Le droit face aux technologies disruptives : le cas de la blockchain

Thibaut Labbé

▶ **To cite this version:**

Thibaut Labbé. Le droit face aux technologies disruptives : le cas de la blockchain. Droit. Université de strasbourg; CEIPI, 2021. Français. NNT : . tel-03518287

HAL Id: tel-03518287
https://theses.hal.science/tel-03518287

Submitted on 9 Jan 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.

Distributed under a Creative Commons Attribution - NonCommercial 4.0 International License

UNIVERSITÉ DE STRASBOURG

ÉCOLE DOCTORALE 101

Centre d'Études Internationales de la Propriété Intellectuelle [CEIPI]

THÈSE présentée par :

Thibaut LABBÉ

soutenue le : **14 décembre 2021**

pour obtenir le grade de : **Docteur de l'université de Strasbourg**

Discipline / Spécialité : Droit privé

Le droit face aux technologies disruptives : le cas de la *blockchain*

THÈSE dirigée par :
M. MACREZ Franck Maître de Conférences, HDR, Université de Strasbourg

RAPPORTEURS :
Mme LE GOFFIC Caroline Professeure, Université de Lille
Mme FAVREAU Amélie Maître de Conférences, HDR, Université de Grenoble

---

AUTRES MEMBRES DU JURY :
Mme FAVRO Karine Professeure, Université de Haute Alsace

L'Université de Strasbourg n'entend donner aucune approbation, ni improbation aux opinions émises dans cette thèse. Ces opinions doivent être considérées comme propres à leurs auteurs.

À Camille,

Pour tout, et à jamais,

À Éléanore,

Pour tout, et pour toujours,

Remerciements

La rédaction de cette thèse s'apparentait à un aboutissement intellectuel. Il s'agissait d'appréhender, construire et répondre à des problématiques nouvelles, présentant des intérêts personnels et professionnels.
Mais personne n'est capable de décrire de manière exhaustive tout ce que cela peut impliquer. C'est, pour moi, l'un des buts de ces remerciements. Remercier toutes ces personnes qui ont pu m'aider, m'aiguiller, me soutenir, me secouer, m'encourager, ou ceux qui ont pu simplement être là, dans la myriade des implications que de tels travaux ont. Pouvoir témoigner de l'aventure fantastique que constitue un tel projet.

La confiance dans la rédaction de tels travaux est indispensable, et pour me l'avoir accordée en tant que directeur de thèse, et tout au long de mes travaux, M. Franck Macrez, directeur du centre de recherche du CEIPI, ne sera jamais assez remercié.

Enfin, une telle aventure ne serait être possible sans un accompagnement particulier, et c'est pourquoi je suis reconnaissant de pouvoir dire :

Aux membres de mes différents comités de thèse, pour leur disponibilité et leurs remarques toujours constructives,

À mes amis proches, la *Cigogne Squad*, pour ces rires, ces amitiés, ces moments et tous ceux qui suivront,

À tous ces auteurs, que j'ai pu lire,

À tous ceux qui m'ont relu, et à ceux qui me liront,

Merci.

Sommaire

INTRODUCTION

PREMIÈRE PARTIE : LE CONSTAT D'UNE APPROCHE DÉSORDONNÉE

TITRE 1 : UN ÉCLATEMENT DU CADRE JURIDIQUE APPLICABLE

Chapitre 1 : Approches économiques et juridiques anarchiques

Chapitre 2 : Transformations techniques subies des rapports civils

TITRE 2 : UNE EMERGENCE PERTURBEE D'UN NOUVEAU MODELE DE GOUVERNANCE

Chapitre 1 : Des lacunes étatiques sur la gouvernementabilité des données

Chapitre 2 : Au profit des stimulations de la gouvernance privée des données

SECONDE PARTIE : POUR UNE APPLICATION ORDONNÉE

TITRE 1 : D'UNE APPLICATION SEMANTIQUE DES REGIMES DE PROPRIETE LITTERAIRE ET ARTISTIQUES

Chapitre 1 : L'adéquation de la protection du logiciel pour la blockchain

Chapitre 2 : La concordante protection de la blockchain par le droit des bases de données

TITRE 2 : VERS UNE APPRECIATION FONCTIONNELLE DU DROIT DE LA DONNEE

Chapitre 1 : Dualisme d'une approche protectionniste de la donnée

Chapitre 2 : Complémentarité naturelle entre droit et technique

CONCLUSION GENERALE

Liste des principales abréviations utilisées

Aff.	Affaire
ADAN	Association de Développement des Actifs Numériques
AG	Assemblée générale
Al.	Alinéa
AJD	Actualité juridique Dalloz
AN	Assemblée Nationale
Ann.	Annexe
ANSSI	Agence nationale de la sécurité des systèmes d'information
Ass. Plén.	Assemblée plénière
BLD	Bulletin législatif Dalloz (ALD à partir de 1983)
BRDA	Bulletin Rapide Droit des Affaires
CA	Cour d'appel
CADA	Commission d'accès aux documents administratifs
Cass.	Cour de cassation
Cass. ass. plén.	Arrêt de l'assemblée plénière de la Cour de cassation
Cass. ass. mixte	Arrêt de la chambre mixte de la Cour de cassation
Cass. ass. réun.	Arrêt des chambres réunies de la Cour de cassation
CC	Conseil Constitutionnel
CCC	Contrats, concurrence, consommation
C. Civ.	Code civil
C. com.	Code de commerce
C. consomm.	Code de la consommation
C. pén.	Code pénal
CE	Conseil d'état
CEDH	Convention européenne des droits de l'homme
Cf.	Conférer, consulter
CGI	Code général des impôts
Cir.	Circulaire
Civ.	Cassation, chambre civile
CNIL	Commission Nationale de l'Informatique et des Libertés
CNNum	Conseil national du numérique
CPI	Code de propriété intellectuelle
Crim.	Cassation, chambre criminelle
D	Dalloz, recueil Dalloz-Sirey
Délib.	Délibération
DGCCRF	Direction générale de la concurrence, de la consommation et de la répression des fraudes
Ibid.	Au même endroit
INPI	Institut national de la propriété intellectuelle
J.Cl.	JurisClasseur (civil, pénal, etc.)
JCP	Semaine juridique (JurisClasseur périodique : générale, entreprises, etc.)
LCEN	Loi pour la confiance dans l'économique numérique
LGDJ	Librairie générale de droit et de jurisprudence
LIL	Loi Informatique et Libertés
LINC	Laboratoire d'Innovation Numérique de la CNIL
NTIC	Nouvelles technologies de l'information et de la communication
OCDE	Organisation de coopération et de développement économiques
OMPI	Organisation mondiale de la propriété intellectuelle
PLA	Propriété littéraire et artistique
PME	Petites et moyennes entreprises
POC	*Proof of Concept*
Prop.	Proposition
PUF	Presses Universitaires de France
Rapp.	Rapport (ou rapporteur)
RCS	Registre du commerce et des sociétés

RDA	Revue droit des affaires
RD bancaire et bourse	Revue de droit bancaire et de la bourse
RDC	Revue des contrats
Règl.	Règlement
RFPI	Revue Francophone de la propriété intellectuelle
RGPD	Règlement Général sur la Protection des Données personnelles
RGNP	Règlement Générale sur la protection des données Non Personnelles
RIDA	Revue internationale du droit d'auteur
RLDA	Revue Lamy Droit des affaires
RLDI	Revue Lamy Droit de l'immatériel
RPI	Revue de propriété intellectuelle
RPPI	Revue pratique de la prospective et de l'innovation
RTD Civ.	Revue trimestrielle de droit civil
RTD Com.	Revue trimestrielle de droit commercial
S.	Suivant
SAFARI	Système automatisé pour les fichiers administrateurs et le répertoire des individus
SS.	Suivants
TIC	Technologies de l'information et de la communication
TGI	Tribunal de Grande Instance
TPE	Très petites entreprises

Introduction

« *Les nouvelles technologies deviennent rapidement si omniprésentes qu'il est parfois difficile de se souvenir à quoi les choses ressemblaient avant leur arrivée*. »

Celui qui pourrait changer le monde, 2017, Aaron Swartz (1986-2013)

1. En quelques années, et depuis une première démocratisation dans un article paru dans la revue The Economist[1], la *blockchain*[2] ou technologie des chaînes de blocs ou encore dispositif d'enregistrement partagé[3] a suscité un engouement aussi bien au sein des secteurs financiers ou plus largement technologiques, mais aussi juridiques. Le caractère disruptif, souvent mis en avant de cette technologie, bien que connue depuis 2008[4], est un adjectif qui « se dit d'une entreprise, d'un produit, d'un concept, etc., qui créent une véritable rupture au sein d'un secteur d'activité en renouvelant radicalement son fonctionnement[5] ». Mot-clé ou effet « *buzzword* », le caractère disruptif d'une technologie provient pourtant d'une réalité « dans laquelle de nouveaux entrants sont en mesure de concurrencer progressivement des acteurs établis en proposant de nouveaux types de services et en s'appuyant, le plus souvent, sur une technologie nouvelle[6] ». Caractérisée ainsi, le terme de disruptif est utilisé majoritairement dans le milieu des technologies de l'information et de la communication, ce dit caractère disruptif régulièrement mis en avant, notamment pour favoriser un engouement d'intérêt, de manière légitime, ou non.

---

[1] The Economist, *The promise of the blockchain : the trust machine, 31 oct. 2015,* Disponible à : https://www.economist.com/leaders/2015/10/31/the-trust-machine

[2] Par commodité de langage, au sein de cette étude, les termes « *blockchain* », « protocole *blockchain* », « chaîne de bloc » ou « dispositif d'enregistrement partagé » pourront servir de manière homologue

[3] Ordonnance n° 2016-520 du 28 avril 2016 relative aux bons de caisse

[4] La technologie *blockchain* est la technologie servant de base à la monnaie virtuelle Bitcoin, NAKAMOTO S. « Bitcoin : A Peer-to-Peer Electronic Cash System », 2008, disponible à https://bitcoin.org/bitcoin.pdf ; est la personne, ou le collectif de personnes, ayant donné naissance au bitcoin. L'hésitation entre les deux termes précédents venant de l'incertitude, encore actuelle, sur la paternité de ce concept.

[5] Larousse. (s.d.). Disruptif. dans LAROUSSE *en ligne*, https://www.larousse.fr/dictionnaires/francais/disruptif/25982

[6] SMATT PINELLIET S., DAMELETET L., SOMONONT M., PAILLAT R., *Conférence annuelle de l'Incubateur du barreau de Paris*, La Semaine Juridique Edition Générale n° 49, 5 déc. 2016, p.1333

Ce caractère de la *blockchain* se démontre aujourd'hui empiriquement, et dans une première approche, à travers le secteur financier. La *blockchain* se veut être une technologie dont la mise en application simplifie l'ensemble d'opérations financières, sans intervention d'un tiers validateur (ou certificateur, ou encore de confiance), résolvant le problème de la double dépense[7], apparaissant donc aujourd'hui comme disruptive, par rapport aux systèmes actuels pyramidaux, imposant l'intervention d'un tel tiers (une banque le plus généralement) pour effectuer des opérations de crédit ou de débit.

2. L'intérêt de l'étude du caractère disruptif d'une technologie emporte un certain paradoxe dans le cadre des nouvelles technologies, qui sont, *de facto*, toujours nouvelles. Le champ temporel de l'étude d'une technologie novatrice est, par nature, restreint ; il serait, par exemple, saugrenu d'étudier Internet au prisme des nouvelles technologies, tant son étendue et son utilisation quotidienne font que cette technologie de mise en réseau est devenue quelconque dans les temps actuels. Néanmoins, le laps de temps, pendant lequel une technologie reste « nouvelle » emporte tout intérêt ; au-delà du simple intérêt intellectuel de pouvoir analyser l'ensemble des tenants et aboutissants d'une technologie dont la mise sur le marché entraîne moult réactions multisectorielles, les réactions du droit positif à un instant « T » ou celles anticipées à moyen et long terme, que ce soit à travers un appareil répressif ou un cadre de régulation nous amène à percevoir et appréhender les réponses juridiques positives ou négatives à cette même technologie. Surtout, il est d'autant plus stimulant d'étudier la construction d'une telle réponse, compte tenu de la différence de temporalité que l'on peut trouver entre une technologie et son encadrement légal potentiel.

3. Il est de l'apanage du juriste, peu importe sa spécialisation ou ses affects, de continuellement se questionner sur ces nouveaux objets, comme le rappelle le professeur Supiot : « Le droit occupe quant à lui une position à mi-chemin entre l'art et la technique. Sa référence ultime n'est ni la vérité, ni l'esthétique, mais la justice[8] », et c'est cette recherche de justice que le juriste s'efforce de réaliser à chaque apparition d'un nouvel objet juridiquement non identifié[9].

[7] La problématique de la double dépense sera exposée ultérieurement dans le cadre de cette étude.
[8] SUPIOT A., *La gouvernance par les nombres* (Essais), Fayard, 18 mars 2015, p.2
[9] ROUSSILLE M., *Le Bitcoin : objet juridique non identifié,* Revue Banque & Droit, n°159, janv.-fév. 2015

4. L'intérêt premier de la présente étude est de participer à au questionnement de savoir si le droit positif est capable, aujourd'hui, et donc dans une appréciation temporelle immédiate, d'appréhender les utilisations et les conséquences d'une technologie[10], pris en sa nature la plus littéraire, en ce qu'elle est l'application de formules mathématiques ou de concepts informatiques.

Un second attrait, intrinsèquement lié au premier, est l'occasion, pour le juriste, pris dans sa définition la plus simple[11], de dépasser ses matières universitaires d'exercice, et ainsi de percevoir si le juriste - d'aujourd'hui - est capable de se saisir d'objets qui sortent de ses prérogatives classiques tenant à l'analyse du seul Droit. Pour porter cet attrait plus loin, il s'agit en réalité de savoir si le juriste - de demain - a intérêt à devenir disruptif lui aussi. À ce titre, il a déjà été mis en avant que la compréhension et une nécessaire pédagogie sont indispensables à ce type d'étude[12], poussant, une nouvelle fois, le monde du juridique à étendre ses préceptes et surtout ses domaines classiques de connaissances.

5. Ainsi, avant même de savoir comment réguler les usages d'une technologie - ou une technologie - il ne faut pas omettre une question première : « doit-on réguler » ? Une étude sur l'appréciation d'une technologie par le droit, qu'elle soit au bénéfice ou non d'une régulation, ne peut passer outre différentes définitions techniques, tant le conditionnement de l'application d'une quelconque norme ne peut se faire de manière efficiente sans la compréhension de l'objet auquel elle s'applique. C'est pourquoi dans le cadre de la présente introduction, un volet important sera consacré aux définitions techniques (A), mais aussi à une première définition juridique, permise par l'introduction de *blockchain* dans notre droit positif, avec l'introduction de la notion de dispositif d'enregistrement partagé (B).

[10] Larousse. (s.d.). Technologie. dans LAROUSSE *en ligne*, https://www.larousse.fr/dictionnaires/francais/technologie/76961, consulté le 10/06/2017

[11] Larousse. (s.d.). Juriste. Dans LAROUSSE *en* ligne, https://www.larousse.fr/dictionnaires/francais/juriste/45215, consulté le 10/06/2017

[12] MIS J.-M., *Les technologies de rupture à l'aune du droit*, Dalloz IP/IT 2019, p.425

A. Définitions techniques

1. Concept général : présentations

6. Il convient également de faire un point linguistique sur le terme de *blockchain*, afin d'éviter toute confusion dans la suite de la présente étude. D'une part, quand on parle de « la » *blockchain*, on fait référence à la technologie même, la méthode technique permettant le stockage et la transmission d'informations, fonctionnant sans administrateur central qui en contrôle l'ensemble[13] ; il est même recommandé d'utiliser la notion de protocole *blockchain*, au sens de la définition d'un protocole informatique[14]. D'autre part, on utilise le terme « une » *blockchain*, pour faire référence à une application de cette technologie, liée à un usage particulier (par exemple *Bitcoin* est la *blockchain* sur laquelle est basée la crypto-monnaie *Bitcoin* - BTC-).

7. Comprendre la technologie *blockchain* peut faire appel à des connaissances à la fois informatiques, mathématiques, et même, dans une certaine mesure, philosophiques. L'usage d'une métaphore peut aider à sa compréhension. Un nombre fini[15] d'élèves se trouvent dans une pièce, scindée en autant de bureaux, ayant une vision sur un panier de pommes. Chacun des élèves peut voir le panier, mais jamais de manière complète (seul l'ensemble des visions des élèves présents permettrait d'avoir un dénombrement adéquat) mais ils ne peuvent interagir directement entre eux, et restent cloisonnés de manière individuelle. Ainsi, ils ne possèdent chacun qu'une partie de l'information finale à retrouver et doivent parvenir à déterminer le nombre de pommes exact. Ils peuvent toutefois communiquer entre eux, mais l'épaisseur des cloisons fait que l'information met toujours un certain temps à leur parvenir[16]. Répartis en autant de bureaux que le nombre qu'ils sont, ils ne peuvent se réunir, et encore moins avoir une personne de confiance qui relayerait entre eux une information fiable. Parmi ces élèves se trouvent certains « cancres », qui ne souhaitent pas que le nombre de pommes

---

[13] CAPRIOLI E., *La blockchain ou la confiance dans une technologie*, La Semaine Juridique, édition générale, n°23, 6 juin 2016, p.672

[14] Un protocole informatique (ou parfois tout simplement un protocole quand le contexte de l'informatique est clair) est un ensemble de règles qui régissent les échanges de données ou le comportement collectif de processus ou d'ordinateurs en réseaux ou d'objets connectés. Un protocole a pour but de réaliser une ou plusieurs tâches concourant à un fonctionnement harmonieux d'une entité générale. https://fr.wikipedia.org/wiki/Protocole_informatique (consulté le 15/07/2017)

[15] Un nombre fini ou ensemble fini est un ensemble possédant un nombre fini d'éléments, c'est à dire qu'il est possible de compter ses éléments. Le résultat étant un nombre entier.

[16] À ce titre, on peut parler d'information asynchrone, ou décalée.

soit révélé. Ils vont donc omettre des informations, en donner des erronées, ou même garder le silence.

Ils ont comme défi de donner le nombre exact de pommes présentes dans le panier. La difficulté de cette situation est donc la suivante : comment, de par une multitude d'informations possibles, fiables ou non, les élèves pourront décider, de concert, du nombre exact de pommes dans le panier ?

8. C'est ici que les mathématiques revêtent une importance ; car en réalité, un algorithme[17] permet de répondre à cet objectif (la détermination du nombre de pommes), tout en prenant compte les potentielles erreurs (les élèvent ne souhaitant pas que le nombre de pommes soit révélé).

Cet algorithme a été conçu par l'informaticien Leslie Lamport[18], et trouve application dans le milieu informatique. C'est là l'esprit de la technologie *blockchain* : l'utilisation d'un consensus entre des acteurs fiables et d'autres qui peuvent se trouver défaillants afin de permettre une prise de décision. D'un point de vue strictement mathématique et algorithmique, la technologie *blockchain* consiste en la création, l'alimentation et la gestion d'une base de données particulièrement singulière, dont l'architecture repose fondamentalement sur un arbre de Merkle[19], c'est-à-dire une continuité de fichiers informatiques ayant fait l'objet d'une technique de chiffrement, dite de hachage[20], afin de condenser l'information brute dans un format prédéfini, dont les chiffrements successifs permettent un suivi et une traçabilité de l'information.

---

[17] Algorithme : Ensemble de règles opératoires dont l'application permet de résoudre un problème énoncé au moyen d'un nombre fini d'opérations. Un algorithme peut être traduit, grâce à un langage de programmation, en un programme exécutable par un ordinateur. Larousse. (s.d.). Algorithme. dans LAROUSSE *en ligne*, https://www.larousse.fr/dictionnaires/francais/algorithme/2238. Une autre définition de l'algorithme existe : « l'étude de la résolution de problèmes par la mise en œuvre de suites d'opérations élémentaires selon un processus défini aboutissant à une solution » (arrêté du 27 juin 1989 pour l'enrichissement du vocabulaire informatique, JO 16 sept. 1989, p.11725

[18] LAMPORT L., SHOSTAK R. et PEASE M., *The Byzantine Generals Problem*, ACM Transactions on Programming Languages and Systems, vol. 4, no 3, juil. 1982

[19] Un arbre de Merkle, ou arbre de hachage, inventé par Ralph Merkle en 1979.

[20] Cf. *Infra*, p.212

9. La technologie *blockchain* est un protocole de gestion numérique de données, décentralisé[21], infalsifiable[22] et fondée sur les échanges « pairs à pairs [23]» dans des réseaux[24], reposant, le plus souvent sur un logiciel open-source/libre[25], (soit un logiciel mis gratuitement à disposition par leurs auteurs, mais sous certaines conditions[26]), chacun des participants à un tel protocole est désigné être un « nœud ». De manière simplifiée, un réseau utilisant un protocole *blockchain* est constitué d'autant de nœuds, reliés ensemble par un réseau maillé, dont les données exploitées sont répliquées et sauvegardés par chacun d'entre eux.

