peut être influencée par des facteurs différents, l'origine géographique d'un individu ou les goûts des individus. D'après un sociologue français, tout individu est un *homo oeconomicus* qui optimise ses profits sans forcément rechercher de rétribution symbolique ni psychologique [88].

13.3.1 Nos recommandations :

- Pour le registre public, nous recommandons de créer un tel système quand les individus n'ont pas accès aux informations détaillées.
    - **Distinguer les personnes travaillant dans le système public (fonctionnaires, politiciens, élus) dont la fortune est au centre de l'intérêt public des autres personnes.**
    - **Créér un sytème de scan de la pièce d'identité pour obtenir le droit d'accès aux informations détaillées ou utiliser une pratique similaire à celle utilisée pour la signature électronique.**

Avec cette pratique, il sera possible d'éviter de connaître les informations détaillées sur la personne concernée même si l'on obtient son numéro d'identité.

- Mêmes recommandations pour le site des élections. Nous pensons qu'il faut utiliser le système de scan de l'identité ou ajouter des options supplémentaires pour obtenir un droit d'accès aux systèmes
- Interdire la demande de numéro d'identité de la part des commerces et anonymiser les données du commerce.

Ces deux cas (sites internet de registre public et site des élections) restent toujours préoccupants.

Table des figures

BIBLIOGRAPHIE

1. 32nd International Conference of Data Protection and Privacy Commissioners, *Resolution on Privacy by Design,* Jerusalem, Israel 27-29 October, 2010

2. ADAM Luis, *Zdnet*, « La CNIL s'inquiète des dispositifs de mesure de fréquentation en magasin », 20 août 2014, https://www.zdnet.fr/actualites/la-cnil-s-inquiete-des-dispositifs-de-mesure-de-frequentation-en-magasin-39805017.htm

3. AFP et A.T, « Facebook : comment sont exploitées vos données personnelles ? », 30 janvier 2019, https://www.rtbf.be/info/medias/detail_facebook-comment-sont-exploitees-vos-donnees-personnelles?id=10132214

4. AFP relaxnews, « Sécurité en ligne : 52 % des sites ne protègent pas assez les données personnelles de leurs visiteurs » in *Fashbion Network,* 5 janv. 2016, https://fr.fashionnetwork.com/news/Securite-en-ligne-52-des-sites-ne-protegent-pas-assez-les-donnees-personnelles-de-leurs-visiteurs,612778.html

5. Altares (groupe), « Défaillances et sauvegardes d'entreprises en France » https://www.altares.com/fr/publications/etudes-defaillances-sauvegardes-entreprises/

6. ANTO´N A.I., EARP J.B., HE Q., STUFFLEBEAM W., BOLCHINI D., and JENSEN C., "Financial Privacy Policies and the Need for Standardization," 2004, https://ssl.lu.usi.ch/entityws/Allegati/pdf_pub1430.pdf

7. Association des archivistes français, *Principes et pratiques du métier d'archiviste*, Paris, 2004

8. Bhattacharya Santanu, « AI predictions for 2019. 2019 will be a watershed for AI », 31 décembre 2018, https://towardsdatascience.com/ai-predictions-for-2019-610b8de56aad

9. BECCHETTI-BIZOT, Inspectrice générale de l'éducation nationale, *Repenser la forme scolaire à l'heure du numérique Vers de nouvelles manières d'apprendre et d'enseigne,* rapport IGEN 2017-056, mai 2017

10. BEKY Ariane, "Big Data et analytique : un marché promis à une croissance à deux chiffres", *silicon.fr,* 18 août 2021, https://www.silicon.fr/big-data-analytique-croissance-414574.html#

11. BLAU P.M., Exchange and Power in Social Life, 1986, Routledge

12. BRAS Jean-Louis, Rapport sur la gouvernance et l'utilisation des données de santé, septembre 2013

13. BREAUX T.D., VAIL M.W., ANTO´N A.I., "Towards Compliance: Extracting Rights and Obligations to Align Requirements with Regulations," 2006.