De manière synthétique, cette technologie utilise des outils de cryptographie asymétrique, une technologie de chiffrement[27]. Lorsqu'une transaction est réalisée au sein d'une *blockchain*, ses conditions de réalisation sont vérifiées par l'ensemble des serveurs connectés (aussi appelés nœuds), et en cas de succès dans la vérification de l'opération, cette dernière est horodatée, puis ajoutée au sein d'un « bloc », mis à la chaîne d'autres, partagés

[21] Par opposition à une architecture centralisée, dans laquelle les données sont stockées sur un ou plusieurs serveurs centraux, détenus par les fournisseurs de services, ne pouvant être modifiées par leurs utilisateurs ou usagers. MÉADEL A., MUSIANI F., *Abécédaire des architectures distribuées*, Presse des Mines, 2015

[22] Ou plutôt réputée infalsifiable. Il s'agit ici d'une commodité de langage ; si l'emploi de ce terme sera répété dans le cadre de cette étude, il convient de préciser que tout système informatique ne peut être garanti à 100%. La *blockchain*, en ce qu'elle repose notamment sur des procédés cryptographiques, ne peut être considéré comme étant inviolable perpétuellement. cf. CAPRIOLI E., *Mythes et légendes de la blockchain face à la pratique*, Dalloz IP/IT 2019, p.429

[23] Réseau décentralisé « pairs à pairs » ou P2P ou « peer-to-peer » fait référence à un réseau d'égaux, ou de pairs, qui, à l'aide de systèmes de communication et d'échanges appropriés, permet à deux ou plusieurs individus de collaborer spontanément, sans nécessairement avoir besoin d'une coordination centrale. DE FILIPPI P., contribution n°4, *Abécédaire des architectures décentralisées*, Presses des Mines 2015

[24] DE ROSNAY J., *La blockchain décryptée - les clefs d'une révolution*, Préface, Netexplo, juin 2016

[25] BERTRAND A-R. *Dalloz action, Droit d'auteur* - Chapitre 202 – *Logiciels* – 2010, § 2 - Logiciels « libres », 202.90. Définition

[26] BAUGRAND T., *Le copyleft et la licence « art libre »*, Mémoire Master Paris II (juin 2002), 80 p. accessible sur www.m2-dmi.com

[27] Cf. *Infra*, p.203 et suiv.

entre les différents serveurs participant à la *blockchain* ; intégrant ainsi cette transaction de manière chronologique et infalsifiable[28] dans un registre[29] immuable.

Ce caractère infalsifiable découle de son fonctionnement ; chaque transaction effectuée sous couvert d'un protocole *blockchain* est vérifiée par l'ensemble des participants du réseau, puis horodatée pour être ensuite partagée entre ces mêmes participants au sein de la base de données partagée entre eux. Cette transaction sera implantée dans un bloc, qui viendra à la suite des autres déjà enregistrés (d'où l'appellation *blockchain* ou « chaîne de blocs »).

10. Pour revenir à notre exemple précédemment illustré, la problématique portant sur la détermination du nombre de pommes pourra être la suivante (de manière simplifiée, et n'utilisant pas d'application algorithmique précise) :

- Chaque élève (même ceux ne souhaitant pas que le nombre de pommes soit révélé) parmi le nombre fini initial va proposer une solution (« il y a N pommes ») ;

- Chacune de ses solutions va être soumise à l'approbation de l'ensemble des élèves, qui vont, dans l'ensemble admettre ou non la solution proposée par chacun d'eux ;

- Chacune des solutions va être comptabilisé et inscrite dans un registre, accessible à l'ensemble des élèves ;

- Par un vote, cette communauté va déterminer le nombre de pommes à la majorité. Si toutes les réponses comptabilisées par les élèves vont être enregistrées, seules celles réputées comme fiables vont être appliquées ;

---

[28] Infalsifiable : en effet, du fait du caractère de technologie de consensus de la *blockchain*, il faudrait pouvoir réunir une puissance de calcul supérieure à la moitié de la puissance de la majorité des serveurs participant à la *blockchain* pour pouvoir en prendre le contrôle et ainsi la modifier. De plus, chaque transaction étant horodatée et implantée dans un bloc, la modification d'un bloc peut mettre en péril la totalité de la chaîne de blocs. Dès lors, toute modification a posteriori d'une *blockchain* aura pour conséquence, d'une part, de laisser une trace partagée sur l'ensemble des serveurs connectés, et d'autre part, potentiellement provoquer une défaillance de l'ensemble de la *blockchain*.

[29] CORNU G., *Vocabulaire juridique*, PUF, collec. Quadrige, 8e éd., 2007 ; Registre : livre constituant un instrument de preuve ou de publicité, parfois doté d'une valeur constitutive, sur lequel on note des informations d'un type qui le caractérise et sert généralement à le dénommer et dont la tenue incombe parfois à un service officiel, parfois au principal intéressé.

- En conséquence, le nombre de pommes sera déterminé par la collectivité et sera réputé fiable car ayant emportée l'adhésion majoritaire.

11. En réalité, cette métaphore entraîne la nécessité d'expliciter une problématique propre à la *blockchain*, sorte d'expression informatique de l'abus de majorité, à savoir « l'attaque des 51%%[30] » (ou attaque « *Goldfinger* »). La presse spécialisée sur la question y voit le défaut de la technologie *blockchain*, à savoir que, et l'exemple précédent peut servir à le démontrer, si une majorité des nœuds devient malveillante, ou si la majorité de ces nœuds n'appartient qu'à un seul opérateur, alors ce dernier, possédant la majorité des nœuds de validations est réputé « contrôler » la *blockchain* mise en place. Pour en faire une application à notre exemple, si la majorité des élèves sont des élèves malveillants, alors le résultat voté par la communauté sera également malveillant. En réalité, l'attaque des 51% repose sur une hypothèse technique et surtout sur une réalité technique bien plus complexe à atteindre[31]. En effet, il faut prendre en compte qu'une « attaque des 51% » sera une attaque visée vers une *blockchain* existante. Or, la robustesse technique d'une *blockchain* porte avant tout sur la collectivité des mineurs, et donc la taille du réseau ainsi mis en place. Prenons l'exemple suivant, basé sur un protocole *blockchain* de faible envergure :

- Une *blockchain* instituée entre 100 nœuds, soit 100 ordinateurs, d'une valeur de 1000 euros ; avec chacun une puissance de calcul propre (considéré comme équivalentes dans le cadre de cet exemple), associé à leur consommation électrique propre (pour l'exemple, une consommation fictive de 10Mws[32]) ;

- Une opération de minage, et donc de validation d'un seul bloc, prenant une (1) heure, par nœud, soit 600*100 (=60000)[33] ;

- Une *blockchain* ayant déjà validé 100 blocs[34] ;

[30] https://fr.wikipedia.org/wiki/Attaque_des_51_%25 (consulté le 20/07/2017)

[31] DELAHAYE J.-P., *L'attaque Goldfinger d'une blockchain*, SCILOGS.fr, 13 janv. 2015, disponible à : http://www.scilogs.fr/complexites/lattaque-goldfinder-dune-*blockchain*/,(consulté le 20/07/2017)

[32] Soit 600Mwh (mega-watt-heure) ; sachant que - au moment de la rédaction de cette étude, 1Mgh = 0,014€.

[33] Soit 60000*0,014= 8400 euros.

[34] Dès lors, la consommation électrique de cette chaîne est, en cumulé, équivalente à 840 000 euros.

Ainsi, pour effectuer une attaque des 51%, il faudra au « pirate », une puissance d'au moins 76 ordinateurs (pour pouvoir représenter à lui seul 51% des nœuds), et réinscrire la totalité des blocs de la chaîne pour en altérer l'historique, soit 100 blocs. Si, dans cette hypothèse, le pirate arrive à prendre le contrôle de la chaîne en une heure, il lui faudra :

- Réinscrire 101 blocs ;

- Maintenir les opérations réalisées par ses nœuds le temps de l'accomplissement de son forfait ;

- Au total, il lui faudra donc 76 ordinateurs, et s'acquitter des frais électriques correspondants, donc une somme avoisinant les 64 millions d'euros[35].

Cela rend ainsi cette opération de piratage extrêmement moins rentable. Il a été estimé, en 2018, que pour réaliser « une attaque des 51% » de la *blockchain Bitcoin*, un coût d'un milliard d'euros pour le matériel et près de 475 000 euros d'électricité par heure de fonctionnement pour être réalisable[36]. À ce sujet, il conviendra également de mentionner, sans pour autant en faire une étude complète - qui serait hors de propos dans cette étude - que la consommation électrique autour des cryptoactifs, et donc de la *blockchain* en tant que telle, peut être notamment réduite par l'emploi de différents protocoles ou autres choix techniques[37].

12. Cette effervescence autour de cette technologie s'explique par les différentes applications qu'elle peut revêtir. Et afin d'être le plus précis possible, il est incomplet de parler que d'un seul type de *blockchain*. Ces précisions emporteront d'ailleurs sens où les différents régimes ou projections juridiques qui pourront être faites autour de la *blockchain* découleront nécessairement de ces typologies d'usages.

---

[35] De manière arrondie, pour le coût des ordinateurs, de la réinscription de 101 blocs avec la consommation énergétique correspondante.

[36] Pour une information sur la consommation électrique du Bitcoin : https://digiconomist.net/bitcoin-energy-consumption (consulté le 25/07/2017)

[37] GRIFFIN A., *Ethereum to change technology underpinning its cryptocurrency to dramatically cut its energy use*, Independent.co.uk, 21 mai 2021, disponible à : https://www.independent.co.uk/climate-change/ethereum-crypto-bitcoin-*blockchain*-energy-b1851004.html, consulté le 27/07/2021

2. Typologies de blockchains

13. La technologie *blockchain* repose sur la mise en place d'une architecture décentralisée[38]. Ainsi, au lieu d'avoir un organe central qui possède à lui seul des documents dont il distribue copie aux clients, chaque ordinateur possède lui-même les fichiers d'un groupe[39].

14. Cette décentralisation[40] apporte trois intérêts majeurs : un renforcement de la sécurité du système (une défaillance d'un organe central pouvant déstructurer tout un réseau, un système géré par *blockchain* nécessite la mise en défaillance d'au moins la moitié de ses organes) ; la suppression de toute activité d'intermédiaire (par exemple, dans une relation contractuelle comprenant une obligation de payer une somme d'argent, le paiement de A vers B on nécessite l'intervention d'un tiers, C, généralement une banque, qui va permettre la transition des fonds ; dans le cadre d'un protocole *blockchain*, le paiement peut être automatiquement validé par l'ensemble des participants à ladite *blockchain*) ; l'authenticité

[38] La notion d'architecture décentralisée, distribuée, répartie, en P2P renvoie à une forme d'organisation particulière : un réseau d'égaux ou de pairs qui, à l'aide de systèmes de communication et d'échanges appropriés, permet à deux ou plusieurs individus de collaborer spontanément, sans nécessairement avoir besoin d'une coordination centrale (SCHODER & FISCHBACH, 2003 ; SCHOLLMEIER, 2001). Toutefois, pour MUSIANI F. Musiani, *Abécédaire des architectures distribuées*, précité :

Il n'existerait pas de définition univoque de ces architectures, mais des éléments communs :

- de multiples unités de calcul composent le réseau (souvent appelés nœuds, dotées chacune de mémoire locale, et communiquent par échanges
- les objectifs de l'application sont obtenus par le moyen d'un partage de ressources (qui peuvent être de plusieurs types), pour servir un but commun (par exemple un problème de calcul à large échelle)
- le système est tolérant vis à vis de la défaillance de nœuds individuels, ce qui a pour conséquence l'absence de point unique d'échec
- le passage à l'échelle se fait de manière souple, puisque les ressources à disposition du réseau augmentent avec le nombre d'utilisateurs
- la structure du système peut être constamment modifiée du point de vue de la topologie et latence du réseau, et le nombre d'ordinateurs qui y sont connectés, puisqu'une pluralité de parcours pour un même paquet de données est possible
- chaque nœud peut n'avoir qu'une vision incomplète ou limitée du système

[39] HIELLE O., *La technologie Blockchain : une révolution aux ombreux problèmes juridiques*, Dalloz Actualités, 31 mai 2016

[40] FAVREAU A., *Blockchain – Aspects techniques*, Répertoire IP/IT Communication, Dalloz, sept. 2021

des transactions, dont copie est conservée au sein de chaque organe faisant partie du réseau *blockchain*. Ces trois intérêts majeurs pouvant être appliqués dans trois types de *blockchain*[41].

15. Un premier type serait une *blockchain* « publique » ; ouvert au plus grand nombre. Dans un tel cas, tous les participants ont accès à la base de données, et peuvent la modifier (dans le sens de l'enrichir d'autres transactions, tel est le cas de la *blockchain Bitcoin*). Un second serait une *blockchain* « à permission » ou hybride ; tous ont accès à une version de la base de données, mais seulement certains nœuds (ou serveurs) sont autorisés à y contribuer, les autres utilisateurs n'ayant que des permissions de lecture (par opposition aux permissions d'écriture). Un dernier serait une *blockchain* « privé » ; l'accès et la modification des informations du *blockchain* seraient réservés à un groupe restreint d'utilisateurs.

16. C'est au sein de ces différentes catégories que l'on peut trouver des applications variées à la technologie *blockchain*. Si la *blockchain* privée est souvent mise de côté, c'est en raison de son caractère potentiellement confidentiel, avec, surtout, un nombre de mineurs limité. Dès lors, seuls les participants d'une telle *blockchain* vont être intéressés par elle, et surtout, comme cela pourra être explicité, une telle *blockchain* ne sera guère différente d'une base de données classique. Il est acquis, pour la pratique informatique, qu'une telle *blockchain* ne revêt qu'un intérêt très faible, et apparaît même comme superflue par rapport à une base de données classique.

17. Les enjeux de la *blockchain* sont évidemment multiples ; par exemple, en ce qui concerne la fonction de paiement, ils peuvent trouver matérialisation dans la sécurisation des transferts d'argent. En effet, de par la nature d'une *blockchain*, un paiement entre deux personnes (ou plusieurs) se trouvera sécurisé, fiable, et surtout, inscrit de manière immuable dans un registre partagé. Ainsi, tous les participants à une telle *blockchain* auront trace du paiement, de son effectivité et de sa validité. La confiance dans un tel paiement se trouvant

[41] Cette catégorie tripartite vient de Open Data Institute (ODI), pour une lecture complémentaire : « Les enjeux et les défis des infrastructures de données utilisant la *blockchain* selon l'Open data institute », LINC (Laboratoire d'Innovation Numérique de la CNIL), 02 août 2016

déplacée des personnes visées vers la *blockchain* directement ; dans une telle configuration, une *blockchain* de type « publique » sera privilégiée.

18. Un second type, dans le cadre de la tenue de registres infalsifiables : une *blockchain* permet de valider et d'authentifier des transactions, des données à un sens plus large. Tenir un registre dans un organe décentralisé régi par une *blockchain* présente un avantage immédiat : là où la corruption de l'organe centralisateur peut mettre en échec l'ensemble d'un système, un système décentralisé permet de s'affranchir de ce risque, et ainsi obtenir un système informatique sécurisé, fiable et durable ; cette application pouvant être réalisée dans le cadre d'une *blockchain* « hybride », dans laquelle on pourra trouver un nombre restreint de mineurs pour une variété d'utilisateurs finaux sans droit d'écriture.

19. Un dernier type, la troisième fonction identifiable d'une *blockchain* fait appel à la notion de « *smart contract* ». Pouvant être traduite par l'appellation « contrat intelligent », cette notion est à ne pas confondre avec la conception juridique classique du contrat[42]. Un « *smart contract* » est un protocole informatique, qui permet l'exécution d'une obligation quand les conditions requises et implantées dans ce dernier sont réalisées. L'utilisation d'un « *smart contract* » dans le cadre de la troisième fonction d'une *blockchain* permet l'automatisation d'exécutions contractuelles. Un exemple tiré d'une application *blockchain* développée par la société Slock.it[43] est le suivant : « je me trouve devant une serrure de porte d'hôtel, serrure connectée et utilisant une *blockchain* ». Deux opérations sont possibles : l'ouverture ou le verrouillage de la porte. Le « *smart contract* », ayant été intégré dans le protocole *blockchain* relié à la porte, déclenchera son ouverture si certaines conditions sont remplies, notamment la libre disposition des lieux. Dans l'affirmative, le « *smart contract* » déclenchera l'ouverture de la porte, et le reste du processus contractuel (paiement, mise à disposition, etc.) se résoudra par une même série d'opérations. Dès lors, le « *smart contract* » inclus dans la *blockchain* permet la conclusion automatique de conditions contractuelles (en

[42] Article 1101 Code civil : « Le contrat est une convention par laquelle une ou plusieurs personnes s'obligent, envers une ou plusieurs autres, à donner, à faire ou à ne pas faire quelque chose / Le contrat est un accord de volontés entre deux ou plusieurs personnes destinées à créer, modifier, transmettre ou éteindre des obligations. » ; version antérieure au 1er oct. 2016 / version actuelle

[43] slock.it, « Slock.it 3 minutes demo », London *Ethereum* Devcon One conference, consulté le 10/08/2017

l'espèce un contrat de réservation hôtelière), en faisant reposer le processus contractuel non pas sur une phase classique de pourparlers ou d'adhésion, mais sur une suite logique d'opérations en amont prévues[44].

20. Cet exemple a permis de mettre en exergue la notion de « *smart contract* » qui peut être incluse dans une *blockchain* ; cette notion, à laquelle on peut faire référence avec l'expression « *Code is law* »[45], permet de se rendre compte, d'une autre façon, des enjeux massifs que peut présenter la technologie *blockchain*. Sans être exhaustif, il permet d'automatiser toute une série de processus contractuels, aussi bien dans le milieu hôtelier que financier, que dans le domaine de la location de biens meubles que dans celui de la santé.

21. C'est notamment pour ces raisons que la *blockchain* est souvent présentée comme étant une technologie dite disruptive, capable de bouleverser la plupart des systèmes actuels, qui reposent sur des systèmes centralisés. En définitive, un protocole *blockchain* est un moyen informatique permettant, à travers un logiciel spécifique, la mise en place d'une base de données décentralisée. En ressort ainsi une dualité de composants primaires techniques, qui fera d'ailleurs l'objet d'une dualité juridique par la suite.

3. Fonctionnement d'une blockchain

22. Chaque transaction effectuée sur une *blockchain* repose sur l'utilisation de techniques informatiques particulières : les algorithmes de chiffrement asymétrique. Ce système repose sur l'utilisation de deux « clés », une clé publique et une clé privée[46]. Ce système, utilisé depuis les années 1970 permet à tout utilisateur de posséder un moyen simple de chiffrer ou déchiffrer un message sur un réseau donné. Et permet ainsi de garantir la confidentialité et l'intégrité d'une information (en s'assurant que l'information ne soit pas déformée ou altérée pendant le processus d'utilisation).

---

[44] La modernisation - ou numérisation - de ces rapports contractuels fait l'objet de développements postérieurs, Cf. *Infra*, p55 et suiv.

[45] LESSIG L., *Code, and Other Laws of Cyberspace*, 1999, Basic Books

[46] Pour l'illustration du fonctionnement d'une *blockchain* : FAURE-MUNTIAN V., MM. DE GANAY C, LE GLEUT R., *Rapport n° 584 (2017-2018),., fait au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques*, déposé le 20 juin 2018

Un utilisateur d'une *blockchain* va créer un identifiant, lui permettant ainsi de posséder les deux clés, publique et privée. En particulier, dans l'utilisation d'une *blockchain* de type *Bitcoin*, cette fonction asymétrique permet de signer toute transaction. Aujourd'hui, la création de cet identifiant va répondre à des exigences proches de celles des exigences « KYC[47] », à savoir la communication de documents d'identité valables et reconnus par les lois de l'état de l'utilisateur. Une fois son « compte utilisateur » crée, l'utilisateur va pouvoir effectuer des transactions sur un *blockchain*, qui seront toutes identifiées grâce à son identifiant. L'ensemble des participants à cette *blockchain* peuvent donc être sûr de l'identité de leurs co-contractants.

B. Définitions juridiques

23. Le législateur français a fait preuve d'énormément d'innovation. Dans l'ordonnance n°2016-520, du 28 avril 2016[48], en ce qu'elle définit le nouvel article L223-12 du Code monétaire et financier : il est permis l'émission et la cession des minibons au sein d'un « dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations ». La France s'est ainsi dotée de la première quasi-définition légale d'une *blockchain*. L'ordonnance susvisée prévoit également qu'un décret pris en Conseil d'état viendra préciser les conditions de validité, et notamment de sécurité, et enfin, elle précise également que la condition d'écrit (nécessaire pour la validité d'une telle opération financière) sera satisfaite par l'utilisation d'une *blockchain*.

24. L'appellation de quasi-définition est une prise volontaire de position. En l'état, définir un objet juridique par ses seules caractéristiques techniques ne parait pas suffisante, d'autant plus que l'ordonnance susvisée n'indique que seule l'inscription en titre sur une *blockchain* aura une valeur juridique, ni les opérations de cession, de conservation ou encore de transfert ne sont visés par l'ordonnance de 2016 dans le cadre de l'utilisation d'une *blockchain*. Il convient de considérer cette innovation législative, relevant une prise en compte relative rapide

[47] Les exigences « KYC » ou Know Your Customer sont des exigences relatives à la connaissance client, son identification, la vérification de son identité et à la lutte contre le blanchiment d'argent, notamment en imposant aux établissements financiers une identification précise de tous les clients. Pour plus d'informations : https://acpr.banque-france.fr/sites/default/files/media/2018/12/17/lignes_directrices_relatives_a_lidentification_la_verification_de_lidentite_et_la_connaissance_de_la_clientele_.pdf, consulté le 10/01/2019

[48] Ordonnance n°2016-520, précitée

(d'un point de vue législatif) d'un nouvel outil technique. Témoin d'une faculté du législateur de donner une expression ou encore une traduction à portée plus juridique à un anglicisme dont l'appropriation rapide par différents acteurs (entreprises, particuliers, etc.) est constatée. L'intérêt d'une telle démarche, à notre sens, est, de prime abord, d'harmoniser un vocable parfois technique et difficile d'appropriation pour l'ensemble des populations ne faisant pas partie d'un univers précis qui aurait vu apparaître une telle notion. L'intérêt d'établir un vocable précis, outre l'affect que possède le monde juridique aux définitions, permet ainsi une reprise de terminologies équivalentes et homogènes pour de futurs travaux.

25. Néanmoins, il ne s'agissait, à travers l'ordonnance de 2016, que d'inscrire une notion, sans pour autant en donner une définition, et la mise à jour du vocabulaire de l'informatique[49] parue postérieurement, la définition suivante : « Mode d'enregistrement de données produites en continu, sous forme de blocs liés les uns aux autres dans l'ordre chronologique de leur validation, chacun des blocs et leur séquence étant protégés contre toute modification. ». L'expression de mode d'enregistrement est à souligner, car elle peut faire référence, de manière sémantique, à la notion de protocole informatique. En conséquence, d'un point de vue *stricto sensu* légal, la *blockchain* n'est qu'un mode d'enregistrement des données. Néanmoins, réduire l'appréciation d'une technologie à sa seule définition dans un sens littéral, n'expurge pas pour autant l'étude des conséquences juridiques de la mise en place d'un tel protocole, pointant l'insuffisance d'une telle démarche.

26. Toutefois, et pour servir les propos précédents, une première approche législative d'un objet juridique non identifié se remarque ; à savoir que le législateur a, dans une première étape, isolé des caractéristiques essentielles servant à protéger les intérêts des tiers (en l'occurrence sur la sécurisation des échanges d'actifs), pour ensuite se laisser le temps de pencher sur une définition plus légale, disons « juridique », qui, à notre sens, doit emporter adhésion.

27. Un schéma de première réaction peut se concrétiser. Sans poser ici la question de la valeur légale des mises à jour du « Vocabulaire de l'informatique », publiée au Journal

[49] JORF n°0121 du 23 mai 2017 - texte n° 20 - Vocabulaire de l'informatique (liste de termes, expressions et définitions adoptés)

Officiel, une telle publication possède le mérite de permettre à tous de connaître une notion particulière, comme pour donner corps à une nouvelle expression, une nouvelle technologie, sans pour autant emporter nouvelle définition dans le Dictionnaire. Comme si l'adage « nul ne peut ignorer la loi » s'appliquait aussi au vocabulaire de l'informatique, pour donner une dimension harmonieuse et faciliter de potentiels travaux futurs sur une notion qui, *de facto*, doit rester la même pour chacun pour en faciliter l'efficacité. Au-delà de simplement harmoniser le vocabulaire de chacun, il démontrer la capacité de donner un premier sens à une notion potentiellement abstraite pour le plus grand nombre, sans pour autant se poser la question du régime juridique de cette dite notion, laissant ce travail aux juristes ou aux magistrats.

28. De manière parallèle à ces premiers éléments de définition purement législatifs, qui auraient donc vocation à être intégrés dans un dictionnaire juridique, une tentative de définition contractuelle peut être réalisée en l'état des connaissances actuelles. Sera ici entendue, comme définition contractuelle, l'expression pragmatique et juridique de la mise en place d'une *blockchain* au sein de documentations contractuelles, donc telle que la pratique pourrait s'en saisir, laissant peut-être ainsi une place non négligeable au principe de liberté contractuelle, mais permettant une appropriation plus aisée.

L'un des points de difficulté autour de la technologie *blockchain* est le fait que sa mise en place requière plusieurs éléments :

- Un logiciel, pouvant gérer l'algorithme de consensus ;
- Du matériel, afin de mettre en place le réseau ;
- La constitution et la gestion d'une base de données décentralisée (même si une partie de cette gestion sera faite automatiquement à travers le logiciel de gestion de consensus) ;
- Et aussi un savoir-faire, aujourd'hui peu répandu au sein de la communauté informatique et/ou juridique.

29. En matière de contrats informatiques, il existe le logiciel « expert », c'est-à-dire un logiciel spécifique (un moteur d'inférence[50]), associé à au moins une base de données spécialisée, et un savoir-faire[51]. On peut également parler de « système expert », formant une création complexe, qu'il serait « souhaitable d'apprécier globalement »[52] pour la doctrine. Il paraît opportun de faire cette appréciation globale quand on étudie la technologie *blockchain*. En effet, la résumer à un simple logiciel ou à une base de données unique, serait réducteur techniquement et juridiquement. La *blockchain* vise à mettre en place toute une architecture informatique complexe, architecture qui sera elle-même le centre décisionnel.

Si un choix est fait pour une appréciation globale telle qu'envisagée précédemment, il est possible de considérer que la gestion contractuelle de la technologie *blockchain* peut se rapprocher de la gestion contractuelle d'un système expert. L'intérêt de faire un tel parallèle est d'entrevoir les conséquences juridiques de la mise en place, contractuelle, d'une *blockchain*. Si on prend le parti de considérer ce contrat comme innommé[53], il faudra le considérer de manière globale, aussi bien en prenant compte notamment des spécificités du droit des logiciels, ou celui des bases de données pour l'élaboration de tout processus contractuel.

30. En réalité, et pour s'inspirer de du principe fondamental de la liberté contractuelle, cette définition juridique peut trouver aussi bien une application que non. À notre sens, cette définition tend à donner un meilleur aperçu purement juridique et a le mérite de permettre une meilleure appréhension de la notion de *blockchain*, mais tend à perdre sens dans le cadre d'une application purement « *open-source* » d'une *blockchain*, ou dans le cadre d'une application internationale. En conséquence, la construction d'un régime *sui generis* dédié à la *blockchain* peut paraître opportune, mais la création d'un nouveau régime juridique propre peut tout aussi présenter ses défauts (cohérence de régime avec la pratique, évolution de ce régime et pérennité de ce dernier). Une construction composite, comme il est possible de trouver avec le contrat multimédia ou de jeux vidéo présente tout autant d'intérêt.

---

[50] Un moteur d'inférence est un logiciel correspondant à un algorithme de simulation des raisonnements déductifs, cf. https://fr.wikipedia.org/wiki/Moteur_d%27inf%C3%A9rence, consulté le 10/02/2019

[51] LE TOURNEAU P., *Contrats informatiques et électroniques* - Dalloz Référence, 10ème édition, p.670

[52] VIVANT M., Lamy - Droit du numérique, *Les systèmes-experts*, Wolters Kluwer, §513 à §518

[53] LATINA M., *Répertoire de droit civil, Contrat : généralités - Classifications des contrats* – Mai 2017 (actualisation : Fév. 2020)

31. **«** Choisir une qualification, c'est adapter un ensemble de solutions de droit [54]». C'est l'essence même de tout travail juridique novateur que de vouloir rattacher un objet juridique non identifié à un objet lui-même défini et éprouvé comportant des éléments préexistants facilitant ce travail. Relevant du droit d'auteur[55], les jeux vidéo sont parfaitement intégrés aujourd'hui dans l'univers numérique. Les débats sur la nature du jeu vidéo se sont cristallisés autour du fait qu'il s'agisse de plusieurs typologies d'éléments, entre le logiciel, les scénarios ou encore la musique. L'arrêt *Cryo*[56] a permis d'identifier le jeu vidéo comme « une œuvre complexe qui ne saurait être réduite à sa seule dimension logicielle, quelle que soit l'importance de celle-ci, de sorte que chacun de ses composants est soumis au régime qui lui est applicable en fonction de sa nature », opérant donc un choix d'une qualification distributive[57] au jeu vidéo. Ce choix de qualification distributive doit, à notre sens, être appliqué à la *blockchain*.

Ses caractéristiques fondamentales, à savoir l'imbrication de plusieurs éléments, pouvant faire l'objet d'une qualification propre (logiciel, base de données, données, etc.) font d'une *blockchain* un objet juridique complexe et composite, dont la nature empêche la réduction à une unique qualification. En conséquence, l'étude d'une *blockchain*, et plus généralement d'un protocole *blockchain* ne saurait se réduire à une approche désordonnée, il en revient, en réalité, à en faire une appréciation ordonnée et méthodique de l'ensemble de ses éléments.

32. Une méthodologie se dessine de nouveau, si la création d'une notion terminologique harmonisée permet de rendre homogène la recherche sur cette dernière, il convient de déterminer le contour de cette même notion, même s'il en ressort un éclatement des composantes applicables (pour reprendre les faits de l'arrêt *Cryo*, on peut concevoir que l'approche unilatérale qui consistait à considérer le jeu vidéo comme un simple logiciel a

---

[54] ATIAS C., *Droit civil, les biens*, 2000, Paris, p.892

[55] Le jeu vidéo, par un arrêt rendu le 7 mars 1986 par la Cour de cassation, réunie en Assemblée plénière, a obtenu la qualification d'œuvre de l'esprit (Cass. Plén., D. 1986. 405, note B. Edelman ; JCP E 1986, II, n°14713)

[56] Cass, 1ère Civ., 25/06/2009, n°07-20.387, arrêt dit *Cryo*, RIDA 2009, n°221, p509

[57] HASSLER T., *Qualification du multimédia : plaidoyer pour une méthode de qualification*, CCC nov. 2000, p.10

complètement éclaté sur la réalité de cet objet vidéoludique), pour au final réaliser une approche ordonnée, basée sur une seule sémantique, pouvant conduire, comme avec le jeu vidéo, à une véritable construction ordonnée, basée sur l'existant.

33. Cette dualité d'approche, extrêmement hétéroclite, et la complexité même d'un tel objet juridique met en exergue une facette propre aux nouvelles technologies, ou, plus généralement, à tout nouveau concept ayant des impacts forts sur notre vie quotidienne, tant d'un point de vue économique ou encore sociétal mais surtout dans une approche juridique. L'éclatement ou plutôt la prise de conscience, de plus en plus véloce de l'impact des nouvelles technologies dans notre quotidien juridique nous amène à nous poser la question suivante :

Comment définir un régime applicable à une technologie disruptive dans le contexte juridique contemporain ?

34. C'est dans le cadre de cette réflexion qu'il conviendra de constater une actuelle approche désordonnée (Partie I), liée en réalité à la complexité d'un sujet qui mêle de nombreuses matières, pour avancer la possibilité d'une approche ordonnée (Partie II) de notre droit positif, si tant est que des réflexes d'analyse sémantique et d'ouvertures interdisciplinaires sont présents.

Première partie : Le constat d'une approche désordonnée

35. La confrontation d'objets juridiques non identifiés[58] au droit positif bouleverse nos conceptions traditionnelles, au point de constater, en prenant l'exemple de la *blockchain* une explosion de la littérature juridique. Une telle inflation doctrinale sur un sujet en tant que tel n'emporte pas *de facto* la considération d'une telle approche désordonnée. Toutefois, l'étude de cette doctrine relève une multiplicité de matières d'études, sans forcément créer de « fil rouge » commun à ces dernières. En effet, la *blockchain* a pu être étudiée à travers un pan pénal (notamment vis-à-vis de l'utilisation du *Bitcoin* pour des transactions illicites[59]), ou encore au regard de ses gains pour le monde de l'art[60] ou encore à travers le financement immobilier[61], démontrant une désorganisation d'approche, notamment quand les différentes études peuvent se borner à faire un simple rappel technique littéral sur la *blockchain*, ne mettant en avant que de simples avantages à court ou moyen terme de l'usage d'une telle technologie. Cela étant, la désorganisation de l'approche d'une telle technique se conçoit, notamment en raison des difficultés liées à sa simple appréhension. Néanmoins, si un éclatement du cadre juridique applicable à cette technologie (Titre 1) est effectivement à constater compte tenu de ses différentes facettes et applications, il en ressort en réalité une émergence de nouveaux modèles de gouvernance (Titre 2), portée par une omniprésence de la donnée au sein de notre société.

[58] ROUSSILLE M., précité

[59] LOUVET N., PDG COINHOUSE, *Les apports de la blockchain et des actifs numériques au secteur financier*, Dalloz IP/IT 2019 p.546 ; cet article mettant en avant cette utilisation, pourtant marginale, l'utilisation de bitcoin sur le « darkweb ».

[60] GIRAUD T., *Vie culturelle - La blockchain est-elle l'avenir de la culture ?* JAC 2017, n°51, p.35

[61] VERBIEST T., RICHEBOURG D., *Blockchains et financement de l'immobilier*, AJDI 2019. 423

Titre 1 : Un éclatement du cadre juridique applicable

Principe de Lavoisier

« Rien ne se perd, rien ne se crée, tout se transforme. »

Antoine Laurent de LAVOISIER (1743-1794)

36. La seule inscription dans le vocabulaire de l'informatique de la *blockchain* (en tant que dispositif d'enregistrement partagé) est le premier pas vers la validation de la méthodologie ci-avant exposée. Partant de la réflexion qui a pu servir l'arrêt Cryo[62], dans la retenue d'un cadre composite pour le jeu vidéo, c'est la compréhension d'une approche quasi chimique qui se dessine. À l'instar du père de la chimie moderne[63], la compréhension d'un nouvel objet peut se résumer en sa première décomposition, pour comprendre l'essence même de chaque élément le composant, pour pouvoir après mieux le reconstruire, l'étudier, le transformer, l'adapter. Si on pousse cette métaphore, pour comprendre le jeu vidéo, et donc construire un régime adéquat à cet objet, ce premier travail de déconstruction a été nécessaire, pour mieux comprendre chaque élément pris individuellement, pour ensuite mieux le recomposer et en déterminer un régime propre et surtout efficace.

37. La *blockchain* a ce mérite, elle éclate toute approche d'étude universelle, dès lors comme l'appréhender de manière efficace, tant deux *blockchain*s peuvent avoir des applications complètement opposées ?

En réalité, pourquoi ne pas appliquer cette approche scientifique, presque « Lavoisienne », à l'étude de la *blockchain* ? Déconstruire ses différents éléments, ses différentes caractéristiques pour mieux en saisir l'essence et ainsi mieux la comprendre. Le caractère disruptif de la *blockchain* a premièrement été constaté au travers de ces applications économiques, cette approche, empirique, nous invite à avoir des approches similaires. C'est pourquoi l'éclatement du cadre applicable à la *blockchain* doit en fait revenir vers ses

[62] Cass, 1ère Civ., 25/06/2009, n°07-20.387, arrêt dit *Cryo*, voir com. HASSLER T., précité.

[63] Lavoisier, dans l'édition de son principe de conversation des masses (ou principe de Lavoisier) a dessiné les bases de la chimie moderne. Lavoisier, Traité élémentaire de chimie, 1789, pp. 140-141

fondamentaux, à savoir les régimes juridiques généraux applicables à une technologie. Majoritairement exploitée (et rendue publique) avec le *Bitcoin*, la *blockchain* mérite alors de premières approches technico-économiques (Chapitre 1), et en ce qu'elle met en avant la suppression de tiers pour la réalisation d'échanges, ce qui permettra logiquement de porter notre étude sur les transformations techniques des rapports civils (Chapitre 2), l'un des fers de lance des différents soutiens à cette technologie.

Chapitre 1 : Approches juridiques et économiques anarchiques

38. L'étude de la *blockchain*, au prisme de ses nombreuses applications (financières, juridiques, scientifiques, cryptographiques, etc.) reflètent non pas un éclatement d'un cadre unique de compréhension, mais l'apparition d'un environnement hétéroclite recentré non pas sur des conceptions économiques, sociales, ou juridiques, mais sur un seul trait commun, une technologie. Cette approche n'est pas fantasque, dans le sens où l'apparition de réseaux de communication développés ont permis une telle apparition. Internet, ce réseau de communication est aujourd'hui utilisé de manière multisectorielle, dont les caractéristiques techniques trouvent des applications de manière quasi-universelle.

39. Dès lors, se focaliser de prime abord sur le cadre applicable à une technologie paraît insuffisant tant la définition d'un tel cadre est chose mal aisée. À l'inverse, une absence de définition peut bloquer la moindre réflexion. Car, à moins de posséder un savoir omniscient, tout étude se trouvera non exhaustive. En réalité, comprendre une technologie face au droit, et donc en étudier les facettes juridiques ne nécessite pas nécessairement une réflexion micro-juridique dans un premier temps, mais plus une approche globale, prise pour les intérêts technico-économiques d'une telle technologie. Ainsi, revenir aux fondements mêmes d'une technologie, reprendre les fondements de construction et d'élaborations sont indispensables à une compréhension correcte de cette même technologie. La technologie des chaînes de blocs, dont la mise en avant date de fin 2008[64] a été créée en réaction quasi épidermique à la crise financière de 2007-2008[65], marquée par les dérives du système financier alors en place. Le but de ce *white paper* est alors de déterminer un système technique monétaire fonctionnant sans organe de contrôle, remettant au centre des opérations financières non plus les opérations-tiers de confiances mais le simple utilisateur, de manière à garantir la traçabilité et la fiabilité de ses opérations. Au point de considérer le *white paper* de Satoshi comme « manifeste crypto-anarchiste, avènement du rêve hayekien de la concurrence monétaire ou encore promesse de

[64] Le 31 oct. 2008, le *white paper* « Bitcoin : A Peer-to-Peer Electronic Cash System » est publié sur le site internet bitcoin.org, il devient la pierre angulaire de la technologie *blockchain*, son auteur est désigné comme « Satoshi Nakamoto » mais est considéré comme un pseudonyme de manière consensuelle à travers le monde ; https://bitcoin.org/bitcoin.pdf

[65] Appelée communément « crise des Subprimes ». Pour plus d'information : https://fr.wikipedia.org/wiki/Crise_financi%C3%A8re_mondiale_de_2007-2008, consulté le 15/08/2019

nouvelles formes de solidarités numériques[66] » Ce fut donc pour une vocation financière - mais aussi, dans une certaine mesure sociologique et philosophique - que le *Bitcoin* a été créé.

40. C'est en raison de cette approche une nouvelle fois marqué de dualité, quoique éclatée, qu'il convient, dans le cadre de ce chapitre d'étudier les raisons mêmes de l'adoption de *blockchain* à travers l'émergence de nouvelles économies de la confiance (Section 1). Également, il est nécessaire d'étudier la possible brevetabilité d'une *blockchain* en tant qu'élément de technique (Section 2), tant l'impact technologique et économique de la *blockchain* est important.

Section 1 : Émergences de nouvelles économies de la confiance

41. C'est l'un des principaux arguments avancés lors de l'adoption de protocoles *blockchain* (qu'ils soient pour supporter des services financiers ou non), le fait qu'une *blockchain* se dédouane de l'impératif de confiance envers un tiers, supprimant ainsi tout intermédiaire. Cette affirmation simple revêt un caractère presque simpliste car, en réalité, il faut avoir conscience du fait que la confiance est simplement « déplacée ». Là où un système pyramidal économique classique - reposant sur des échanges entre A et B, validés par un tiers de confiance, majoritairement une banque dans un cadre financier - repose sur l'intervention d'un tel tiers, un système reposant sur une *blockchain* déplace la notion de confiance vers un protocole informatique sur le simple postulat que deux acteurs vont partager ce même protocole. Il existe donc un transfert de la confiance, en tant qu'élément fondateur et fondamental de l'économie[67], au point que certains lui prêtent le caractère de devenir le « poumons d'une nouvelle économie[68]».

42. C'est à partir de ce postulat à caractère quasi anarchiste[69] que sont nées différentes initiatives avant tout économiques et ont permis d'étudier dans une première mesure les impacts de la *blockchain* dans le cadre du secteur financier. Néanmoins, l'usage du pluriel

[66] BRUNELLE A., *Éloge de la confiance : la Blockchain, l'entreprise et le droit de la concurrence*, Revue Lamy de la Concurrence, 01/12/2019, 89, pp.31-36

[67] ÉLOI L., *Économie de la confiance*, 2019, collection Repères

[68] MEKKI M., *Le juge et la blockchain : l'art de faire du nouveau vin dans de vieilles outres*, disponible à https://mustaphamekki.openum.ca/files/sites/37/2019/10/5.Mekki-juge-et-*blockchain*.pdf, consulté le 07/08/2020

[69] BRUNELLE A., précité.

pour parler « d'économies de la confiance » ne repose pas que sur les seuls versets économiques. En effet, l'usage de la *blockchain* dans le cadre d'initiatives publiques dans le cadre d'un renforcement de la fiabilité de la donnée présente autant d'intérêts.