14. Bureau Van Dijk, https://www.bvdinfo.com/fr-fr/

15. Bureau Van Dijk, https://wrds-www.wharton.upenn.edu/pages/about/data-vendors/bureau-van-dijk-bvd/

16. Bureau de l'inspecteur d'État de Géorgie, « Règles de conservation, d'utilisation et de comptabilisation du protocole d'infraction administrative » Annexe - https://personaldata.ge/cdn/2021/02/ADMINISTRATIVE-OFFENCES-CODE-OF-GEORGIA-consolidated-version-23.12.2017-07.03.2018.pdf

17. BURTON Betsy, HOWARD Chris, "Architecting Digital Business", Gartner Event Summary: *U.S. Symposium/ITxpo*, Orlando (Floride), octobre 2015

18. CAPELLE-BLANCARD Gunther, BELLANDO Raphaëlle, *L'accès aux données bancaires et financières : une mission de service public* ; Rapport du groupe de travail du Cnis, Juillet 2015

19. Capgemini Research Institute, "Championing Data Protection and Privacy", reports 2019

20. CASILLI Antonio, *Les liaisons numériques. Vers une nouvelle socialibilité ?* Seuil, 2010

21. CAVALLARI Peppe, « La culture numérique selon Dominique Cardon », *11 février 2020, https://www.erudit.org/en/journals/sp/2019-sp05120/1067448ar/*

22. Centre d'Accès aux Données Sécurisé CASD, https://www.casd.eu/

23. CHAMPEAU Guillaume, "Promouvoir le « privacy by design » pour les startups européennes", 21 septembre 2016, https://www.numerama.com/business/196332-promouvoir-privacy-by-design-startups-europeennes.html

24. Charte des droits fondamentaux de l'Union Européenne, 2000/C 364/01

25. Charte du G8 pour l'Ouverture des Données Publiques ; 17 et 18 juin 2013 au Sommet de Lough Erne, https://cms.geobretagne.fr/sites/default/files/documents/2013.06.18_Charte-du-G8-pour-l-Ouverture-des-Donnees-Publiques-Francais.pdf

26. Club de la sécurité de l'information français CLUSIF, « Données à caractère personnel », Les Fiches du CLUSIF-RGPD, Club de la sécurité de l'information français, 2018 https://clusif.fr/wp-content/uploads/2019/04/faq_donnees_personnelles.pdf

27. CNIL, Recommandation du 29 novembre 2001 sur la diffusion de données personnelles sur Internet par les banques de données de jurisprudence : pour un encadrement législatif renforçant la protection des données à caractère personnel en matière de diffusion de décisions de justice. Document adopté par la Commission le 19 janvier 2006, https://www.cnil.fr/sites/default/files/typo/document/Bilan_BDD_jurisprudence_decisions_de_justice.pdf

28. CNIL, *24ème Rapport d'activité* 2003

29. CNIL, « Délibération n° 2005-213 du 11 octobre 2005 de la CNIL concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel »

30. CNIL « Synthèse des réponses à la consultation publique sur le Cloud computing lancée par la CNIL d'octobre à décembre 2011 et analyse de la CNIL », 2011

31. CNIL, « Délibération n° 2012-209 du 21 juin 2012 portant création d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion de clients et de prospects »

32. CNIL, « Projet de loi relatif à la géolocalisation » : avis de la CNIL publiée à la demande de la Commission des lois de l'Assemblée nationale, 11 février 2014

33. CNIL, Le G29 publie un avis sur les techniques d'anonymisation, Avis 05/2014, https://www.cnil.fr/fr/le-g29-publie-un-avis-sur-les-techniques-danonymisation

34. CNIL, « Fichiers clients-prospects et vente en ligne », Déclaration n°48, 21 juillet 2016, https://elections.cnil.fr/fr/declaration/ns-048-fichiers-clients-prospects-et-vente-en-ligne

35. CNIL, « Commerce et données personnelles », édition octobre 2016

36. CNIL, « Notoriété et attentes vis-à-vis des algorithmes », Sondage Ifop pour la CNIL, 2017, https://www.cnil.fr/sites/default/files/atoms/files/presentation_ifop_-_presentation.pdf

37. CNIL, « La sécurité des données personnelles », Les guides de la CNIL, 2018

38. CNIL, « Recherches dans le domaine de la santé avec recueil du consentement », 2018 https://www.cnil.fr/fr/declaration/mr-001-recherches-dans-le-domaine-de-la-sante-avec-recueil-du-consentement

39. CNIL, « Recommandation : Le paiement à distance par carte bancaire », 28 février 2019

40. CNIL, « L'anonymisation des données, un traitement clé pour l'open data », 17 octobre 2019

41. CNIL, « Ce qu'il faut savoir sur les règles d'entreprise contraignantes » recommandation de la CNIL, 7 février 2020

42. CNIL, « Verbalisation par lecture automatisée des plaques d'immatriculation (LAPI) : la CNIL met en garde contre les mauvaises pratiques », 25 août 2020, https://www.cnil.fr/fr/verbalisation-par-lecture-automatisee-des-plaques-dimmatriculation-lapi-la-cnil-met-en-garde

43. CNIL, « La Protection des données dans le monde », carte interactive 23/11/2020, https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

44. CNIL, « La CNIL en bref », https://www.cnil.fr/sites/default/files/atoms/files/la_cnil_en_bref_2021.pdf

45. CNIL, « Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing », https://www.cnil.fr/sites/default/files/typo/document/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf

46. CNIL, « Les questions posées pour la protection des données personnelles par l'externalisation hors de l'Union européenne des traitements informatiques » http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/20100909-externalisation.pdf

47. Code civil, Article 1108 « au titre de la validité d'un contrat »

48. Code civil, Article 1116

49. Code civil, article 1128, La validité du contrat (Articles 1128 à 1171)

50. Code civil, Article 1130, « Des différentes manières dont on acquiert la propriété » (Articles 711 à 2278

51. Code civil, Article 1369-2

52. Code civil, Article 1369-3

53. Code civil, Article 1599

54. Code civil, Article 1603, « la responsabilité du vendeur et la livraison de la chose »

55. Code civil, Article 1625, Section 3 : « De la garantie » (Articles 1625 à 1649)

56. Code du commerce, Décret 2012-115 du 2 octobre 2012. art. L441-6.

57. Code des postes et des communications électroniques, Partie législative (Articles L1 à L144)

58. Code du Patrimoine, article L.211-1

59. Code du travail, Article L1222-4

60. Code du travail, Article L. 2323-13

61. Code général des impôts, article 1734

62. Code monétaire et financier ; Partie législative, Articles L111-1 à L773-1

63. Code pénal, Articles 226-1 à 226-7, Article 226-4-1 ; Section 1 : « De l'atteinte à la vie privée »

64. « Code Week », initiative citoyenne soutenue par la Commission Européenne, https://codeweek.eu/about

65. Commission européenne, https://ec.europa.eu/info/index_en

66. Commission européenne, « Peut-on traiter les données pour toutes les finalités ? », avis 03/2003, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/purpose-data-processing/can-data-be-processed-any-purpose_fr

67. Commission européenne, "Binding Corporate Rules (BCR) Corporate rules for data transfers within multinational companies", *Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR*, 11 avril 2018

68. Commission européenne, « Article 29 Working Party", http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140612_wp29_bcr-p_general_ep_president.pdf

69. Commission européenne, « Rapport sur les règles de l'UE en matière de protection des données donnent aux citoyens les moyens d'agir et sont adaptées à l'ère du numérique », Communiqué de presse, Bruxelles, 24 juin 2020

70. Comité des ministres du Conseil de l'Europe, Article 1.2 de la Recommandation n° R (85) 20, 25 octobre 1985

71. Comité des Ministres du Conseil de l'Europe, Recommandation N° R (87) 15 du comité des ministres aux Etats membres visant à « réglementer l'utilisation de données à caractère personnel » (adoptée par le Comité des Ministres le 17 septembre 1987) Madrid, Espagne, 4-6 novembre 2009

72. Confédération suisse, Préposé fédéral à la protection des données et à la transparence, 22 octobre 2015 https://www.edoeb.admin.ch/edoeb/fr/home.html

73. Conseil général de l'économie, de l'industrue, de l'énergie et des technologies, 13 mai 2016, 3Modalités de régulation des algorithmes de traitement des contenus", https://www.economie.gouv.fr/files/files/directions_services/cge/regulation-algorithmes.pdf

74. Constitution de la Géorgie, Article 41

75. Convention des Nations unies relative aux droits de l'enfant, Article 16

76. Convention des Nations Unis sur les contrats de vente internationale de marchandise ; Secrétariat de la CNUDCI, Centre international de Vienne, 2011

77. Convention européenne des droits de l'homme (CEDH), article 5 « Droit à la liberté et à la sûreté »

78. Convention européenne pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, (Convention 108), Strasbourg, 28.01.1981 .