43. « Dans le contexte d'un monde en mutation […] la confiance est une ressource précieuse pour les dirigeants, les collaborateurs, les clients, les partenaires ! »[70]. C'est là que la technologie *blockchain* peut revêtir un intérêt particulier. La notion de tiers de confiance, dans le sens qu'elle désigne une personne, pourrait être remplacée par un système *blockchain*, possédant le critère de fiabilité[71], essentiel à la reconnaissance de la validité de la signature électronique par exemple.

Excluons d'ailleurs la notion de tiers de confiance au sens fiscal du terme[72].En numérique, le tiers de confiance est un acteur du développement de la confiance dans le monde numérique.

La notion de fiabilité est particulièrement subjective ; selon M. Devèze, elle « n'évoque pas une sécurité purement objective, une certitude absolue mais une foi, une confiance raisonnée, une probabilité raisonnable »[73].

Dans notre droit positif, la fiabilité est une condition nécessaire à la validité d'une signature électronique[74]. Ainsi, la fiabilité est, finalement, un élément déterminant quant à la garantie aussi bien de la sécurité des transactions que celle des contractants, et est donc au cœur du contrat électronique, sorte de « chaînon qui relie le technologique au juridique et la caution juridique du technique »[75].

---

[70] BUFFARD P., préface, *Code Informatique, Fichiers et Libertés*, Alain Bensoussan, Editions Larcier, 2014

[71] Art. 1367, C. Civ.

[72] Article 95 ZA, CGI ; « Le tiers de confiance mentionné à l'article 170 ter du code général des impôts qui a conclu avec l'administration fiscale la convention individuelle mentionnée à l'article 95 ZG signe avec son client un contrat qui définit sa mission ainsi que les droits et les obligations de chaque partie.

La mission du tiers de confiance prend effet à la date de signature du contrat conclu avec le client. ». Le rôle d'un tel « tiers de confiance », en droit fiscal, désigne la personne qui bénéficiera de la confiance de l'administration fiscale, dont les informations seront présumées (fortement) fiables.

[73] DEVEZE J., *« vive l'article 1322 ! », Commentaire critique de l'article 1316-4 Code civil, in* Études offertes à P. CATALA, Litec 2001, p.531

[74] Article 1367 Code civil, précité.

[75] AKODAH A., *La preuve des actes juridiques sous le prisme des contrats électroniques,* Revue Lamy Droit de l'immatériel, 45, 1er sept. 2009

44. La fédération nationale des tiers de confiance du numérique[76] s'adresse aux éditeurs de logiciels, aux professions réglementées, ou encore aux prestataires de services en produisant des référentiels ou encore des labels afin que les systèmes d'information soient fiables. Son rôle est aujourd'hui d'autant plus important dans une société où la dématérialisation des échanges se fait de plus en plus commune. À ce titre, cette fédération a lancé un groupe de travail sur les possibilités de la technologie *blockchain*[77].

L'attrait de la technologie *blockchain* est sa possible application en tant qu'outil de fiabilité, et pourrait avoir comme conséquence que la personne qualifiée de tiers de confiance ne serait plus forcément une personne, un organisme, mais pourrait être un système lui-même, dont le fonctionnement garanti à lui seul la fiabilité et l'authenticité des données. En conséquence, c'est pour ces raisons que la presse spécialisée[78] met en avant que la fonction de tiers de confiance soit mise à mal par l'avènement de la technologie *blockchain*. En effet, la mission d'un tiers de confiance est potentiellement remplacée par la mise en place d'un système *blockchain*, diminuant ainsi les coûts (humains notamment), renforçant la sécurité des échanges (du fait de l'inscription horodatée et vérifiée de toute donnée), et ce, en toute transparence (du fait du partage des données entre les différents nœuds du réseau *blockchain*).

Nous pouvons d'ailleurs remarquer la création de Notalis, groupe de travail créé afin de lier la *blockchain* et la profession notariale[79] ; cela étant, un protocole *blockchain* pourra être considéré comme valable en tant que mode de constitution d'une preuve, compte tenu de la possibilité laissée, et ce depuis plusieurs années, par le législateur pour l'utilisation de tels moyens dont la complexité est à la hauteur de la garantie apportée au bénéfice de l'intégrité des données visées. En outre, les événements de début 2020 liées à l'épidémie du « Covid-19 » ont pu démontrer des applications concrètes d'outils de dématérialisation, notamment en

[76] http://fntc-numerique.com ; née en fév. 2001, cette fédération a pour vocation de structurer les échanges numériques.

[77] Dépêches JurisClasseur, 29 avril 2016, « La fédération des tiers de confiances lance un groupe de travail sur la *blockchain* »

[78] GARAPON A., *La blockchain va-t-elle remplacer tous les tiers de confiance* ?, Matières à penser, France Culture, 05/08/2018 ; IPTRUST, *Blockchain et smarts contracts, quid de la suppression du tiers de confiance ?*, IP TRUST, 4 juil. 2017

[79] DELZANNA C., *Trois questions à Caroline Jeanson* - Droit et patrimoine l'hebdo, 1052, 18 avril 2016

autorisant, pour les professions notariales le recours à de telles technologies pour la conclusion d'actes à distance[80].

45. Toutefois, le remplacement de tiers de confiance, tels que les fonctions notariales par exemple, par des protocoles utilisant des technologies *blockchain* n'est, dans le sens de cette étude, pas suffisamment concret à court ou moyen terme. Toujours est-il que la *blockchain*, pris dans l'exemple de *Bitcoin*, possède une idéologie propre, dont la connaissance est essentielle pour comprendre l'essor d'une telle technologie. Il convient ainsi de comprendre l'idéologie de décentralisation de la *blockchain Bitcoin* (§1), née en réaction à un système bancaire centralisé. Cette décentralisation provoquant une effervescence de nouvelles relations de confiance dans l'univers numérique (§2), fondées non pas sur des acteurs ciblés mais sur des aspects purement technologiques.

§1 : L'idéologie de décentralisation de la *blockchain Bitcoin*

46. Dans le cadre de la présente étude, un rappel sémantique doit être effectué ; la terminologie *Bitcoin* (majuscule) fera écho à la *blockchain Bitcoin*, servant de protocole informatique de base pour la gestion de l'actif numérique *Bitcoin*, la terminologie « *Bitcoin* » désignera l'actif numérique - ou token - affilié à cette *blockchain*. Le fonctionnement de la *blockchain Bitcoin* demeure à l'origine de la démocratisation de la technologie des chaînes de blocs ; initiée par le *white paper* de Satoshi[81], la naissance de ce protocole repose sur l'adéquation entre des concepts cryptographiques permettant notamment d'éluder la problématique de la double dépense, permettant ainsi d'être sûr que l'échange d'une donnée, bien non rival[82], ne soit pas effectué deux fois.

47. La donnée, en tant qu'actif incorporel, relié directement à l'informatique, est un bien d'une nature particulière en ce que sa consommation ne la fait pas disparaître. Dans un univers numérique, la non-rivalité de la donnée présente un inconvénient, qui a été illustré notamment en tant que problématique dans le partage de données illicites sur Internet. En effet, la non-rivalité d'une donnée informatique a pour première conséquence que la suppression d'un

[80] Décret n° 2020-395 du 3 avril 2020 autorisant l'acte notarié à distance pendant la période d'urgence sanitaire.

[81] NAKAMOTO S. « Bitcoin : A Peer-to-Peer Electronic Cash System », 2008, précité.

[82] La rivalité est une notion économique, elle désigne la propriété d'un bien dont la consommation par un agent diminue la quantité de bien disponible pour les autres agents.

support de cette donnée ne permet pas de s'assurer de la disparition de la donnée en tant que telle, car répliquable, théoriquement, à l'infini[83]. C'est d'ailleurs l'une des problématiques isolées dans le cadre de la lutte contre la contrefaçon dans l'univers numérique, et inversement, l'une des qualités de ce même univers mis également en avant[84]. Dans le cadre d'un échange monétaire sur internet, la notion de double dépense a tout son intérêt. Dans le cadre d'un échange monétaire classique, vérifié et validé par un tiers de confiance comme un établissement financier (un établissement A sera sûr d'être payé par l'établissement B, pour laquelle la banque X est garante de la présence de fonds), il y aura ainsi une espèce garantie de paiement pour le créditeur, conférée par ce tiers de confiance. Cette garantie pouvant ainsi se trouver dans le cadre d'une échange monétaire classique (dans le sens de physique) ou numérique (dans le sens dématérialisée). Or, le principal enjeu d'un protocole de paiement souhaitant s'affranchir de tiers de confiance comme un banque a une problématique irrésistible : comment être sûr que l'argent promis par B à A n'a pas déjà été dépense, ou pis, a été dépensé deux fois ? Cette question reste cruciale, car en l'absence de moyen de vérification et de traçabilité d'un échange monétaire, le risque premier est de créer une inflation monétaire incontrôlable du fait de l'absence de telles vérifications. Dès lors, la problématique de la double dépense, analysée, notamment, par la doctrine économique[85], met en avant la nécessaire réponse technique permettant de conférer un caractère rival à un bien par essence non rival.

48. La technologie *blockchain* résolvant ce problème de la double dépense, il « suffisait » de concrétiser un système monétaire permettant de garantir les transferts d'actifs, leur traçabilité et leur non-révocabilité pour qu'elle devienne, conformément à l'idéologie de son auteur, un moyen fiable et sécurisé de transférer des fonds. C'est cette inscription en modèle de blocs, reliés les uns aux autres et partagés entre l'ensemble des utilisateurs du réseau qui donne son essence à *Bitcoin*.

---

[83] Il s'agit ici du paradoxe d'Arrow, cf. ARROW K., *Economic welfare and the allocution of ressources for invention. The rate and direction of inventive activity : economic and social factors*, National Bureau of Economic Research, 1962, disponible à : https://www.nber.org/system/files/chapters/c2144/c2144.pdf (consulté le 24/09/2021).

[84] LESSIG L., *L'Avenir des idées : Le sort des biens communs à l'heure des réseaux numériques*, Presses universitaires de Lyon, sept. 2005, 414 p.

[85] W. CHOHAN U., *The Double Spending Problem and Cryptocurrencies*, UNSW Business School ; Critical *Blockchain* Research Initiative (CBRI) ; Centre for Aerospace & Security Studies (CASS), December 19, 2017.

Le but, non dissimulé, est de créer et de favoriser l'adoption d'un système monétaire affranchi des comportements des banques traditionnelles, accusées d'avoir été à l'origine de la crise des « *subprimes* ». L'idéologie de la *blockchain Bitcoin* est de proposer un système fiable, moins couteux et transparent, dans lequel la confiance n'est plus placée auprès d'acteurs tiers, mais dans un système lui-même. La confiance de la bonne réalisation d'une transaction n'étant plus permise grâce à l'intervention d'un tiers mais seulement grâce au fait que les opérateurs partagent le même système, décentralisant les rapports financiers.

C'est dans cette mesure que la *blockchain* est vue comme apportant une « confiance 2.0[86] », se dédouanant d'acteurs pouvant être jugés comme malveillants (au sens informatique du terme), ou même comme des « menaces[87] ». La première « nouvelle économie de la confiance » ainsi présentée a en réalité pour but de s'affranchir des protocoles classiques de gestion monétaire, en mettant en avant le système et l'utilisateur de ce système, et en déplaçant cette confiance sur la technologie plutôt que sur un tiers, comme si ce sentiment de défiance était perçu comme impossible intrinsèquement car il n'y a pas, paradoxalement, de question de confiance à se poser dans le cadre de l'application de formule mathématiques, compte tenu de leur intangibilité[88].

§2 : L'effervescence des nouvelles relations de confiance dans l'univers numérique

49. À l'heure du « tout numérique », à une époque où la rapidité des informations et des transactions devient un enjeu aussi bien international que privé, la gestion de la confiance dans l'outillage numérique demeure un enjeu majoritaire. La fiabilité d'une transaction, ou, beaucoup plus simplement, d'un paquet de données est un enjeu crucial. Une erreur dans une donnée peut facilement fausser toute une étude statistique. La remontée d'informations fiables, par exemple, comme pendant la crise du « Covid-19 » a été un enjeu sanitaire extrêmement

[86] VAMPARYS X., *Blockchain : quelques réflexions sur la confiance 2.0*, JCP E Semaine Juridique (édition entreprise) - 11/10/2018, 41, pp.47-49

[87] DRILLON S., *La révolution blockchain. La redéfinition des tiers de confiance*, RTD com. 2016. p.893

[88] Sans être clairement affirmé dans le cadre de la *blockchain* Bitcoin, le placement de la confiance au sein d'une technologie, régie par les mathématiques, argue dans le sens de l'intangibilité des mathématiques, en opposition avec le caractère variable de l'action humaine.

important. La question de la fiabilité de la donnée, de sa rapidité d'envoi et de réception font partie de problématiques techniques auxquelles la *blockchain* peut répondre.

Elle peut être une source de création de richesses, notamment pour ses capacités à diminuer les coûts dans le traitement de l'information, tout en améliorant sa disponibilité[89], sa vitesse, et sa transparence. À ce titre, elle fait déjà l'objet d'études, que ce soit au niveau d'institutions[90], ou d'associations spécialisées [91]. De manière parallèle, dans le cadre du projet de loi relatif à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, a été inséré un amendement visant à adapter le droit vis-à-vis de cette technologie[92].

De plus, l'innovation opérée par l'ordonnance du 28 avril 2016 (précitée) met en exergue le fait que les avantages obtenus grâce la technologie *blockchain* sont nombreux, notamment en termes de transparence et de publicité des transactions[93]. Il conviendra ainsi de relever qu'il s'agisse, pour le domaine financier des premières réglementations en la matière. Sans compter sur l'impact des tentatives de normalisation et de régulation à un niveau européen[94] ou encore international. Au point qu'une réponse du législateur, en ce qui concerne l'utilisation de la *blockchain* dans le transfert d'actifs numériques, a été de créer un cadre de contrôle et d'homologation des prestataires œuvrant sur ces domaines[95].

---

[89] Sur la notion de disponibilité appliquée aux données, cf. *Infra*, p.184 et suiv.

[90] BOHIC C., *LaBChain : le consortium blockchain de la Caisse des dépôts joue sur l'effet de masse*, ITespresso, 17 fév. 2017, disponible à : https://www.itespresso.fr/labchain-consortium-*blockchain*-caisse-depots-effet-masse-148363.html. À ce titre, la Caisse des dépôts et la Banque de France ont commencé à étudier depuis 2017, notamment en participant au consortium « La BChain »

[91] ADAN, Rapport sur 'état de l'industrie crypto/*blockchain* pendant la crise du Covid-19, juin 2020, disponible à https://adan.eu/rapport/industrie-crypto-*blockchain*-crise-covid-19, consulté le 17/09/2021

[92] Assemblée Nationale, *Amendement n°227, projet de loi relatif à la transparence*, à la lutte contre la corruption et à la modernisation de la vie économique (N°3785)

[93] VABRES R., *Bons de caisse, minibons, blockchain…résurrection ou révolution*, Revue droit des sociétés 2016, repère n°7 - NB : à l'heure actuelle, un décret en Conseil d'État est censé venir préciser le régime de telles opérations ; DE VAUPLANE H., *Financement des entreprises par la blockchain*, RTDF 2016, n°2, p64 / CREMERS T., La *blockchain* et les titres financiers, Bulletin Joly Bourse 2016, 271

[94] D'un point de vue financier, en particulier s'agissant de la régulation des token, l'Europe a pu d'ores et déjà produire plusieurs pistes de réflexion (pour exemple : *Cryptocurrencies and blockchain, Policy Department for Economic, Scientific and Quality of Life Policies, July 2018* ou encore les récentes déclarations du Vice-Président de la Commission Européenne, tenues lors de la Digital Finance Outreach 2020, du 23 juin 2020.

[95] Décret n° 2019-1213 du 21 nov. 2019 relatif aux prestataires de services sur actifs numériques

Néanmoins, force est de constater que mise à part les premières régulations inhérentes au domaine financier[96], au sujet desquelles Me Hubert de Vauplane estimait que : « le régulateur aura un rôle de premier plan à jouer dans la surveillance de la non-falsifiabilité des chaines de consensus[97] » et que pour le professeur Yves Moreau, est plaidée une régulation internationale, qui pour lui serait la seule efficace[98], les seules tentatives de régulation actuelles ne portent que sur le domaine financier.

Il apparaît que la régulation de la *blockchain* en elle-même n'est pas souhaitable car déconnecté des applications auxquels elle peut répondre. De surcroît, réguler une technologie en tant que telle, de manière déconnectée de ses possibilités reviendrait serait un non-sens, pour des raisons expliquées plus loin dans cette étude. Au contraire une régulation réfléchie sur différents éléments pouvant la composer, afin de justement permettre une démocratisation efficace de la *blockchain* sans en limiter les usages. Cette réflexion sur la régulation de la *blockchain* est en fait une véritable question sur la confiance que l'on peut accorder à une technologie. Se pose d'ailleurs ici la question des possibilités techniques et juridiques des solutions de chiffrement[99].

50. De manière prospective, la considération du recentrement et du renforcement de la confiance dans les technologies de l'information a tout intérêt dans une économie de la *data* ou encore économie de l'hyper-information[100] . Reprenant des concepts économiques de base, mais dans les théories économiques sur la notion même d'entreprise[101], la notion de confiance est actuellement dans ce que l'on pourrait nommer « nouvel âge d'or », au service de l'utilisation des données qui peut être faite par les différents acteurs concernés par elles. C'est l'attrait d'un protocole *blockchain*, décliné à la suite de ses premières applications financières

---

[96] MM. MARINI P. et MARC F., *Rapport d'information* n° 767 (2013-2014), fait au nom de la commission des finances, déposé le 23 juil. 2014, Recommandation du Conseil et annexe (lignes directrices régissant la sécurité des systèmes d'information), 26 nov. 1992

[97] DE VAUPLANE H., *Blockchain : la question de la preuve par consensus au cœur de la gouvernance*, Revue Banque, n°796

[98] Pr. MOREAU Y, Université de Leuven, Belgique, lors du colloque « Le Gig Bang *Blockchain* », 14 janvier 2016, https://*blockchain*france.net/2016/02/02/la-place-de-letat-et-du-droit-dans-la-*blockchain*/, (consulté le 02/02/2017).

[99] Cf. *Infra*, p.203 et suiv.

[100] BETBÈZE J-P. *Les 100 mots de l'économie*, 2019, collection « Que sais-je », PUF.

[101] CJCE, 23 avr. 1991, aff. C-41/90, Höfner et Elser, ECLI:EU:C:1991:161, pt. 21 ; la notion d'entreprise ainsi retenue par la CJCE met en avant la dichotomie nécessaire pour le fonctionnement d'une entreprise, à savoir la confiance placée dans le dirigeant d'entreprise, chargé d'équilibrer le fonctionnement interne de l'entreprise avec les contraintes externes, à savoir celles du Marché. Pour M. Brunelle (précité) la *blockchain* invite à la réflexion quant au concept d'entreprise, la frontière entre ces intérêts dichotomiques étant potentiellement gommées par l'utilisation d'une technologie reposant sur l'absence de tiers de confiance.

(*Bitcoin* en premier lieu). Pour rappel, l'utilisation du pluriel dans la notion de nouvelles économies de la confiance permet de mettre en avant les attraits d'une technologie permettant la sécurisation et le partage d'informations non rivales tout en permettant de s'assurer de leur traçabilité (et donc de s'assurer de leur modification ou non modification). Dans une mesure à vocation plus administrative, certaines institutions ont pris en compte les intérêts d'une telle technologie, sans pour autant attendre une régulation complète de la part du législateur. Ce qui peut être un comportement à reconnaître et à encourager dans une certaine mesure.

L'un des exemples de la prise en comptes des intérêts de la *blockchain,* notamment au service d'une meilleure administration de la justice[102], se trouve pour un registre public en particulier. La tenue du RCS appartient au Tribunaux de Commerce. Ce registre public a pour objet de favoriser la rapidité et la sécurité de la vie des affaires, un véritable état civil officiel et commercial des entreprises. Il présente des caractéristiques importantes, au service de la rapidité et de la sécurité de vie des affaires (par exemple, l'inscription au RCS confère la personnalité morale aux entreprises), et est ainsi un vecteur primordial de l'information des tiers. Il est dénombré aujourd'hui 134 tribunaux de commerce en France, au sein desquels les échanges peuvent prendre de nombreuses formes, allant du recommandé, au courriel, au coffre-fort électronique.

L'organisation hétéroclite de ces différents greffes, que ce soient leurs systèmes d'information, ou l'utilisation de canaux de communications disparates, l'information ne circule pas toujours à la même vitesse, également, les différents vecteurs de sécurité, auxquels le RCS doit répondre.

51. Dans une seconde approche, il est à noter de profonds et actuels changements dans la vie économique des entreprises, ainsi que l'importance d'accéder à une information rapidement, et surtout de manière fiable. Prenons une situation simple ; une société commerciale souhaite ouvrir un second établissement, en dehors de son ressort habituel (une société Nancéienne souhaitant ouvrir un établissement en Dordogne). De manière schématique, cette société devra faire état de l'ouverture de cet établissement auprès du RCS de Bergerac, notamment en vue de l'information des tiers.