79. Cour de Cassation, Chambre Civile 1, du 23 octobre 1990, 89-13.163

80. Cour de Cassation, Chambre Civile, Chambre sociale, 13 janvier 2009, 07-44.718

81. Cours de cassation, Chambre Civile, Chambre sociale, Arrêt du 23 avril 2013, 11-26.099, https://www.legifrance.gouv.fr/juri/id/JURITEXT000027367452/

82. Cour (grande chambre), Arrêt du 13 mai 2014. Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A62012CJ0131

83. Déclaration de confidentialité procédure d'évaluation du respect des exigences d'honorabilité et de compétences, https://acpr.banque-france.fr/sites/default/files/declaration-confidentialite-fit-and-proper-fr_0.pdf

84. Décret n°91-1404 du 27 décembre 1991 autorisant l'utilisation du répertoire national d'identification des personnes physiques par les employeurs dans les traitements automatisés de la paie et de la gestion du personnel

85. Décret n° 2003-303 du 27 mars 2003 relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques pour les déclarations sociales incombant aux entreprises et modifiant le code de la sécurité sociale (deuxième partie : Décrets en Conseil d'État), Article R115

86. Décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne

87. DEGRAVE Elise et VENDEROSE Benoît, « Privacy by Design et E-gouvernement : un modèle inédit en Belgique », *Pyramides* N°26-27, *Des outils numériques pour améliorer le fonctionnement de l'Etat : solutions ou problèmes ?* 2016, https://journals.openedition.org/pyramides/9921

88. DEMEULENAER Pierre, *« Homo oeconomicus », Enquête sur la constitution d'un paradigme*, Presse Universitaires de France, 2003

89. *La Dépêche*, « Sécurité en ligne : 52 % des sites ne protègent pas assez les données personnelles de leurs visiteurs » ; 5 janv. 2016, https://www.ladepeche.fr/article/2016/01/05/2250000-securite-ligne-52-sites-protegent-assez-donnees-personnelles-visiteurs.html

90. Digital Economy and Society Index (DESI), European Commission, "Thematic chapters", 2020, https://digital-strategy.ec.europa.eu/en/policies/desi

91. Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la « protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données »

92. Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le « traitement des données à caractère personnel le secteur des communications électroniques »

93. Directive de l'UE relative à la protection des données aux règles d'entreprise contraignantes applicables aux transferts internationaux de données, Document de travail WP 74: « Transferts de données personnelles vers des pays tiers: Application de l'article 26 (2) de la directive de l'UE », adoptée le 3 juin 2003

94. Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la « conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications », et modifiant la directive 2002/58/CE

95. Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à « la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données », et abrogeant la décision-cadre 2008/977/JAI du Conseil

96. Directive UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016

97. DOUEIHI Milad, *La Grande Conversion numérique (*traduction de *Digital Cultures*). Seuil, 2008

98. DUNCAN George T., PEARSON Robert W., "Enhancing Access to Microdata While Protesting Confidentiality: Prospects for the Future", Statistical Science, Vol. 6, No. 3, août 1991

99. EZRACHI Ariel et STUCKE Maurice, « Written Evidence (OPL0043) » in *Online Platforms and the Digital Single Market*, House of Lords, Select Committee on European Union, 10th Report on Session 2015-16, Avril 2016, https://publications.parliament.uk/pa/ld201516/ldselect/ldeucom/129/129.pdf

100. Fédération e-commerce et vente à distance, « Les chiffres clés 2019 », https://www.fevad.com/wp-content/uploads/2019/06/Chiffres-Cles-2019_BasDef-1.pdf

101. Fichiers des incidents de remboursement des crédits aux particuliers FICP, https://www.service-public.fr/particuliers/vosdroits/F17608

102. Financement Participatif France - Bilan Crowdfunding, « La finance participative 4 ans après » - 24/01/2019, https://financeparticipative.org/la-finance-participative-4-ans-apres/

103. FLECHAUX Reynald, « Espionnage de la NSA : les 8 leçons d'Edward Snowden », 7 août 2014 http://www.silicon.fr/espionnage-nsa-8-lecons-edward-snowden-96014.html

104. GAUDIAUT Tristan, "La Totalité des données créées dans le monde équivaut à...3, *World Economic Forium weforum.org*, 26 avril 2019, https://fr.weforum.org/agenda/2019/04/la-totalite-des-donnees-creees-dans-le-monde-equivaut-a/

105. GAUDIAUT Tristan, « Les pays les plus robotisés au monde », 21 novembre 2021, https://fr.statista.com/infographie/15793/industries-les-plus-automatisees-densite-robots-industriels-par-pays/

106. GDPR Expert, « Droit à l'effacement, « Droit à l'oubli » Article 17 », https://www.gdpr-expert.eu/article.html?id=17#textesofficiels

107. Georgian Government, "Statute on the Activities of and Procedure for Discharge of Powers by the Personal Data Protection Inspector", Approved by Georgian Government 19 July, 2013 # 180 Resolutions

108. Georgian Young Lawyers Association GYLA, https://gyla.ge/ge

109. Georgian Young Lawyers Association, GYLA, « Avis sur la nouvelle loi sur la protection des données personnelles» au Parlement https://gyla.ge/index.php/ge/post/saiam-parlaments-personalur-monacemta-dacvis-shesakheb-akhali-kanonis-taobaze-mosazrebebi-tsarudgina#sthash.nwSLTv5S.dpbs

110. GLASER B.C. and STRAUSS A.L., *The Discovery of Grounded Theory.* Aldine Publishing, 1967

111. Groupe de travail « Article 29 », « sur la protection des données » (organe consultatif européen), « Avis 2/2010 sur la publicité comportementale en ligne » adopté en juin 2010, https://cnpd.public.lu/content/dam/cnpd/fr/publications/groupe-art29/wp171_fr.pdf

112. Groupe de travail « Article 29 », « sur la protection des données », Avis 1/2008 sur les aspects de la protection des données liées aux moteurs de recherche »

113. Groupe de travail « Article 29 », « sur la protection des données », « Avis 4/2007 sur le concept de données à caractère personnel »,, juin 2007, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_fr.pdf

114. Groupe de travail « Article 29 », « Avis sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier des écoles) », 11 février 2009

115. HANNA Fabien, « Etude « Value Me » de Microsoft Advertising sur la valorisation des données personnelles », 20/07/2015 https://news.microsoft.com/fr-fr/2015/07/20/etude-value-de-microsoft-advertising-sur-la-valorisation-des-donnees-personnelles/

116. HASSAN Gabriel, « Comment un consultant de Trump s'est emparé de 50 millions de profils Facebook », in *Courrier International,* 18 mars 2018, https://www.courrierinternational.com/article/revelations-comment-un-consultant-de-trump-sest-empare-des-donnees-de-50-millions-de-profils

117. HENNION Romain, TOURNIER Hubert, BOURGEOIS, Eric, « Cloud computing : décider, concevoir, piloter, améliorer »*,* in *Systèmes d'information & management* 2013/1 (Volume 18), pages 124 à 125 Eyrolles, 2012

118. IDC International Data Corporation, « Analyse de future », « Future of Digital Infrastructure », https://omny.fm/shows/idc-future-enterprise/future-of-digital-infrastructure

119. IDCheck, une société d'AriadNext, « Vérification de documents », https://fr.idcheck.io/solutions/verification-documents/

120. IDFI Institute for Development of Freedom of Information of Georgia, "Georgia in the UN E-Government Survey – Review of 2020 Results", https://idfi.ge/en/e-governance-e-participation-georgia-index-2020

121. IFR, International Federation of Robotics, *Executive Summary World Robotics* 2019 Industrial Robots,
https://ifr.org/downloads/press2018/Executive%20Summary%20WR%202019%20Industrial%20Robots.pdf

122. INSERM (dir.). « Trouble des conduites chez l'enfant et l'adolescent. Rapport. », Les éditions Inserm, Paris, 2005, https://www.ipubli.inserm.fr/handle/10608/60

123. Institut CSA Consumer Science & Analitics pour Orange, « Les Français et la protection des données personnelles », études de 2014, https://csa.eu/news/les-francais-et-la-protection-des-donnees-personnelles/

124. International Labour Office Geneva, ILO, « Management of alcohol and drug related issues in the workplace », Appendix V. « Guiding principles on drug and alcohol testing in the workplace as adopted by the ILO Interregional Tripartite Experts Meeting on Drug and Alcohol Testing in the Workplace , 10-14 May 1993, Oslo (Hønefoss), Norway »