[102] LABBE T., *L'état au défi des blockchains, régulations (s) et usages publics de la technologie blockchain,* RFPI, numéro spécial, fév. 2021

En pratique, plusieurs modes de transmission de cette information peuvent être envisagés, tels qu'un télé-service, ou la transmission d'informations par courrier. Or, ces modes de communication présentent souvent des lacunes (un site internet non sécurisé, la perte d'un courrier, etc.). C'est pour remédier à ces problématiques, tout en garantissant une rapidité de traitement de l'information qu'un POC[103] a eu pour but d'établir le réseau suivant :

- Chaque greffe sera considéré comme mineur et comme utilisateur du réseau *blockchain* permissioné ;

- Dès lors, aucune autre entité autre que les différents greffes inscrits en tant que tels auront la qualité de mineur et pourront agir en écriture sur le réseau ;

- Dès qu'une information devra être partagée, le greffe 1 soumettra celle-ci au réseau ainsi mis en place ;

- L'information, une fois vérifiée, sera mise à la suite d'autre, qui fera l'objet de validation de la part de l'ensemble des mineurs ;

- Une fois le consensus informatique atteint, l'information sera répertoriée et dupliquée auprès de l'ensemble des mineurs, soit l'ensemble des greffes, dans des délais extrêmement rapides ;

- Toute modification ultérieure devra ensuite faire référence aux précédentes informations.

L'apparition de technologies qualifiées ou potentiellement qualifiées de disruptives mettent à mal nos conceptions et application de la logique juridique classique « objet/régime applicable ». Or, la question de la brevetabilité d'une *blockchain*, en la mettant en perspective avec les notions d'innovation [104] et d'invention [105] - corollaires de cette question de brevetabilité - paraît indissociable d'une étude de la réaction du droit face à des technologies.

---

[103] Un *POC* ou *Proof-of-Concept*, est une démonstration de faisabilité, une réalisation ayant pour vocation de montrer la faisabilité d'un procédé ou d'une innovation (pour plus d'informations : https://fr.wikipedia.org/wiki/Preuve_de_concept, consulté le 20/10/2021).

[104] MOULIN F., *Innovation et invention, comparaison du point de vue juridique*, janv. 2010 disponible à http://hal.grenoble-em.com/hal-00451615/document

[105] Pour rappel, le terme « invention », en occultant le rapport avec la notion de trésor, est « la découverte d'une nouveauté scientifique », CORNU G., *Vocabulaire juridique*, précité.

Rappelons que la *blockchain*, dans une conception, ici retenue, d'œuvre complexe, amène à une détermination éclatée des différents régimes applicables, sans réussir, *de facto*, à une harmonisation parfaite de ces régimes. La question de la brevetabilité de l'élément logiciel devient ainsi fondamentale pour parvenir à une étude plus exhaustive de cette technologie, notamment compte tenu de l'aspect financier relatif à la protection d'une telle technologie, mais reste témoin de l'éclatement du cadre applicable aux nouvelles technologies.

52. Il est ainsi démontré, de manière empirique, que la *blockchain* a permis un affranchissement des lignes étatiques sur la question de la gestion monétaire - à tort ou à raison - plaçant l'informatique et de pures théories mathématiques devant une gestion étatique. Plaçant la question de la confiance au centre des échanges économiques plutôt que la mise en balances d'intérêts économiques, éclatant le cadre applicable, créant une extension complexe des différents cas d'applications d'une *blockchain*.

La question de la brevetabilité s'inscrit ainsi dans cet éclatement du cadre applicable, tout en demeurant essentielle compte tenu des éléments intrinsèques de la mise en place d'un protocole *blockchain*.

Section 2 : Une validité contestable du monopole économique du brevet d'une *blockchain*

53. Le développement d'une révolution numérique[106] reliée au caractère essentiel de l'outil informatique dans le développement économique des entreprises, induit la recherche d'une protection efficace en termes d'innovation informatique.

Ce domaine de l'innovation est particulièrement vaste au sein de l'informatique ; qu'elle porte sur l'amélioration de moyens de communication, ou la collecte toujours plus massive de données[107], ou encore la sécurisation des échanges électroniques. La technologie

[106] La notion de « révolution numérique » peut comporter plusieurs éléments de définition, dont la combinaison des notions de « révolution » et de « numérique » peut poser des questions d'ordre informatique ou même philosophiques. En France, il est possible de trouver la plus ancienne occurrence de cette expression dans la revue Sciences et Avenir, n°95, du 1er déc. 1993.
https://fr.wikipedia.org/wiki/R%C3%A9volution_num%C3%A9rique#cite_note-8 (consulté le 08/09/2018)

[107] Dans le cadre de la présente étude, ne seront pas abordés les concepts de *big* data, les laissant à notamment BOUGEARD A., doctorant CEIPI.

blockchain demeure une réponse - parmi d'innombrables autres - à la sécurité des échanges électroniques, doublée d'une décentralisation de ces échanges, avec, pour promesse, une amélioration ostensible de la gestion de différents réseaux informatiques. Avant tout, l'innovation induit une prise de risque financier. En témoigne au sein de la propriété littéraire et artistique, la consécration de plusieurs régimes dédiés aux investisseurs[108] (régime de protection du producteur de phonogrammes ou de producteurs de bases de données par exemple). Au sein de la propriété industrielle, cette protection est assumée, plaçant le brevet comme outil majeur de l'économie[109]. D'où l'intérêt, pour la personne assumant ce risque financier, de vouloir protéger ses investissements contre une exploitation lui causant un préjudice financier.

La protection de l'investissement réalisé lors de l'élaboration d'un projet *blockchain*, donc mettant en œuvre notamment un logiciel et une base de données spécifiques, induit nécessairement une recherche des différents régimes applicables, en suivant une logique de protection distributive, entérinée notamment par l'apport de l'arrêt *Cryo*[110].

Pour reprendre une analyse de ce type, il convient de rappeler une nouvelle fois qu'une *blockchain* ne peut être résumée à un seul élément, pris dans sa conception de protocole informatique, mais doit être analysée comme une somme, une œuvre complexe « qui ne saurait être réduite à sa seule dimension logicielle, quelle que soit l'importance de celle-ci, de sorte que chacune de ses composantes est soumise au régime qui lui est applicable en fonction de sa nature[111] ».

54. Il est ainsi possible de retenir plusieurs éléments centraux : une base de données, un logiciel, un savoir-faire spécifique. Une *blockchain* ayant notamment pour trait la création et l'alimentation d'une base de données décentralisée, doublée du fait qu'il s'agisse de ce que l'on peut nommer une nouvelle technologie (dans le sens où il s'agit d'une technologie en cours de démocratisation), induit un poids conséquent en termes d'investissement, aussi bien informatiques, humains ou financiers. Justifiant une recherche constante de méthodes de protection optimisées, invitant à la question particulière de la protection dudit logiciel.

---

[108] EDELMAN B., *La propriété littéraire et artistique*, 2008, PUF
[109] GAY C., *Management de l'innovation,* Dunod, 2017, *pp.47-48*
[110] Cass, 1ère Civ., 25/06/2009, précité
[111] *Ibid.*

Si l'étude des méthodes de protections reliées aux régimes de propriété littéraire et artistique, en particulier s'agissant de la protection des bases de données créées, alimentées, ou encore gérées par une *blockchain* (privée, publique ou hybride), seront étudiées dans le cadre de la présente étude[112], et que la protection du savoir-faire relève notamment du secret des affaires[113], la potentielle protection au titre du droit des logiciels appelle nécessairement une étude particulière, à savoir le débat sur la brevetabilité du logiciel. Cette étude particulière devant s'inscrire (ou s'exclure) au bénéfice des développements postérieurs présents dans cette étude[114].

55. Par ailleurs, l'attrait de l'étude de la brevetabilité d'un protocole *blockchain* paraît indispensable tant la protection accordée par un titre de propriété industrielle est considérée importante, économiquement parlant, et surtout redoutable (aussi bien à un niveau contractuel qu'à un niveau contentieux). Le brevet représentant un investissement et une méthode de protection plus laconique (présence d'un dépôt auprès de l'INPI en France, durée de validité, simplicité - apparente - de valorisation et de défense) qu'une protection au titre de la propriété littéraire et artistique.

Au surplus, cette partie d'étude illustre le caractère hétérogène de l'appréciation faite de la technologie *blockchain*, et il s'impose de pouvoir l'étudier, même s'il peut en ressortir une exclusion de l'applicabilité de ce régime de propriété industrielle. Nonobstant ces remarques liminaires, il convient également de préciser que la présente étude se bornera volontairement à une étude de la brevetabilité d'un protocole *blockchain* « seul », c'est-à-dire utilisé de manière autonome, sans appui d'autres méthodes ou technologies. Par exemple, pourraient visées ici les méthodes algorithmiques ou autres utilisations de l'intelligence artificielle - forte ou faible - utilisées conjointement avec une *blockchain*, même si ces méthodes particulières feront l'objet de quelques développements. Cette remarque portant parfaitement sens car les attraits de l'utilisation d'une *blockchain* avec l'exploitation de données médicales, recoupées par un algorithme en matière de santé pourraient être facilement démontrables même s'ils seraient hors de propos ici.

---

[112] *Cf. Infra, p.139 et suiv.*

[113] À ce titre, la loi n° 2018-670 du 30 juil. 2018, qui transpose la directive n°2016/943/UE du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués. Pour un premier aperçu sur la notion, cf. Secret des affaires, Fiches d'orientation, juil. 2019, Dalloz.

[114] cf. Titre 2 : Application sémantique des régimes de propriété littéraire et artistique

56. Revenant ainsi à une étude de la brevetabilité en quatre points. Si le premier point porte sur les exclusions préalables à une brevetabilité d'une *blockchain* (§1), nécessaires pour circonscrire l'applicabilité ou non du brevet à la *blockchain*, conduit à une application inadéquate des critères retenus dans le cadre de la construction du brevet par le droit national et européen (§2). Néanmoins, le caractère technique discutable d'une *blockchain* (§3) peut inviter à considérer les brevets d'ores et déjà déposés sur des projets *blockchain*[115], conduisant à explorer des incertitudes parasites restantes (§4).

§1 : Les exclusions préalables d'une brevetabilité d'une *blockchain*

57. De manière préalable, toute approche de la brevetabilité d'une *blockchain* doit prendre en compte les spécificités des régimes de propriété industrielle. L'approche classique du domaine de la brevetabilité, avant même de déterminer les critères de brevetabilité, induit de préciser différents cas d'exclusion des *blockchain*s, et donc ici de logiciels, utilisés dans les domaines thérapeutiques, chirurgicaux, ou de diagnostics, ou encore celles contraires à l'ordre public ou aux bonnes mœurs[116], malgré un développement actuel de différentes utilisations de *blockchain* dans le domaine de la santé[117]. Étant toutefois noté que les principales applications de la *blockchain* dans le milieu de la santé sont en premier lieu des applications des capacités de registre et de traçabilité des données de santé. Enfin, une partie de la présente étude sera également centrée sur l'utilisation d'une *blockchain* (logiciel) dans le domaine du vivant (les procédés microbiologiques, le corps humain, les races animales ou encore les variétés végétales). En particulier, seront étudiées les exclusions prises dans une approche prenant en compte le développement de solution logicielles permettant l'amélioration de la connaissance médicale et thérapeutique, en tant que solution visant particulièrement à devenir un domaine thérapeutique, chirurgical ou de diagnostic, en tant qu'objectif réel.

De manière pragmatique, la composante logicielle d'une *blockchain* a principalement pour but d'assurer l'inscription en bloc ou encore les moyens de communication et d'enregistrement des données entre les différents mineurs, ainsi, même s'il parait hautement

---

[115] Cf. *Infra*, note n°153

[116] Art. L611-17, CPI

[117] Pour des exemples d'application dans le domaine de la santé : BOBÉE F., *Blockchain et santé : présentations et cas d'usages*, Bitconseil, 3 juil. 2019, disponible à https://bitconseil.fr/*blockchain*-sante-presentation-cas-usage/ (consulté le 20/05/2019).

improbable d'inclure une couche logicielle spécifique pour laquelle la protection au titre du brevet serait recherchée. Cette même recherche de protection pourrait se réaliser pour l'ensemble des éléments d'une *blockchain* en ce qu'elle pourrait porter sur des applications couvertes potentiellement par le brevet. Dit autrement, étudier la brevetabilité d'une *blockchain*, revient à étudier le seul axe possible de brevetabilité d'une *blockchain* grâce à sa dimension logicielle, considérée comme porte d'entrée vers le brevet. Les exclusions seront ainsi étudiées d'une part à travers celles portant sur les traitements thérapeutiques et méthodes de diagnostic (A), et d'autre part les exclusions liées aux bonnes mœurs et à l'ordre public (B).

A/ Les exclusions liées aux traitements thérapeutiques, méthodes de diagnostic

58. De manière générale, l'article L. 611-16 du CPI dispose : « Ne sont pas brevetables les méthodes de traitement chirurgical ou thérapeutique du corps humain ou animal et les méthodes de diagnostic appliquées au corps humain ou animal. Cette disposition ne s'applique pas aux produits notamment aux substances ou compositions, pour la mise en œuvre d'une de ces méthodes ».

De manière complémentaire, peut être cité un arrêt de la Cour d'appel de Paris, en date du 29 octobre 1997[118], retenant que les méthodes de traitement chirurgical ou thérapeutique comme : « un ensemble de démarches raisonnées, suivies et reliées entre elles, émanant de l'homme du métier destinées à parvenir à la découverte des moyens de prévenir, de traiter, de soulager, de dissiper ou d'atténuer les symptômes d'un trouble résultant d'une affection ou d'un dysfonctionnement du corps humain ou animal, ou de le guérir ». Concernant les méthodes de diagnostic, la décision T385/86 du 25 septembre 1997[119], précise que « seules doivent être exclues de la brevetabilité, en tant que méthodes de diagnostic, les méthodes dont le résultat permet directement de prendre une décision au sujet d'un traitement médical. Pour savoir si une méthode constitue une méthode de diagnostic au sens de l'article 52(4), première phrase CBE, il y a donc lieu de vérifier si la méthode revendiquée comprend effectivement toutes les étapes dont l'exécution est nécessaire à l'établissement d'un diagnostic médical. Les méthodes qui fournissent uniquement des résultats intermédiaires ne constituent pas encore

[118] CA Paris, 4e ch., 29 oct. 1997, « Biolase Technology Inc. », PIBD 1998, n°646, III, p30.
[119] OEB, 25 sept. 1987, T385/86, JO OEB 1988, p308.

des méthodes de diagnostic au sens de l'article 52(4), première phrase CBE, même si elles peuvent servir à poser un diagnostic ».

En dépit de faits d'espèce applicables, il peut en ressortir ainsi une apparente exclusion de protection d'une *blockchain* (prise dans sa dimension logicielle) par le brevet si tant est que cette *blockchain* soit utilisée dans des conditions conformes aux développements précédents.

B/ Les exclusions liées aux bonnes mœurs et à l'ordre public

59. Concernant les inventions contraires aux bonnes mœurs et à l'ordre public non susceptibles de protection (industrielle, littéraire ou artistique), l'exclusion de toute brevetabilité à ce titre figure au sein de l'article L.611-17 du CPI (modifié par la loi du 6 août 2004[120]), qui dispose : « Ne sont pas brevetable les inventions dont l'exploitation commerciale serait contraire à la dignité de la personne humaine, à l'ordre public ou aux bonnes mœurs, cette contrariété ne pouvant résulter du seul fait que cette exploitation est interdite par une disposition législative ou réglementaire », sachant que la notion d'ordre public sera prise dans son sens le plus général, tel qu'il est possible de le retrouver dans tout dictionnaire juridique, l'ordre public étant « pour un pays donné, à un moment donné, l'état social dans lequel la paix la tranquillité et la sécurité publique ne sont pas troublées[121] ».

S'agissant des difficultés liées à l'appréciation des bonnes mœurs, il est possible de retenir de manière résumée qu'elle « expriment finalement (…) un point d'équilibre nécessaire entre la liberté individuelle et l'organisation des relations sociales[122] ».

60. S'agissant des difficultés liées à l'appréciation de la notion de l'ordre public, notion habituellement associée aux bonnes mœurs, et pour reprendre la conception traditionnelle de Hauriou[123], elle-même inscrite dans l'article L2212-2-1 du Code général des collectivités territoriales, l'ordre public comprend notamment la sûreté et la sécurité (sécurité physique des personnes et/ou intégrité matérielle des biens), ou encore la tranquillité publique. Il est également possible de citer deux arrêts particulièrement importants pour la construction

[120] Loi n°2004-800 du 6 août 2004 relative à la bioéthique

[121] G. CORNU, *Vocabulaire juridique*, précité.

[122] FENOUILLET D., *La loi, le juge et les mœurs : la Cour de cassation aurait-elle emménagé rive gauche ?*, RDC 2005. 1284

[123] HAURIOU M., *Précis de droit administratif et de droit public*, 1re édition 1892, rémiz. Dalloz 2002

extensive de cette notion, à savoir les arrêts « Communes de Morsang-sur-Orge[124] » et « Société Films Lutécia[125] », permettant à l'ordre public d'avoir un corollaire au sujet de la dignité humaine et de la moralité publique. Également, dans une logique propre au brevet, peut être cité un arrêt de l'OEB[126] et un de la Cour de cassation[127].Ces notions ainsi rappelées, il faut prendre note que la dimension logicielle d'une *blockchain* ne pourrait pas bénéficier d'une protection par le brevet en cas d'atteinte à l'ordre public ou aux bonnes mœurs.

C/ Les exclusions liées corps humain, aux obtentions végétales et aux races animales

61. Conformément aux exclusions formulées par le CPI, confortée notamment par la jurisprudence de l'OEB, l'existence de l'exclusion de la brevetabilité liées au corps humain, aux variétés végétales et aux races animales est premièrement rappelée par ce même Code. L'article L611-18 al. 2 du CPI[128] dispose que « Seule une invention constituant l'application technique d'une fonction d'un élément du corps humain peut être protégée par brevet », qui est en soi une nuance par rapport à la directive de 1998[129], excluant ainsi toute composante logicielle portant sur ces aspects de la protection de la brevetabilité.

La directive de 1998 prévoit également une interdiction visant les races animale, interdiction transposée au sein de l'article L611-19 du CPI, et cette interdiction a pu être reprise par une décision du 3 octobre 1990 par l'OEB**[130]**, qui précisait que les « brevets européens ne sont pas délivrés pour les procédés essentiellement biologiques d'obtention d'animaux ». La présente étude se bornera a rappelé que les variétés végétales possèdent un régime de protection propre[131], et qu'en l'état de la présente étude, et surtout en l'absence de décisions sur ce sujet, il n'est pas opportun d'en faire une application à la dimension logicielle d'une *blockchain*.

62. Cette appréciation conduit à rappeler les éléments d'applicabilité du régime de protection par brevet, positivement ou négativement, vis-à-vis du logiciel, aussi bien pour une

[124] CE, ass., 27 oct. 1995, Cne de Morsang-sur-Orge

[125] CE, sect., 18 déc. 1959, Sté « Les films Lutétia »

[126] OEB, CRT, 21 févr. 1995, « Plant Genetics Systems », JO OEB 1995. 545 ; D. 1996. somm. 290, obs. MOUSSEON, SCHMIDT et GALLOUX.

[127] Cass. Com., 29 mars 2011, n°10-12.046, Propr. intell. 2011, no 40, p. 325, obs. SABATIER

[128] Art. L611-18 al. 2, CPI, modifié par la loi n°2204-800 du 6 août 2004 relative à la bioéthique, transposant la directive communautaire n°98/44 du 6 juil. 1998 relative à la protection juridique des inventions biotechnologiques

[129] Directive n°98/66 du 6 juil., précitée

[130] OEB, 3 oct. 1990, JO OEB 1990, p.476

[131] https://www.inpi.fr/fr/comprendre-la-propriete-intellectuelle/les-autres-modes-de-protection/les-obtentions-vegetales (consulté le 02/07/2020)

construction de régime dans le cadre d'une dimension nationale qu'européenne, invitant ainsi au rappel du caractère technique d'un brevet mais mettant surtout en exergue le caractère dual du logiciel. À noter que si le caractère technique du brevet sera ici étudié, son caractère novateur du brevet comme condition d'accessibilité de protection ne sera pas envisagé, partant du postulat que la présente étude appréhende la technologie *blockchain* en tant que technologie disruptive et donc par essence novatrice.

§2 : Une application inadéquate de la construction du brevet à la *blockchain*

63. La potentialité de la protection d'une *blockchain* par le brevet, une fois les exclusions réglementaires rappelées doit suivre le schéma de construction national (A) mais également en prenant les réflexions retenues dans le cadre d'une construction européenne (B) afin d'en faire une correcte application.

A/ Construction nationale.

64. La potentielle protection du logiciel par brevet est présente régulièrement sur le devant de la scène juridique, et ce, depuis les années 1980. Il est possible de citer, à ce titre, la Convention de Munich du 5 octobre 1973, qui a exclu expressément la possibilité de breveter les programmes d'ordinateur ; solution reprise, dans une interprétation en faveur de cette conception, par la jurisprudence.