125. JORF Article R115, Modifié par Décret n°2003-303 du 27 mars 2003, art. 2, 3 avril 2003

126. Journal du droit international (Clunet), « Liberté de l'establishment », N3, 2009-07-01

127. KASPAROV Garry, « Ma défaite contre *Deep Blue* était une victoire pour l'humanité » https://www.letemps.ch/sport/garry-kasparov-defaite-contre-deep-blue-etait-une-victoire-lhumanite

128. LELOUP Damien, UNTERSINGER Martin, DUCOURTIEUX Cécile, « Les conséquences de l'invalidation de l'accord « Safe Harbor » sur les données personnelles », *Le* Monde, 6 octobre 2015

129. LIN L., NUSEIBEH, B., INCE D., JACKSON M., and MOFFETT J., "Introducing Abuse Frames for Analyzing Security Requirements," *Proc. 11th IEEE Int'l Conf. Requirements Eng*., pp. 371-372, 2003.

130. Loi n°78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés ; article 32, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/

131. Loi n° 2004-575 du 21 juin 2004 « pour la confiance dans l'économie numérique (LCEN ou LEN) », https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000017759461/

132. Loi consommation, « Entrée en vigueur de l'extension à deux ans de la garantie légale de conformité », N°1275, 21 mars 2016, http://proxy-pubminefi.diffusion.finances.gouv.fr/pub/document/18/20658.pdf

133. Loi consommation, promulguée le 17 mars 2014, publiée le 18 mars 2014 et entrée en vigueur le 19 mars 2014

134. Loi de Géorgie « sur la protection des données personnelles », №5669, 28 décembre 2011

135. Loi n° 94-665 du 4 août 1994 relative à l'emploi de la langue française, https://www.legifrance.gouv.fr/loda/id/LEGITEXT000005616341/

136. Loi Informatique et Libertés du 6 janvier 1978 « Article 69 » modifiée en annexe

137. Loi n° 2000-230 du 13 mars 2000 « portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique », https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000441676/

138. Loi n° 2004-575 du 21 juin 2004 « pour la confiance dans l'économie numérique » NOR: ECOX0200175L Version consolidée »-au 17 mars 2017

139. Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

140. Loi n° 2011-525 du 17 mai 2011 « de simplification et d'amélioration de la qualité du droit »

141. Loi nº 2014-344 du 17 mars 2014 « relative à la consommation », dite « loi Hamon »

142. Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, NOR: ECFI1524250L, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000033202746/

143. LUCAS André, DEVEZE Jean, FRAYSSINET Jean, « Droit de l'informatique et de l'internet », Presses universitaires de France, 2001

144. MARTY Frédéric, « Algorithmes de prix, intelligence artificielle et équilibres collusifs », Sciences Po - OFCE Working Paper, n°14, 2017-05-01.

145. MAY M.J., GUNTER C.A., and LEE I., "Privacy APIs: Access Control Techniques to Analyze and Verify Legal Privacy Policies," *19th IEEE Computer Security Foundations Workshop (CSFW'06)*, 2006, pp. 13 pp.-97

146. MERCIER Marie et SAVARY René-Paul, « Demain les robots : vers une transformation des emplois de service. » Rapport d'information fait au nom de la délégation sénatoriale à la prospective sur robotisation et emplois de service », n° 162 (2019-2020) - 28 novembre 2019, https://www.senat.fr/notice-rapport/2019/r19-162-notice.html

147. Ministère de l'économie, des finances et de la relance, « La Garantie légale de conformité étendue à deux ans », 23 mars 2016, https://www.economie.gouv.fr/consommation-garantie-legale-de-conformite-etendue-a-2-ans

148. Ministry of Transports and Communications of Finland, "Act on communications Administration", 25 juillet 2003, Laki viestintähallinnosta, No. 625/2001 of 29 June 2001, https://www.finlex.fi/en/laki/kaannokset/2001/en20010625_20030397.pdf

149. MONTJOYE YA., HIDALGO C., VERLEYSEN M. *et al.,* "Unique in the Crowd: The privacy bounds of human mobility". *Sci Rep* 3, 1376, 2013, https://doi.org/10.1038/srep01376

150. National Agency of Public Registry of Georgia NAPR, https://www.napr.gov.ge/udzravi

151. NUM, société d'applications CNC, https://num.com/fr/societe

152. OCDE, « Convention fiscale », Article 26

153. OCDE, « Échange automatique de renseignements : ce que recouvre l'échange automatique, son mode de fonctionnement, ses avantages et les progrès restant à accomplir », 2012

154. OCDE, « Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel », septembre 1980

155. Office of the Personal Data Protection, « Inspector, Report on the State of Personal Data Protection and Activities of the Inspector of Georgia », 2015 : https://personaldata.ge/cdn/2019/01/personal-data-protection-report-.pdf et 2018 : https://personaldata.ge/en/download/5446 et 2019 : https://personaldata.ge/en/download/6667

156. ONU, « Pacte international relatif aux droits civils et politiques », Article 16

157. Ordonnance de l'inspecteur de l'État de Géorgie « sur l'approbation du formulaire du protocole de violation administrative du bureau de l'inspecteur d'État, ses règles de stockage, d'utilisation et de comptabilité », 8 janvier 2020

158. Ordonnance de l'inspecteur d'État de Géorgie « sur l'approbation de la règle de vérification (inspection) de la légalité du traitement des données à caractère personnel » ; 2 juillet 2019

159. PWC PricewaterhouseCoopers, https://www.pwc.com/us/en/services/consulting/library/artificial-intelligence-predictions-2019.html

160. RAYMOND Jean-Luc, « DESI 2019 : Les chiffres clés du numérique en Europe et en France », in *Francenum,* Le portail de la transformation numérique des entreprises de la République française, 14/06/2019, mis à jour le 27/06/2020, https://www.francenum.gouv.fr/comprendre-le-numerique/desi-2019-les-chiffres-cles-du-numerique-en-europe-et-en-france

161. RAYNAL Juliette, « Piratage bancaire : comment 100 millions de personnes ont été touchées par un vol de données » ; la Tribune, 30/07/2019, https://www.latribune.fr/entreprises-finance/banques-finance/piratage-bancaire-comment-100-millions-de-personnes-ont-ete-touchees-par-un-vol-de-donnees-824884.html

162. REFFAY C. & TEUTSH, « Anonymisation de corpus réutilisable : masquer l'identité dans altérer l'analyse des interactions », *Environnements Informatiques pour l'Apprentissage Humain,* Lausanne Suisse, juin 2007, https://edutice.archives-ouvertes.fr/docs/00/15/88/77/DOC/Reffay_Teutsch.doc

163. REFFAY C., BLONDEL F.M, GIGUET EM, « Stratégies pour l'anonymisation systématique d'un corpus d'interactions plurilingues » ; Degache, C. & Garbarino, S. (Ed.) (2012). Actes du colloque IC2012. Intercompréhension : compétences plurielles, corpus, intégration. Université Stendhal Grenoble 3 (France), 21-22-23 juin 2012, https://edutice.archives-ouvertes.fr/edutice-00718390/document

164. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, Article 26 de la directive en annexe 1 relatif à « la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données », et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

165. REYNDERS Didier and U.S. Secretary of Commerce Wilbur Ross, "Joint Press Statement from European Commissioner for Justice", 10/08/2020

166. RGPD, Le règlement général sur la protection des données, 23 mai 2018

167. RGPD, « Obligation de notification concernant la rectification, l'effacement de données ou limitation du traitement, article 15 (amendement 114) »

168. ROLLAND Sylvain, « Données personnelles : Les Citoyens sont désarmés face aux géants du Net » *La Tribune,* 29 octobre 2015, https://www.latribune.fr/technos-medias/internet/donnees-personnelles-les-citoyens-sont-desarmes-face-aux-geants-du-net-516884.html

169. ROUVROY Antoinette et BERNS Th., « Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ? In *Réseaux* 2013/1 (n° 177), pages 163 à 196, https://www.cairn.info/revue-reseaux-2013-1-page-163.htm

170. ROUVROY Antoinette, « Des données et des hommes. Droits et libertés fondamentaux dans un monde de données massives », Centre de recherche information, droit et société, Conseil de l'Europe, Strasbourg, le 11 janvier 2016

171. SAMARATI P., DE VIMERCATI S.C. (2001) « Access Control: Policies, Models, and Mechanisms ». In: Focardi R., Gorrieri R. (eds), *Foundations of Security Analysis and Design. FOSAD 2000. Lecture Notes in Computer Science,* vol 2171. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45608-2_3