La Cour d'appel de Paris, dans un arrêt en date du 2 novembre 1982 a ainsi pu retenir que « l'élaboration d'un programme d'ordinateur est une œuvre de l'esprit originale dans sa conception et son expression allant au-delà d'une simple logique automatique et contraignante ; il ne s'agit pas d'un mécanisme intellectuel nécessaire : en effet, les analystes programmeurs ont à choisir, comme les traducteurs d'ouvrages, entre divers modes de présentation et d'expression et leur choix porte ainsi la marque de leur personnalité ».

La notion de programme d'ordinateur est une notion qu'il est possible de retrouver dès le Code de la propriété intellectuelle[132], et généralement, on trouve plus facilement cette notion

[132] Art. L610-10, CPI

dans les textes, qu'il s'agisse de l'accord ADPIC de 1994[133] ou encore dans le traité de l'OMPI de 1996[134], et habituellement, il conviendrait d'utiliser cette notion plutôt que de logiciel. Si la nuance existe, par commodité de langage, les deux termes seront utilisés ici sans distinction. Cette jurisprudence pouvant s'expliquer notamment par le fait que l'on peut considérer le langage informatique comme une typologie de langage propre ; un langage créé par l'homme pour la machine, et qu'à ce titre, il peut être considéré comme empreint de personnalité. D'autres éléments de réflexion invitent également à considérer le logiciel, en particulier dans son expression informatique, comme une composante de méthodes mathématiques, exclues de toute brevetabilité[135].

65. Toutefois, un arrêt de la Cour d'appel de Paris, en date du 4 juin 1984, pris en application de la loi du 11 mars 1957, vient contrecarrer l'analyse précédente ; en effet, il a été retenu que « on ne saurait assimiler à une œuvre de l'esprit la création de logiciels, qu'il s'agisse du concept ou des analyses, même lorsque ces derniers ont pour objet l'élaboration d'un jeu[136] ».

Cette lecture nouvelle de la protection des logiciels par le juge, dans une époque marquée, il faut le rappeler, par le lancement, quelques mois plus tôt du premier Macintosh[137], induit une incertitude sur la protection applicable au logiciel. Toutefois, la loi du 3 juillet 1985 instaura un compromis, aussi bien politique qu'économique, en instaurant une protection du logiciel au titre des œuvres de l'esprit.

66. Ce compromis ayant été entériné par l'Assemblée Plénière de la Cour de cassation en rendant trois arrêts en ce sens, en date du 7 mars 1986[138] ; par ces arrêts, la Cour rappelle les critères de l'originalité applicables au logiciel, composants essentiels de la propriété littéraire et artistique, faisant entrer le logiciel, en tant que tel, dans le champ de protection de la propriété littéraire et artistique, et non pas dans celui de la propriété industrielle et donc du brevet. Cela étant, la dimension logicielle d'une *blockchain* semblerait aller contre une protection au titre du brevet.

---

[133] Accord ADPIC, 15 oct. 1994, cf. art. 10.1
[134] Traité de l'OMPI du 20 déc. 1996, cf. art. 4
[135] Art. 52, (2), CBE, Exclusion de la brevetabilité pour les méthodes mathématiques
[136] CA Paris, 4 juin 1984, JCP 3, 1985, p.88, note M. VIVANT
[137] 24 janv. 1984, lancement du premier Macintosh, remplaçant l'Apple II, par Apple Computer Inc.
[138] Arrêts du 7 mars 1986, RDPI 1986, n°3, pp.205-212

B/ Construction européenne

67. Dans un tel cadre, il convient de mentionner la Convention de Munich relative au brevet européen (CBE), qui a exclu les programmes d'ordinateur en tant que tels[139], position reprise par les différentes dispositions réglementaires en vigueur. Ces dispositions devant exclure ainsi la protection du logiciel par le brevet. Néanmoins, dans le cadre de la construction du régime de protection du logiciel par le droit du brevet, force est de constater la dualité entre deux courants, depuis les années 90 ; le premier, français, qui a pu exclure la protection du logiciel en tant que tel par le brevet, et le second, européen, chapeauté par l'influence de l'OEB[140], qui va l'accepter.

68. Pouvant être considéré comme pratique *contra legem*, l'OEB a développé cette pratique sur des motivations parfois « floues et volontairement obscures[141] » conférant une protection par le brevet au logiciel, même pris en tant que tel. Cette position, ayant déjà été critiquée[142], reste source d'ambiguïté, tant les directives internes de l'OEB rappellent que les programmes d'ordinateurs ne sont pas pour autant « exclus(s) de la brevetabilité par les articles 52(2) et (3)[143] ». Et récemment, l'OEB a de nouveau précisé sa position en rappelant que « les programmes d'ordinateur sont exclus de la brevetabilité en vertu de l'article 52(2)c) et (3) s'ils sont revendiqués en tant que tels. Cependant, conformément aux critères généralement applicables au titre de l'article 52(2) et (3) (G-II, 2), l'exclusion ne s'applique pas aux programmes d'ordinateur qui présentent un caractère technique[144] ».

69. Une nouvelle fois, dans une dimension applicable à la *blockchain*, la protection au titre du brevet semble être difficile d'accès en l'absence d'un caractère technique.

---

[139] Article 52 (2) CBE

[140] Office Européen des Brevets

[141] VIVANT M., Lamy Droit du Numérique, Section 4 - *La brevetabilité du logiciel, Wolters Kluwer* n°2714 et suiv.

[142] MACREZ F.., *Logiciel et brevetabilité : « Recherche clarté désespérément »*, RLDI 2019/51, n°1663

[143] Directives relatives à l'examen pratique, OEB, Partie G, Chapitre II-3

[144] Directives relatives à l'examen pratique, OEB Partie G, Chapitre II-15

§3 : Le caractère technique discutable de la *blockchain*

70. Précision sémantique oblige, l'utilisation de cette expression peut faire comprendre que le « législateur n'a pas voulu exclure toutes les inventions qui incorporent des parties de programmes d'ordinateur[145] », conforté par la jurisprudence[146]. Ainsi, l'étude de ce caractère technique parfait indissociable de l'application du régime de protection du brevet au logiciel, car si le logiciel est exclu du brevet en tant que tel, le logiciel en tant que composante apparaît comme concerné par le droit des brevets, au nom de son caractère technique.

D'un point de vue européen, l'OEB, s'agissant du programme d'ordinateur, retient également comme fondamental son caractère technique pour accéder au statut d'invention et donc être éligible au brevet, à un point que la Grande Chambre de l'OEB a pu rappeler**[147]**. Confortant ainsi la position de l'OEB *contra legem* d'accepter la protection au titre du brevet pour le logiciel.

71. D'un point de vue français, le CPI reste clair : « Sont brevetables, dans tous les domaines technologiques, les inventions nouvelles impliquant une activité inventive et susceptibles d'application industrielle **[148]** » La recherche du caractère technique pour l'obtention d'un brevet est fondamentale, au point de déterminer ce qui reste brevetable ou non. Cette position a pu notamment être reprise par la jurisprudence**[149]**, mettant en avant ce fondement. Cet arrêt a d'ailleurs l'intérêt d'aborder la question des bases de données, le rattachant ainsi plus facilement à l'objet de notre présente étude de la *blockchain*. La jurisprudence avait d'ailleurs retenu que « considérant qu'il résulte de ces éléments que l'invention consiste dans la présentation d'une méthode intellectuelle de recherche d'informations selon un procédé de combinaison de mots-clés et de catégories qui n'est pas caractérisé techniquement de sorte qu'elle n'est pas brevetable**[150]** ». Imposant ainsi le caractère technique comme condition d'accès au brevet. Cette position ayant comme résultat d'arriver

---

[145] DRILLON S., *La protection des logiciels par brevet d'invention*, Thèse Droit, Université de Strasbourg, 2012, voir également MACREZ F., *Créations informatiques : bouleversement des droits de propriété intellectuelle ? Essai sur la cohérence des droits*, collection CEIPI, 2011, Lexisnexis

[146] Voir notamment : OEB, T1171/97, 17 September 1999, et T121/06, 25 janv. 2007

[147] OEB, gde ch. rec., 12 mai 2010, G3/08, JOOEB 2011, p. 10 ; Propr. intell. 2011, n^{o} 39, p. 243, obs. Warusfel

[148] Art. L611-10, Code de la propriété intellectuelle

[149] CA Paris, pôle 5, 2^{e} ch., 16 déc. 2016, JurisData n^{o} 2016-027594

[150] *Ibid*.

à la même position que l'OEB pour les programmes d'ordinateurs faisant partie d'une solution technique. La Cour d'appel de Paris a pu prendre la position suivante : « il convient d'apprécier si au-delà de la formulation adoptée, la revendication prise dans son ensemble, porte sur un programme d'ordinateur revendiqué en tant que tel (…) Le fait que les différents moyens compris dans la combinaison revendiquée soient mis en œuvre par un ou plusieurs logiciels, n'est dès lors pas un motif d'exclusion au sens de l'article L.611-10[151] », invitant ainsi à une lecture *a contrario* signifiant que le programme d'ordinateur, s'il est partie d'une solution technique dont le caractère technique est démontrable, peut alors prétendre à une protection au titre du brevet. Ainsi, et par exemple, une *blockchain* utilisée dans un « couple matériel-logiciel[152] » pourrait faire l'objet d'un brevet.

72. Ces réflexions appliquées à un protocole *blockchain*, pris pour sa seule dimension logicielle peuvent alors exclure la *blockchain* de toute brevetabilité. Toutefois, la pratique démontre que des brevets sur des *blockchains* existent d'ores et déjà[153], qu'ils soient déposés dans une logique défensive (dans un but de protection d'intérêts internes) ou dans une logique agressive (au point de réaliser des *patents troll*[154]). En reste que si la pratique permet ce dépôt, ce n'est pas sans soulever d'importantes questions de validité ou d'exploitation, en particulier compte tenu du caractère technique de la *blockchain* imposant une réplication du protocole à une échelle potentiellement internationale (posant ainsi des questions l'application du principe de territorialité du brevet)[155].

73. Néanmoins, il ne nous semble pas que l'appréciation d'une technologie disruptive ne peut correctement se faire sans une approche globale et non déconnectée des différents éléments la composant. Cela étant, l'appréciation d'un protocole *blockchain* est dès lors d'autant plus complexe, et la lecture de la jurisprudence (française ou européenne) ainsi que de la littérature laisse planer des doutes toujours aussi insaisissables sur la potentielle brevetabilité d'une *blockchain* en raison de plusieurs incertitudes, non exhaustives tout en

---

[151] CA Paris, 4e ch. sect. B, 5 juin 2009, « Kone (venant aux droits de la SAS Ascenseurs Cierma) c. Jean-Patrick Azpitarte », PIBD 2009, n°903, III, p.1332

[152] MACREZ F., *Créations informatiques : bouleversement des droits de propriété intellectuelle ? Essai sur la cohérence des droits*, collection CEIPI, 2011, Lexisnexis

[153] Par exemple : brevet n°W02019098873 ; NB : au 17/10/2021, la base de données de l'INPI (data.inpi.fr), pour donner suite à son interrogation via le mot-clé « *blockchain* » récence 549 brevets.

[154] Dans le domaine de propriété intellectuelle, le *patent troll* est une entreprise dont l'activité principale est de se constituer un portefeuille de brevets dans le seul but d'en tirer profit au biais d'une licence ou d'un contentieux.

[155] BARBET-MASSIN A., KHATAB A., *Les « brevets blockchain » : état des lieux et perspectives, 2018*, Expertises, 435, p.176

semblant accepter la brevetabilité d'un logiciel d'une *blockchain* en présence d'un caractère technique de ce dernier, comme put en témoigner l'actuelle pratique de l'OEB sur cette question[156].

§4 : Les incertitudes parasites restantes

74. En l'état de la réglementation nationale applicable, compte tenu des développements liés aux constructions nationales et européennes du brevet, la *blockchain* n'apparaît pas comme facilement brevetable. Néanmoins, des incertitudes demeurent, d'une part lors qu'une *blockchain* est considérée comme élément essentiel d'un ensemble brevetable (A), et d'autre part, en tant que protocole informatique reposant sur des composants algorithmiques importants, la question de l'algorithme peut également demeurer (B).

A/ La *blockchain* comme élément essentiel d'un ensemble brevetable

75. La dimension logicielle d'une *blockchain* est en fait partie d'une solution technique plus vaste, comprenant - pour rappel - plusieurs éléments, et ses applications étant diverses et variées, certaines utilisations de *blockchain* sont réalisées dans le cadre de solutions techniques pure, par exemple le cas des serrures connectées[157]. En ressort alors une *blockchain* non pas prise pour sa seule dimension logicielle mais considérée comme un procédé qui lui peut être concerné par une potentielle brevetabilité, comme cela a pu être retenu, par exemple, dans un arrêt « Schlumberger[158] », malgré une réaffirmation de l'exclusion de la protection du logiciel par le brevet par un arrêt plus récent[159]. Force est de constater une application des débats actuels autour de la protection du logiciel, comme élément essentiel d'un ensemble brevetable, par le brevet, pour une *blockchain*. La prudence conduirait, dans une approche purement pragmatique, de rechercher dans une étude préalable (et construire dans le cadre d'une stratégie de protection des actifs immatériels) de rechercher une telle protection au nom de l'utilisation d'une *blockchain* dans un ensemble brevetable.

---

[156] OEB, *Talking about a new revolution : blockchain*, Conference report, dec. 2018, disponible à https://www.epo.org/news-events/news/2019/20190314_fr.html

[157] Cf. projet « slock.it », précité

[158] CA Paris, 15 juin 1981, PIBD 1981, n° 285, III, p. 175 et PIBD 1983, n° 318, III, p. 45

[159] TGI Paris, 3e ch., 1re sect., 18 juin 2015, n° 14/05735

B/ La question de l'algorithme

76. Outre la définition classique exprimée précédemment[160], un algorithme peut être également vu comme une suite finie et non ambigüe d'opérations ou d'instructions permettant de résoudre une classe de problèmes[161]. La question de la brevetabilité d'une *blockchain* prise pour sa composante algorithmique n'est pas dénudée d'intérêt dans le sens où l'algorithme de consensus nécessaire pour l'établissement d'un protocole *blockchain* va conditionner ses performances mais aussi ses applications. Par exemple, l'algorithme de consensus de la *blockchain Bitcoin* permet un enregistrement d'un nouveau bloc de données toutes les 10 minutes environ (et environ une transaction toutes les 7 secondes, là où la *blockchain* Ethereum valide un bloc toutes les 15 secondes environ (et approximativement 20 transactions par seconde)[162]. Cette différenciation de vitesse d'exécution ayant pour effet que *Bitcoin* est principalement utilisé pour effectuer des transferts d'actifs là où la *blockchain* Ethereum pourra être utilisée notamment pour soutenir des *smart contracts*.

La conception d'un nouvel algorithme, même s'il reste avec une fonctionnalité identique aura des caractéristiques techniques différentes, et pour reprendre les développements précédents, pourra faire l'objet d'une protection par le brevet. Dès lors, une *blockchain* possédant un « nouvel algorithme », présentera, sous condition de présence du caractère technique, une possibilité pour la brevetabilité.

77. Sur l'articulation potentielle des protections, l'étude de la brevetabilité d'un protocole *blockchain* permet de mettre en avant la complexité de cet objet composite, dont l'essence même est d'articuler plusieurs composantes différentes (logiciels, base de données, etc.). Logiquement, la question de l'articulation des protections dans cette approche technico-économique revêt un intérêt intellectuel particulier. Autant la question de la brevetabilité ne peut être en l'état tranchée (notamment parce qu'il ne s'agit pas du but de la présente étude), autant la question de la potentielle articulation des protections ne doit pas être mise de côté tant elle a son importance notamment économique.

[160] Cf. note n°17

[161] https://fr.wikipedia.org/wiki/Algorithme#cite_note-1, consulté le 10/01/2020

[162] https://www.ig.com/fr/trading-cryptomonnaies/comparaison-des-cryptomonnaies, consulté le 10/01/2020

Comme a pu le rappeler Franck Macrez, « le choix des mots n'est pas neutre : articuler des droits ne revient pas à les cumuler[163] ». Compte tenu du principe de non-cumul des protections, l'articulation des différentes protections revêt un atout économique intéressant quand il s'agit de développer et promouvoir des technologies dites disruptives. L'investissement, aussi bien matériel qu'humain, ne peut se réaliser sereinement sans protection adéquate des différentes productions.

Ces propos relatifs à l'articulation sont d'ailleurs à ajouter à la préconisation d'établir une méthodologie distributive pour l'appréhension des différents objets de droits[164], notamment pour parvenir à une application correcte des nombreux régimes. Cette même méthodologie conduit à concevoir le logiciel comme à la fois œuvre de l'esprit (tel qu'assimilé par le droit positif français) mais aussi comme invention (en tant que sujet d'une protection par le brevet), pouvant donner ainsi le statut de « cumulard[165] » au logiciel. Néanmoins, si la dimension logicielle d'une *blockchain* apparaît comme potentiellement visée par ces deux types de protection (droit d'auteur et brevet), l'incertitude demeure tant certains courants de la doctrine ne conçoivent pas cette possibilité, en raison notamment du caractère purement fonctionnel du logiciel[166] que certains pans de la pratique, eux, continue à arguer sur la facilité de protection du logiciel par le brevet[167].

78. S'il ressort de la pratique actuelle certaines incertitudes sur la possibilité ou non de procéder au dépôt d'un brevet sur un logiciel, et donc, sur une *blockchain*, force est de constater que la démocratisation de cette technologie peut ne pas simplifier le débat, mais au contraire le complexifier compte tenu des applications hétéroclites d'une telle technologie.

---

[163] MACREZ F., *Logiciel : le cumulard de la propriété intellectuelle*, Thèmes et commentaires, Dalloz, 2011

[164] *Ibid*.

[165] *Ibid*.

[166] GAUDRAT P., *La protection des logiciels par le droit d'auteur : Bilan et perspectives*, RIDA oct. 1988, p. 77, no °19 et no °22.

[167] LEBKIRI A., *La propriété industrielle et la transformation numérique de* l'économie, Regards d'experts, INPI, 2015 disponible à https://www.inpi.fr/sites/default/files/2_1_extrait_pi_et_transformation_economie_numerique_inpi.pdf, consultés le 20/01/2020

Conclusion du Chapitre 1

79. La démocratisation de la *blockchain* depuis 2015 a créé l'explosion d'une « bulle *blockchain* », parallèle à la bulle internet des années 2000 ; le parallèle se poursuivant avec l'appréhension d'une technologie qui a pu bouleverser de nombreux secteurs économiques et même de nombreux cadres juridiques posés (par exemple, à travers l'essor du commerce électronique). Ces approches techno-économiques sont en fait le reflet des travaux qui ont pu être faits avec l'émergence d'Internet et tout l'ambiguïté des applications possibles de ce nouveau réseau mondial. Le caractère ambigu de la *blockchain* est notamment marqué par toutes ses utilisations potentielles, par exemple dans le cadre de *blockchain* conditionnant l'utilisation d'objet connectés ou pour l'utilisation de nouveaux moyens de paiements. Toutefois, cette complexité ne présente pas pour autant de difficultés, même pour des notions qui sortent d'un champ d'étude précis comme celui de la propriété littéraire et artistique. En effet, pour l'appréciation de la brevetabilité ou non d'une *blockchain*, la question se résoudra en premier lieu par rapport à l'usage qui sera fait du protocole en question, et le droit positif actuel nous invite d'ores et déjà à cette réflexion, qui sera réussie si une approche globale mais distributive est réalisée.

Toutefois, et à l'appui de ces approches techno-économiques, la *blockchain* ne peut se résumer à une transformation de simples aspects techniques ou financiers, la désintermédiation promise par la *blockchain* a nécessairement des impacts sur les rapports civils, entre personnes physiques ou morales.

Chapitre 2 : Transformations techniques subies des rapports civils

80. Illustré avec l'un des arguments les plus provocateurs de la *blockchain*, à savoir la suppression des tiers de confiance, la *blockchain* a le premier mérite de poser la question - à tendance quasi anarchiste[168] - de savoir si les tiers de confiance actuels sont nécessaires quand la technique permet de les remplacer avec un objet dénudé de risques de corruption ou de malversations. Plus loin encore, l'un des autres arguments présentés de la *blockchain* est sa capacité à être inaltérable, publique et surtout fiable, faisant ainsi de la *blockchain* l'instrument de preuve le plus parfait qui soit car ne dépendant même pas d'un officier ministériel pour avoir le caractère de « preuve suprême[169] ». Cette approche, désordonnée, car touchant à diverses branches du Droit reste nécessaire pour une appréciation efficace d'une telle technologie tant on peut lui attribuer la capacité d'apporter des éléments de révolutions juridiques. La *blockchain* possède sans conteste un potentiel pour transformer les rapports civils, pris dans leurs sens les plus élémentaires, à savoir leur démonstration (la preuve), et leur élaboration (les rapports contractuels). C'est pourquoi il convient de se pencher sur la validité de la *blockchain* face au droit actuel de la preuve (Section 1), entendu comme étant la « démonstration de l'existence d'un fait (matérialité d'un dommage) ou d'un acte (contrat, testament) dans les formes admises ou requises par la loi »[170]. Dans la lignée des actes juridiques, il semble logique d'étudier la modernisation des rapports contractuels (Section 2) permise par la *blockchain*, notamment grâce à l'apparition des *smart contracts*.

[168] L'anarchie est un état de fait d'une population dans laquelle aucune autorité ne s'exerce. À ce titre, l'exclusion de tout tiers de confiance, représentant l'autorité dans le bon fonctionnement des échanges étant l'un des fers de lance de la *blockchain*, on peut lui accorder ce qualificatif. G. CORNU, *Vocabulaire juridique*, précité.

[169] La notion de hiérarchie de preuve, pouvant placer l'acte authentique en tant que mode de preuve parfait, car attesté par un officier ministériel peut être considéré comme ayant une « faiblesse » par rapport à un écrit inscrit sur une *blockchain*, en effet, l'officier ministériel ne reste qu'un « tiers » à l'acte de base, alors qu'une *blockchain* évite justement l'intervention d'une personne autre que les parties en présence. Cette analyse n'étant, bien entendu, que l'un des arguments avancés par les communautés « pro-*blockchain* » et ne reflètent pas pour autant l'avis de l'auteur, pour des raisons exprimées ci-après.

[170] G. CORNU, précité.

Section 1 : Chamboulement des régimes de preuve face à la *blockchain*

81. De manière liminaire, il convient de faire une première précision, afin d'exclure certains développements des réflexions à suivre, en particulier s'agissant du droit pénal. Outre l'opportunisme de ce choix intellectuel, la preuve en droit pénal permet avant tout d'établir la véracité de certains faits. Si l'utilisation d'un protocole *blockchain*, en particulier pour ses fonctions d'horodatage et de partage d'informations entre les différents utilisateurs (en écriture ou en lecture seule) d'un réseau peut avoir ses intérêts, l'objectif de la preuve en droit pénal est surtout d'établir l'existence de faits constitutifs d'une infraction et enfin pouvoir établir la culpabilité d'un suspect (en respect avec le principe de la présomption d'innocence). Compte tenu du fait que les principes de la preuve pénale sont régis par des principes forts tels que le principe de liberté de la preuve[171] (sous couvert que la loi n'en dispose pas autrement), ou encore celui de l'intime conviction du juge pénal dans le rendu de sa décision[172].

Sachant également que le juge pénal portera son intérêt sur la matérialité des faits et le respect du principe de légalité des délits et des peines plutôt que sur les moyens utilisés par le prévenu pour réaliser une infraction (outre les potentielles aggravations de circonstances en fonction de moyens pouvant caractériser ces aggravations). Dichotomie entre l'infraction et sa technique de commission, l'actualité peut, pour autant, être empressée d'assimiler *blockchain* (et en particulier les cryptoactifs[173]) et comportements répréhensibles, mais seule l'infraction restera, de manière légitime[174]. Dès lors, l'étude d'un protocole informatique et sa validité face au droit de la preuve en pénal, perd sens compte tenu des principes précédemment exposés. La commission d'une infraction découlant moins des différents outils utilisés, puissent-ils être qu'informatiques, que de l'infraction en tant que telle, l'utilisation d'une *blockchain* pour la

---

[171] Article 427, Code de procédure pénale

[172] *Ibid*.

[173] TETEREL N., Bruno Le Maire, financement du terrorisme et bitcoin, Cointribune, 21 oct. 2020, disponible à https://www.thecointribune.com/actualites/bruno-le-maire-financement-du-terrorisme-et-bitcoin-btc/ (consulté le 21/10/2020)

[174] Le Monde avec AFP, 30 janv. 2020, *Démantèlement d'une vaste escroquerie internationale de faux placements en bitcoins*, Le Monde – Pixels, disponible à https://www.lemonde.fr/pixels/article/2020/01/30/demantelement-d-une-vaste-escroquerie-internationale-de-faux-placements-en-bitcoins_6027804_4408996.html (consulté le 21/10/2020).

Dans cette affaire d'escroquerie, ce n'est pas la présence de Bitcoin (et donc de la technologie *blockchain*) qui fut mise en cause, mais bien l'infraction pénalement répréhensible d'escroquerie.

commission d'actes répréhensibles n'apporte de difficultés que pour l'appréciation des faits ou la compréhension des différents moyens utilisés plus que pour la caractérisation de ces mêmes faits.

82. Toutefois, la facette pénale, prise dans le sens où certaines infractions sont facilitées ou même créées grâce à l'essor de la *blockchain* (même si, dans une approche pragmatique et empirique, elles ne représentent que de maigres portions de son utilisation[175]), ne doit pas être omise pour autant. La *blockchain*, visée principalement pour le *Bitcoin* et les autres cryptoactifs est régulièrement malmenée et même fustigée[176]. Déterminer si cela est à tort ou à travers n'est pas l'objet de la présente étude, même si une rigueur intellectuelle impose de le mentionner. Le *Bitcoin* est souvent décrié pour ses facultés à faciliter les paiements sur internet, principalement sur le *dark web*[177], et possède, encore aujourd'hui, une réputation sulfureuse. Cette réputation ayant été notamment acquise pour ses utilisations sur *Silk Road*, une plateforme d'activités - profondément - illicites[178]. Néanmoins, s'attarder sur le caractère illicite, justifié ou non, de *Bitcoin* et par extension sur celui de la *Blockchain* et de tous les autres cryptoactifs serait comme de fustiger l'ensemble Internet pour l'exercice d'activités illégales, sans se poser la question de la dichotomie entre l'outil et son usage.

83. Néanmoins, l'exclusion de ces développements, à savoir la portée ou encore le régime de l'utilisation d'une *blockchain* en droit pénal nous amène à faire un premier parallèle avec d'autres principes généraux de ce même droit, qui se retrouve applicable en droit positif, à savoir des impératifs de clarté et de sécurité juridique. Ces impératifs conduisant naturellement à se poser en recul sur la construction d'une norme, position qui invite alors à se focaliser encore plus en amont, invitant à réfléchir avant tout sur la capacité de compréhension de l'objet qui sera appréhendé par cette norme.

---

[175] À l'heure actuelle, les principales infractions mises en lumière à travers la technologie *blockchain* sont de l'ordre purement financier, à savoir le détournement de fonds ou encore le blanchiment d'argent. Ces facettes financières représentant le principal argument des « anti-bitcoin », et occultent de facto l'ensemble de la technologie des chaînes de blocs.

[176] PFISTER C., *Monnaies digitales : du mythe aux projets innovants*, Le Bulletin de la Banque de France n°230 : Article 1

[177] SAENKO L., *Le Darkweb : un nouveau défi pour le droit pénal contemporain*, Dalloz IP/IT 2017 p.80

[178] PETIT A., *Visite guidée du Darkweb cybercriminel*, Dalloz IP/IT 2017 p.86

Comme a pu le rappeler la doctrine, en particulier le professeur Mathieu[179], la notion de sécurité juridique, tout en étant marqueur de l'évolution de la norme doit permettre aussi de garantir la qualité d'une norme. Au-delà des oppositions relevées entre l'ordre judiciaire et administratif[180], force est de constater que la qualité de la rédaction ou encore la clarté (sans pour autant en exclure la complexité) de la norme en deviennent des éléments essentiels. Dans la lignée du principe de sécurité juridique, et pour faire un parallèle avec les premières réglementations du législateur français pour les aspects financiers liés aux cryptoactifs et à la *blockchain*, une volonté de protection des tiers (pour sécuriser leurs investissements et éviter les dérives financières) est présente. En effet, même si ce principe de sécurité juridique n'est pas inscrit dans nos principes constitutionnels français et qu'il reste controversé[181], tenir compte de ce principe reste « séduisant[182] », en particulier sur le fait qu'il nous invite à une réflexion sur les méthodes d'élaboration même de nos différentes normes, comme pour nous pousser à réfléchir plus loin qu'une simple réponse législative et/ou encore réglementaire pour tout nouveau sujet, en faisant une critique, peu dissimulée, contre ce que l'on nomme inflation législative[183]. Nous appelant à nouveau alors à mieux penser la norme et à s'inviter dans un premier temps à étudier si le droit positif est capable d'appréhender une situation nouvelle, et ainsi appeler à un « silence législatif (…) d'or[184] ».

84. C'est dans cette vision que l'étude des régimes de preuve face à la *blockchain*, à travers la lisibilité et la sécurité juridique d'opérations[185] trouve son intérêt. Apporter une réponse ou à défaut des éléments de réponse et/ou de lecture sur l'utilisation et le régime associées à un tel protocole, - surement - mal compris, peut avoir son intérêt, notamment pour les propos qui nous intéressent ici, à savoir la gestion de la preuve en droit civil, dans cet objectif de protection des tiers, auréolé du principe de sécurité juridique.

---

[179] MATHIEU B., *Réflexions en guise de conclusion sur le principe de sécurité juridique*, Cahiers du Conseil Constitutionnel n°11 (Dossier : le principe de sécurité juridique), Déc. 2001

[180] *Ibid*.

[181] GUINCHARD S., *Répertoire de procédure civile, Procès équitable – Contenu du droit à un juge*, Dalloz, Mars 2017 (actualisation : Juil. 2020), §189

[182] SOULAS DE RUSSEL D., RAIMBAULT P., *Nature et racines du principe de sécurité juridique : une mise au poin*t, Revue internationale de droit comparé. Vol. 55 N°1, Janv.-mars 2003. pp.85-103

[183] BENHAMOU Y., *Réflexions sur l'inflation législative*, Recueil Dalloz 2010 p.2303

[184] CARBONNIER J., *L'inflation des Lois*, *in Essais sur les lois*, Defrénois, 1979, p.272

[185] Le terme « opérations » est ici utilisé dans sa formule courante, afin de désigner aussi bien des rapports relatifs à des faits juridiques ou des actes juridiques, pris en ayant exclu les rapports pénaux.

Comme le souligne Me Marc Lipskier[186] notre droit positif ne devrait pas poser de problèmes et est même enclin à accueillir la technologie *blockchain*, affirmation dont il convient de mesurer la portée et les conséquences. La preuve est l'une des matières fondamentales juridiques, et a fait l'objet de nombreuses réformes. La dernière majeure en date est la grande réforme du droit des obligations de 2016, et il est traditionnellement étudié de manière parallèle l'administration de la preuve (la charge de la preuve et l'échange de la preuve) et les différents modes de preuve (notamment les distinctifs entre preuve parfaite ou imparfaite[187]).

85. Il convient également de rappeler la possibilité de l'imbrication d'une *blockchain* avec les régimes classiques de preuve avec deux typologies de choix : celui des parties (à savoir l'utilisation d'une convention de preuve[188], de manière antérieure à un potentiel litige) et celui du juge, qui conserve son appréciation, pouvant également aller jusqu'à ordonner une mesure d'instruction pour garantir le concours des parties à la résolution des litiges. Outre les critères classiquement entendus par le droit de la preuve, les différentes initiatives privées telles quelles ont pu être mises en avant, et la montée en puissance d'une gouvernance de la donnée[189] ne permettent pas d'exclure la possibilité, contractuelle, pour une ou plusieurs parties d'essayer de s'affranchir des cadres législatifs actuels pour pouvoir donner plus de poids à une éventuelle *blockchain* mise en place par elle(s).

Traditionnellement, on entend la convention de preuve[190] comme une convention au sens strict du terme, faisant application du principe de liberté contractuelle[191]. Néanmoins, face à ce principe, le régime de la convention de preuve comporte des conditions à ne pas omettre, faute de quoi une telle convention n'emportera que difficilement force obligatoire.

---

[186] LIPSKIER M., Interview, *La blockchain décryptée - les clefs d'une révolution, Blockchain* France, Netexplo, 2016

[187] MALINVAUD P., *Introduction à l'étude du droit*, 18e éd., 2018, LexisNexis, no 548

[188] On rappellera, simplement, que la validité des conventions de preuve, dans un univers numérique, ont été entérinées par la loi n°2000-230, 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, et avant cela, par la Cour de cassation (Cass. 1ère Civ., 8 nov. 1989, no 86-16.196).

[189] Cf. *Infra*, p.102 et suiv.

[190] Preuve : règles de preuve – Les principes fondamentaux – Encyclopédie Dalloz – Répertoire de droit civil – oct. 2018 (actualisation : juin 2019) : Une convention de preuve peut porter aussi bien sur la charge de la preuve, son admissibilité ou sa force probante, elle a pour objet de « réduire l'aléa de la preuve judiciaire afin qu'il ne remette pas en cause les prévisions des parties »,

[191] En ce sens, et pour ce qui concerne les conventions de preuve, la liberté contractuelle s'illustre alors dans la capacité des parties à aménager les différents critères de la preuve ; appliqué à une situation utilisant une *blockchain*, l'idée serait que les partis conviennent que les seules modes de preuves admis soient les différents enregistrements de données via une *blockchain*, par exemple pour prouver un transfert d'actif.

En premier lieu, et comme le rappelle à très juste titre la doctrine, une telle convention ne sera efficace que si les parties ont la libre disposition de leurs droits, nécessitant ainsi une étude au cas par cas[192], d'autant plus que ni la jurisprudence ni la loi n'ont donné de caractère dominant ou hiérarchique à la preuve en fonction des techniques utilisées[193]. Il ne serait de toute façon pas souhaitable qu'une telle hiérarchie ou une telle appréciation de la preuve puisse se faire que pas le seul biais technologique, au risque d'institutionnaliser une preuve à « deux vitesses technologiques », qui seraient représentées, presque par définition, toujours par une première, avantagée, qui bénéficiant des progrès technologiques les plus avancés, et une seconde, cantonnées à des outils technologies moins élaborés. Dans le cas où une telle convention de preuve porte sur des droits dont les parties ont cette libre disposition, il conviendrait également de lister et de vérifier les conditions classiques de validité du contrat (consentement, capacité, licéité), sans omettre également l'ensemble des règles relatives au droit des obligations (dont le développement n'est pas l'objectif dans cette étude). S'agissant des conventions de preuve, nul doute sur leur validité, tant elle devra rester dans les limites déjà connues du droit positif ; la *blockchain* ne restant qu'un outil parmi d'autres, la question de la validité des conventions de preuve portant sur l'utilisation d'une *blockchain* ne saurait poser de difficultés.

86. Le rappel sur la distinction entre preuve parfaite et imparfaite conduit naturellement à énumérer ces différents modes de preuve. Traditionnellement, il est entendu comme mode de preuve différentes possibilités, telles que : le témoignage, l'aveu, la présomption, le serment et enfin l'écrit. De manière évidente, toute preuve gérée grâce à une *blockchain* sera considérée comme écrit, à défaut d'un autre rattachement possible aux autres modes de preuve. Les développements suivants se borneront ainsi à étudier la validité d'une preuve supportée par une *blockchain*, prise en tant qu'écrit. D'ailleurs, le régime d'écrit électronique se devra d'être étudié ; en effet, si la variété des modes de preuve est une matière aujourd'hui fort documentée (s'agissant des preuves littérales, ou encore testimoniales, il pourra être fait référence aux articles 1363 et suivants du Code civil). Ce qui nous conduit à aborder deux volets, celui de

[192] MAGNIER V. *Enjeux de la blockchain en matière de propriété intellectuelle et articulation avec les principes généraux de la preuve*, Dalloz IT/IP 2019, p.76

[193] Règlement (UE) n °910/2014 du Parlement européen et du Conseil du 23 juil. 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, règlement dit « eIDAS ». On pourra rappeler les dispositions applicables à la signature électronique qui ne font références qu'à une notion de mécanisme - peu importe son expression technique - permettant de garantir l'authenticité d'un acte et d'une signature propre à son auteur.

l'admission crédible de la preuve par *blockchain* (§1) et la force probante mesurée d'une preuve supportée par une *blockchain* (§2).

§1 : L'admission crédible de la preuve par *blockchain*

87. La preuve est un « acte ou un fait juridique versé au soutien d'une prétention pour fonder les allégations des parties au litige[194] », gérée notamment par les articles 1353 et suivants et Code civil : « on appelle preuves, en jurisprudence, les manières réglées par les lois pour découvrir et pour établir avec certitude la vérité d'un fait contesté[195] ». À noter que peuvent être exclus les faits juridiques qui se prouvent par tout moyen[196].

L'article 1358 du Code civil pose le principe de l'apport de la preuve par tout moyen[197], tant que le mode de preuve rapporté respecte l'exigence de licéité[198]. S'agissant de l'écrit, la construction du régime de la preuve a dû attendre les années 2000 pour présenter une définition de l'écrit en particulier face à l'essor des écrits électroniques[199]. Il convient de rappeler que les articles 1366[200] et 1367[201] du Code civil, modifiés par la loi portant adaptation du droit de la preuve aux technologies de l'information (…)[202] ont permis de poser le principe d'égalité entre la preuve écrite et la preuve électronique.

88. Il convient également de considérer la preuve littérale comme une alternative : cela peut être soit un écrit (de manière classique, à savoir une « suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quel que

---

[194] Preuve (Droit civil), Fiche d'orientation, avr. 2020, Dalloz

[195] TOULLIER C., BONAVENTURE M., *Le droit civil français, suivant l'ordre du code…*, Paris, Warée, 1824, vol. n° 3

[196] Art. 1348, C. Civ.

[197] Code civil, article 1358 : « Hors les cas où la loi en dispose autrement, la preuve peut être apportée par tout moyen. ».

[198] LARDEUX G., *Répertoire de droit civil, Preuve : modes de preuve*, Dalloz, §7., oct. 2019

[199] RAYNOUARD A., *Adaptation du droit de la preuve aux technologies de l'information et à la signature électronique*. Observations critiques, Defrénois 2000. 593.

[200] Article 1366, Code civil : « L'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ».

[201] Article 1367, Code civil, portant sur la signature nécessaire à la perfection d'un acte juridique : « (…) Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État ».

[202] 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

soit leur support[203] »), soit un écrit électronique. L'article 1365 du Code civil, précité, donne donc la notion d'écrit, reste à savoir si des informations contenues sur une *blockchain* peuvent avoir la qualité d'écrit conformément à ce même code. En pratique, rappelons que la *blockchain* permet l'inscription de données sous forme de blocs, l'ensemble d'une *blockchain* n'étant, en définitive qu'un arbre de Merkle[204]. Si un bloc peut effectivement être réduit à sa simple expression « *hash*ée[205] », il n'en ressort pas moins que cette expression est un condensé de plusieurs informations[206], notamment :

- la transaction (et donc l'identification des participants à ces transactions) ;
- la version et le numéro du bloc au sein de la *blockchain* visée ;
- l'identification du bloc précédent ;
- les informations d'horodatage.

Dès lors, si l'écrit doit matérialiser « une volonté destinée à produire des effets de droit[207] », alors l'ensemble des éléments constitutifs d'un bloc répond à la description d'une telle volonté. En effet, la mention de la date, de l'heure mais également l'identification de la transaction et de ses auteurs est une description littérale de ce que les parties à cette transaction ont souhaité réaliser, conférant ainsi la qualité d'écrit à un bloc d'une *blockchain*. Cela étant, cette simple affirmation omet un caractère fondamental d'une *blockchain*, à savoir sa nature électronique.

À la lecture du Code civil, l'écrit sous forme électronique peut constituer un mode de preuve littérale « à la condition que puisse être dûment identifié la personne dont il émane »[208], en de telles conditions, l'écrit électronique à la même valeur que l'écrit « classique ». Ce qui importe, c'est l'intégrité garantie d'un tel écrit. Cette intégrité, au demeurant importante dans un univers numérique, sera la condition *sine qua non* pour qu'il soit accepté en tant que tel, en cas de conflit, par le juge. Ensuite, la notion de signature demeure fondamentale, permettant

---

[203] Art. 1365, C. civ.
[204] Cf. *Supra*, p.12
[205] Soit une suite définie de caractères alphanumériques.
[206] LARS L., *Qu'est-ce qu'un bloc dans la technologie blockchain*, Cryptoast, 27 janv. 2019, disponible à : https://cryptoast.fr/bloc-*blockchain*-crypto-explication (consulté le 05/07/2019)
[207] LARDEUX G., *Répertoire de droit civil*, précité
[208] Art. 1366, C. Civ.

de parfaire l'écrit, à condition qu'elle soit issue d'un procédé fiable, permettant notamment l'intégrité de l'acte auquel elle se rattache, notamment dans des situations qui ont déjà pu être rappelées par la Cour de cassation[209] s'agissant des écrits électroniques. La Cour de cassation a déjà pu retenir que le courriel seul ne vaut pas écrit électronique, dès lors que ne sont pas vérifiées, par le juge, les conditions posées par les articles 1366 et 1367 du Code civil. La *blockchain* étant un procédé réputé fiable et surtout garantissant l'intégrité de ses données, notamment avec l'utilisation de protocoles informatiques de chiffrement considérés comme aujourd'hui fiables, l'intégrité d'une *blockchain* lui permet de se voir conférer la qualité d'écrit électronique. Néanmoins, pour en faire des écrits « parfaits », la notion de signature sera essentielle.

89. Pour parachever la notion d'écrit et en faire une preuve dite « parfaite », la signature de son auteur doit être présente, à défaut, on ne pourra retenir qu'un commencement de preuve écrite. La signature revêt son importance car elle exprime le consentement de son auteur à la production d'effet de droits. La signature étant « (l') apposition (en général manuscrite) que fait une personne de son nom[210] », et, au regard du Code civil, le moyen d'identification de son auteur[211]. Tout absence de signature ne rend l'écrit concerné qu'imparfait. Concernant la signature électronique, elle consiste en « l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache[212] ».