172. valeurs par des valeurs plus générales P., « Protecting respondents' identities in microdata release", *IEEE Transactions on Knowledge and Data Engineering*, vol. 13, n° 6, 2001

173. SCHMID Matthias, SCHNEEWEISS Hans, KUCHENHOFF Helmut, "Statistical Inference in a Simple Linear Model Under Microaggregation", Department of Statistics, University of Munich, Munchen, Germany

174. Sénat, session ordinaire N° 589 2013-2014, Ordonnance n° 2005-650 du 6 juin 2005 relative à « la liberté d'accès aux documents administratifs et à la réutilisation des informations publique »

175. Sénat, Ordonnance, n° 2016-131 du 10 février 2016 « portant réforme du droit des contrats, du régime général et de la preuve des obligations » Art. 1102

176. Service Public, « Vente à distance : droit de rétractation du consommateur », https://www.service-public.fr/particuliers/vosdroits/F10485

177. State Inspector's Service, Géorgie, https://personaldata.ge/en/about-us

178. State Inspector's Service, « Report on the Activities of the State Inspector's Service », with the assistance of the Norwegian Government, the United Nations Development Program (UNDP) and the Office of the High Commissioner for Human Rights (OHCHR), 2019, https://personaldata.ge/cdn/2020/10/Report-on-the-activities-of-the-State-Inspectors-Service-2019.pdf

179. Tax Justice Network, taxjustis.net, « Le reporting pays par pays : Comment favoriser la transparence des sociétés multinationales? », https://www.taxjustice.net/cms/upload/pdf/TJN_0806_Country_by_Country_-_Franais_.pdf

180. THERY Jean-François, FALQUE-PIERROTIN Isabelle, « Internet et les réseaux numériques », étude adoptée par l'Assemblée générale du Conseil d'État, 2 juillet 1998, https://www.vie-publique.fr/rapport/24331-internet-et-les-reseaux-numeriques-etude-adoptee-par-lassemblee-gener

181. THOMPSON Simon G., DSc, NIXON Richard M., „How Sensitive Are Cost-Effectiveness Analyses to Choice of Parametric Distributions?" *Medical Decision Making* vol. 25, 4: pp. 416-423. , 1 Juillet 2005

182. THOMSON Judi, HETZLER Elizabeth, MacEACHREN Alan, GAHEGAN Mark, PAVEM Misha, "A typology for visualizing uncertainty," Proc. SPIE 5669, Visualization and Data Analysis 2005, 11 March 2005

183. THOUVENIN D., « Les Banques de tissus et d'organes : les mots pour les dire, les règles pour les organiser », *Les Petites Affiches*, numéro spécial relatif à la révision des lois bioéthiques, 18 février 2005, N 35

184. TNS Sofres, « Comment partager sans se sur-exposer ? La place des photos dans la vie numérique », Conférence de presse 12 décembre 2012, https://www.cnil.fr/sites/default/files/typo/document/Etude_2012_place_des_photos_dans_la_vie_numerique.pdf

185. *La Tribune,* « Droit à l'oubli : la Cnil dit non au recours de Google », 21/09/2015

186. TRUC Olivier, « La Finlande va autoriser les entreprises à surveiller les courriels de leurs salarié », *Le Monde*, 5 février 2009

187. UNESCO Organisation des Nations Unies pour l'éducation, la science et la culture, « de la culture pour le développement », Indicateurs publié en 2014

188. UNTERSINGER Martin et LELOUP Damien, « Hollande et le PS s'en prennent de nouveau à « l'anonymat sur Internet » », *Le Monde.fr,* 17.12.2013

189. UNTERSINGER et BELOUEZZANE Sarah, « Le gouvernement présente sa stratégie numérique pour la France », *Le Monde,* 18 juin 2015

190. YEUNG Karen, Rapporteuse pour le Conseil de l'Europe : « Étude sur les incidences des technologies numériques avancées (dont l'intelligence artificielle) sur la notion de responsabilité, sous l'angle des droits humains », https://rm.coe.int/etude-sur-les-incidences-des-technologies-numeriques-avancees-dont-l-i/168096bdac

191. ZAVE P. and JACKSON M., "The Four Dark Corner's of Requirements Engineering," *ACM Trans. Software Eng. Methods*, vol. 6, http://www.cse.msu.edu/~chengb/RE-491/Papers/dark-corners-re-zave-jackson.pdf