Comme exposé précédemment, un bloc contient l'identification de son auteur, mais comporte-t-elle sa signature pour autant ? Il convient en effet de distinguer l'identification de la signature, la première n'emportant pas *de facto* le consentement de la personne visée. Néanmoins, le fonctionnement d'une *blockchain* est tel que la personne identifiée est celle pouvant être réputée l'auteur de la transaction. L'utilisation d'une *blockchain* étant permise seulement après création d'un identifiant, lui-même conditionné au respect des règles d'utilisation de la *blockchain* (par exemple, pour des *blockchain*s ayant pour objet la gestion d'actifs numériques, l'ensemble des obligations « KYC »[213]), toute inscription d'un bloc est signée numériquement de l'identifiant de la personne initialement identifiée. Ainsi, toute

[209] Cass. 1ère Civ., 30 sept. 2010, n°09-68.555, PBI, RTD Civ. 2010, p.785, note FAGES B.
[210] CORNU G., précité.
[211] Art. 1367, C. civ.
[212] Art. 1316-4, al. 2, C. civ.
[213] Cf.. *Supra*, p.20

blockchain possédant ces caractéristiques pourra relever de la notion de signature, achevant ainsi sa qualité d'écrit électronique.

90. Outre ces premiers acquis issus de tout précis de droit de la preuve, il faut enfin rappeler la valeur d'un adage, consacré par la réforme de 2016 du droit des obligations : « Nul ne peut se constituer de titre à soi-même »[214], valant pour la preuve des actes juridiques. L'étude, non exhaustive, d'un tel adage face à la *blockchain* demeure un intérêt, sur l'utilisation de la *blockchain* pour se créer des preuves, notamment d'antériorité, dans le cadre du droit d'auteur[215]. Toutefois, il conviendra de préciser que, même si cet adage, de par sa simplicité mais aussi son impact dans l'esprit de tout juriste, n'en reste qu'avec une portée limitée, comme a pu le démontrer la doctrine[216]. Il en reste surtout une lecture sur la possibilité laissée ou non de se constituer une preuve parfaite de manière unilatérale. En particulier, est-ce que l'utilisation d'une *blockchain* répondrait à l'application d'un tel adage ? Le positionnement sur cette question peut être bref et tranché. Une *blockchain* tire sa force de la multitude de ses participants, et une *blockchain* utilisée par une seule et même personne, n'a que peu d'intérêt. À part se créer artificiellement une perte financière inutile compte tenu de la complexité de la mise en place d'un tel protocole (au point qu'une *blockchain* supportée par un seul acteur ne pourrait être considérée comme une *blockchain* en tant que telle[217]), ne se trouve en pratique pas. En conséquence, tout acte inscrit sur une *blockchain* reste soumis à l'approbation (même mathématique) de l'ensemble des participants, et il s'avère que c'est l'action de l'ensemble de ces participants qui donne tout son intérêt à la *blockchain*, faisant alors apparaître une information ou un acte non pas unilatéral mais multilatéral, par essence même. En conséquence, l'architecture même d'une *blockchain* pourra expurger l'application de cet adage.

Par ailleurs, à rappeler également, qu'en matière commerciale, à l'égard des commerçants, les actes de commerce peuvent se prouver par tous moyens à moins qu'il n'en soit autrement disposé par la loi[218] (principe de libre preuve).

---

[214] Art.1363, C. civ.

[215] Cf. *supra*. p.70

[216] MOULY-GUILLEMAUD C., *Nul ne peut se constituer de titre à soi-même... C'est-à-dire ?*, RTD civ. 2018. 45.

[217] On renverra, sur ce point, à la définition technique d'une *blockchain*, imposant un réseau décentralisé, faisant intervenir une pluralité d'acteurs.

[218] Art. L110-3, C. Com.

91. Nous pouvons prendre en compte, dans le cadre de la présente étude, que la *blockchain* demeure un outil, et que son usage facilite effectivement la pré-constitution de preuves (notamment par en conférant une date certaine aux actes enregistrés de cette façon) et que son utilisation pourra effectivement dépendre du contexte contractuel visé[219]. Cette appréciation relevant d'une application purement sémantique d'un protocole *blockchain*. En effet, une *blockchain* ne reste qu'un protocole informatique, c'est-à-dire une méthode d'organisation particulière de données. Inscrire la *blockchain* en tant que nouveau mode de preuve n'apporterait rien au droit positif, comme le soulignent certains auteurs[220]. La véritable question sous-jacente de l'étude des conditions d'admission d'une *blockchain* en tant que preuve est de s'interroger sur la consécration de régimes particuliers des données « *blockhainées* » plutôt que sur le protocole en tant que tel et surtout sur le régime donné par le législateur à ces données compte tenu d'environnements particuliers[221].

Pour établir un parallèle pour comprendre cette différence sémantique, il convient en fait de se poser la question de la valeur probante d'un registre ou des éléments contenus dans un registre (rappelons-le, la *blockchain* peut être utilisée en tant que registre[222]). Un registre n'étant qu'un outil, il ne possède qu'une valeur relative, propre à son auteur ou son administrateur[223]. En conséquence des développements précédents, la notion d'écrit par une *blockchain* se trouve facilement applicable, et fait alors intégrer la *blockchain* au sein de la liste des outils permettant de créer un écrit (en particulier électronique), au même titre que le client de messagerie courriel. Cette réflexion nous pousse à nous interroger sur les caractéristiques des données utilisées à travers un protocole *blockchain*. La question est n'est pas de savoir si une *blockchain* est une preuve admise ou non (la présente étude tend à démontrer la réponse positive à cette question) mais de savoir si les données visées, grâce à l'utilisation d'une *blockchain*, remplissent les différents critères d'admission et la force

---

[219] MAGNIER V., *Enjeux de la blockchain en matière de propriété intellectuelle et articulation avec les principes généraux de la preuve*, Dalloz IT/IP 2019, p.76

[220] DOUVILLE T., *Blockchain*s et preuve, Recueil Dalloz, D. 2018. p.2193

[221] DAOUI L., *Notaires du Grand Paris : présentation du tout premier dispositif de blockchain notariale*, Affiches Parisiennes, 7 juil. 2020, disponible à : https://www.affiches-parisiennes.com/notaires-du-grand-paris-presentation-du-tout-premier-dispositif-de-*blockchain*-notariale-10653.html (consulté le 20/08/2020)

[222] Registre : Livre constituant un instrument de preuve ou de publicité, parfois doté d'une valeur constitutive, sur lequel on note des informations d'un type qui le caractérise et sert généralement à le dénommer et dont la tenue incombe parfois à un service officiel, parfois au principal intéressé. G. CORNU, *Vocabulaire juridique*, PUF, collec. Quadrige, 8e éd., 2007

[223] Sur ce point, il sera possible d'effectuer un parallèle avec les différents livres comptables issus du Code de commerce, n'emportant valeur première que pour leurs auteurs.

probante requise devant un juge en tant que mode de preuve. Ce n'est qu'à ces conditions qu'une preuve, supportée par un protocole *blockchain*, pourra être rattaché au mode de preuve par écrit. Cela étant, les critères d'admission étant étudiés, la force probante de la preuve par *blockchain* doit être analysée.

§2 : Une force probante mesurée de la preuve par *blockchain*

92. La notion de force probante invite naturellement à s'interroger sur la valeur et donc la hiérarchie au sein des différents modes de preuve d'un moyen considéré. C'est pourquoi il convient d'étudier le degré d'autorité relatif de la preuve par *blockchain* (A) mais également ses limites (B).

A/ Le degré d'autorité relatif de la preuve par *blockchain*

93. La rédaction du Code civil démontre, notamment en ses articles 1369[224] et 1370[225] l'existence d'une hiérarchie entre les différents modes de preuve. Sans pour autant exposer ici les différentes règles hiérarchiques entre les différents modes de preuve, la *blockchain* a le mérite de vouloir bousculer les genres, notamment quand on rappelle qu'elle a pu faire l'objet d'un amendement (même rejeté) pour conférer *de facto* une valeur probatoire forte[226]. Se poser la question de la force probante de la preuve par *blockchain* a néanmoins le mérite de se poser la question du bien-fondé ou non des possibilités offertes par une telle technologie pour faire évoluer ou à défaut améliorer nos modes de preuve actuels, qu'il s'agisse du caractère authentique d'une transaction effectuée sur une *blockchain* ou sur la notion même de signature électronique (et donc étudier la possibilité d'utiliser une *blockchain* pour une telle signature).

94. Le caractère authentique d'un acte ne découle pas directement de l'outil utilisé ; l'article 1369 du Code civil rappelle que cette condition est fixée par décret pris en Conseil

[224] Art. 1370, C. Civ. : « L'acte authentique est celui qui a été reçu, avec les solennités requises, par un officier public ayant compétence et qualité pour instrumenter. Il peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixées par décret en Conseil d'État. Lorsqu'il est reçu par un notaire, il est dispensé de toute mention manuscrite exigée par la loi. »

[225] Art. 1370, C. Civ : « L'acte qui n'est pas authentique du fait de l'incompétence ou de l'incapacité de l'officier, ou par un défaut de forme, vaut comme écrit sous signature privée, s'il a été signé des parties ». La combinaison de cet article avec le précédent démontre que l'acte authentique demeure « supérieur » à l'acte sous seing privé de par sa dé-classification en l'absence de compétence de l'officier ministériel concerné.

[226] Cf. *Infra*, p.65

d'État. L'acte authentique, qu'il soit électronique[227] ou non, découle de son auteur, un officier ministériel. Au contraire de différentes propositions passées, quoique sûrement volontairement provocantes[228], en l'espèce, il n'y a pas, à ce jour, de décret envisageant le caractère authentique d'un acte passé via une *blockchain*, publique, hybride ou privée). Néanmoins, en dépit d'un tel décret, nous pouvons faire un premier parallèle avec les conditions notamment de sécurité que doit présenter un outil utilisé pour que l'écrit s'y rapportant soit assimilable à un écrit électronique. Si l'article 1366 du Code civil nous indique clairement que l'écrit électronique est assimilable à l'écrit papier, encore faut-il que puisse être clairement identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions permettant son intégrité.

Il apparaît que les caractéristiques d'une *blockchain* remplissent ces conditions ; dans un premier temps, l'identification de la personne ne semble pas être un obstacle. En effet, en dépit du fait de considérer que les opérations passées, par exemple, sur la *blockchain Bitcoin*, sont anonymes, l'ensemble des opérations réalisées peuvent être attribuées à une personne identifiée ou identifiable, grâce à la nature même des différents identifiants de mineurs ou d'usagers de la *blockchain*. Ici, tout acte inscrit dans une *blockchain* notariale sera rattaché à mineur précis de la *blockchain*, en l'espèce, le notaire procédant à l'enregistrement de l'acte ou le service de publicité foncière souhaitant alimenter l'historique de propriété d'un bien immobilier.

95. Par ailleurs, concernant les conditions relatives à l'intégrité, l'architecture d'une *blockchain* permettant de posséder une traçabilité parfaite de l'ensemble des actes passés mais également de se prémunir contre toute modification ultérieure, ce caractère semble *de facto* respecté, en raison de la nature même de la technologie, en particulier quand sont utilisées des fonctions de hachage pour comparer deux documents. La *blockchain* devient ainsi un moyen idéal pour pouvoir s'assurer de la fiabilité d'une copie d'un acte dans un monde où l'information n'est pas rivale. L'utilité de la *blockchain* pour la communication de copies exécutoires dans le cadre de la dématérialisation des actes[229] semble avérée et c'est en ce sens

[227] FONTAINE M., *L'acte authentique électronique : état des lieux et perspective*, Revue Lamy Droit civil, 01/11/2019, 175, pp.32-34

[228] Assemblée nationale, Amendement n°CF2, relatif à la transparence, à la lettre contre la corruption et à la modernisation de la vie économique, (N° 3623), 13 mai 2016

[229] MEKKI M., *Colloque Blockchain et métiers du droit : "La fin des tiers de confiance* ?", 21 mars 2019

que la technologie *blockchain* permet de faciliter ces échanges. Néanmoins, la *blockchain* restant un protocole informatique, donc un moyen technique, il n'y a pas lieu de tenir une comparaison entre une personne physique et ce qui reste fondamentalement un outil. De la même manière, nous pouvons exclure, dans le cadre de cette étude, le caractère authentique d'actes passés sur une *blockchain*.

96. En suite directe à la lecture des articles 1366 et 1367 du Code civil, la notion de signature électronique[230] est un parfait exemple du rattachement de la technique au droit ; en effet, le législateur a conféré une valeur juridique importante à l'utilisation de procédés techniques ayant une valeur particulière, permettant ainsi la démocratisation de ces procédés au service d'une dématérialisation des échanges.

Une signature électronique est entendue comme procédé[231], ou pour utiliser un synonyme proche, un protocole, faisant ainsi un premier parallèle entre *blockchain* et signature électronique. Sans l'avoir réellement anticipé (la notion de signature électronique étant antérieure à la notion de *blockchain* en tant que telle), le législateur a laissé, à travers une rédaction neutre et intelligible, la possibilité pour la signature électronique d'évoluer, et de bénéficier de l'apparition de nouvelles techniques pour toujours plus garantir la fiabilité et l'authenticité des actes soumis à une telle signature.

En reprenant les dispositions de l'article 1367 du Code civil, la présomption de fiabilité d'une signature électronique provoque un renversement de la charge de preuve, preuve incombant ainsi à la personne contestant la validité d'une telle signature. Cette présomption étant acquise si les conditions de fiabilité sont remplies[232]. Cette présomption est accordée car il est difficile de démontrer qu'une signature électronique qualifiée de fiable ne l'est, en réalité, pas[233]. Les principes de la technologie *blockchain* pourraient fournir ces conditions, et donc

---

[230] Art. 1367 C. Civ : « Lorsqu'elle est électronique [la signature], elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État ».

[231] Définition : Manière de s'y prendre, méthode pratique pour faire quelque chose, par exemple : Un nouveau procédé de fabrication. Larousse. (s.d.). Procédé. Dans LAROUSSE *en ligne*, https://www.larousse.fr/dictionnaires/francais/proc%c3%a9d%c3%a9/64051 (consulté le 25/05/2020)

[232] Article 2 du décret du 30 mars 2001, JO 31 mars 2001, pp. 5070-5072 ; une signature électronique doit être propre au signataire, créée par des moyens que le signataire puisse garder son contrôle exclusif, garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable.

[233] En application des dispositions du règlement eIDAS, les signatures qualifiées disposent d'une présomption d'exactitude, qu'il convient de combattre, notamment en rapportant la preuve de l'absence des critères de qualification du dispositif de signature électronique, pour contester de telles signatures.

être utilisés en tant qu'outil de certification, néanmoins, en l'absence de toute intervention du législateur, la *blockchain* ne reste qu'un outil, bénéficiant de la présomption simple accordées aux outils de signature électronique. En dépit du fait qu'une lecture croisée du règlement dit eIDAS[234] imposant une identification univoque du signataire, excluant donc *de facto* la seule utilisation d'une *blockchain* pour satisfaire les critères d'une signature électronique qualifiée.

97. La création de données se fait notamment grâce à des outils cryptographiques (dont nous avons vu précédemment que leur utilisation est permise par le droit positif), l'utilisateur garde le contrôle (système de cryptographie asymétrique, utilisant une clé publique et une clé privée, gardée sous contrôle), et l'inscription de toute donnée au sein d'une chaine de blocs, de manière infalsifiable et durable. Ces éléments répondent aux objectifs d'intangibilité requis par la loi. Permettant ainsi d'assurer le caractère d'identification, d'intégrité et de fiabilité des procédés mis en place. Ces développements en appellent d'autres de manière parallèle, à savoir une étude rapide sur la cryptographie, ou techniques de chiffrement, notamment pour déterminer si l'utilisation de tels procédés sont licites. Même si elle fera l'objet de développements plus poussés ultérieurement[235], que l'on pourra constater de nombreux parallèles possibles entre la *blockchain* et d'autres dispositifs ou d'autres notions déjà connues par notre droit.

Mais il ne s'agit ici qu'une appréciation rapide, dont l'intérêt est de mettre en lumière le parallèle entre signature électronique et *blockchain* en tant que protocole de signature, donc en tant que technique pour authentifier des données. À défaut de qualification d'une *blockchain* en tant que procédé de signature électronique qualifié, la principale conséquence est d'empêcher son utilisateur de bénéficier du régime avantageux de présomption précédemment cité ; n'enlevant rien à la possibilité ou non de présenter devant un juge un acte passé via une *blockchain*.

98. En l'état actuel de la législation, la force probante d'une preuve par *blockchain* ne sera pas plus ou moins forte que celle d'un écrit classique (qu'il soit authentique ou non, qu'il soit parfait ou non), car, encore une fois, l'outil doit être écarté de la valeur probatoire d'un écrit. Juger la puissance d'un écrit « *blockchainé* » aura la même valeur intellectuelle et juridique

[234] Règlement (UE) n°910/2014, précité ; Exigences relatives à une signature électronique avancée (extraits) : « Une signature électronique avancée satisfait aux exigences suivantes : a) être liée au signataire de manière univoque ; b) permettre d'identifier le signataire ; (…) ».

[235] Cf. Parie 2, Titre 2, Chapitre 2

que de sonder la pertinence d'un écrit réalisé à l'aide d'un stylo premier prix ou à l'aide d'un stylo « Montblanc ». Néanmoins, l'occultation d'une telle réflexion en doit pas conditionner l'avenir d'une telle technologie. Si le système de preuve français peut reposer sur des principes tels que ceux de la vraisemblance ou de la certitude[236], la démocratisation d'une telle technologie peut avoir, d'une part, pour objet de moderniser nos outils de preuve et la façon dont on peut gérer nos données, plus efficacement et de manière plus sécurisée, comme nous allons pouvoir le voir à travers l'exemple de la gestion de l'antériorité en droit d'auteur grâce à la *blockchain*. D'autre part, l'essor de telles technologies peuvent aussi aider à moderniser nos rapports contractuels.

Aux termes de l'article L111-1 du Code de propriété intellectuelle[237], l'auteur jouit d'une protection de son œuvre dès sa création, sans formalité préalable ou postérieure. Tout dépôt ultérieur ou concomitant à la création d'une œuvre n'aurait qu'une force purement probatoire et non attributive d'un droit de propriété[238]. Dès lors, pour l'auteur, tout l'intérêt de se créer des preuves de sa création est de pouvoir démontrer, en cas de litige, le bien-fondé de sa qualité d'auteur de l'œuvre et ainsi pouvoir combattre une éventuelle revendication sur sa création ou encore défendre son œuvre d'une quelconque contrefaçon. Afin de s'aménager et surtout de faciliter une telle preuve de sa qualité d'auteur sur sa création, les méthodes sont multiples : le dépôt de son œuvre via une enveloppe Soleau[239] , un dépôt de son œuvre auprès d'une société de gestion collective, ou encore un envoi à soi-même d'un courrier en AR/R. Toutes ces méthodes ont comme premier but de conférer une date certaine à une création. La date de dépôt d'une œuvre (et donc la date de sa préposée création) étant un élément essentiel dans tout contentieux relatif au droit d'auteur. S'agissant de ce critère de date, et même d'horodatage, la *blockchain* revêt un intérêt tout trouvé, dans le sens où l'utilisation d'un tel protocole informatique permet à son utilisateur de créer une empreinte à date certaine de sa transaction (puisse-t-elle porter sur l'existence à un instant T de son œuvre).

99. Il en ressort un élément parfaitement séduisant pour tout auteur : le fait de pouvoir accéder à une protection fiable, peu onéreuse et surtout extrêmement rapide grâce au dépôt de

---

[236] KINSCH P., *Entre certitude et vraisemblance, Le critère de la preuve en matière civile, in* De Code en Code, Mélanges en l'honneur de G. Wiederkehr, 2009, Dalloz, p.455

[237] Art. L111-1, CPI : « L'auteur d'une œuvre de l'esprit jouit sur cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous »

[238] BINCTIN N., *Droit de la propriété intellectuelle*, LGDJ, 4e éd., 2016, n° 44.

[239] https://www.inpi.fr/fr/proteger-vos-creations/lenveloppe-soleau/enveloppe-soleau (consulté le 20/08/2020)

son œuvre sur une *blockchain*. En effet, étant donné la traçabilité de son dépôt, son intégrité et la faculté de le vérifier à tout moment, même à distance, la *blockchain* présente des avantages concurrentiels indéniables par rapport à d'autres modes de production de preuve pour la titularité et l'antériorité d'une création[240]. Il est également possible de noter une actualité grandissante autour de l'attrait de la *blockchain* pour la gestion de droits de propriété intellectuelle[241], d'autant plus que le système probatoire inhérent à une *blockchain* est parfaitement compatible avec notre système actuel[242]. De surcroît, s'agissant de la notion de divulgation[243] en droit d'auteur, il apparaît qu'un enregistrement ne constituait pas une telle divulgation. En effet, l'œuvre enregistrée sur une *blockchain* n'apparaissant pas en tant que telle mais seulement en tant qu'empreinte (ou fichier « *hash*é ») et compte tenu du fait qu'il s'agisse d'une fonction irréversible, aucune divulgation au public ne saurait être retenue pour un tel enregistrement[244].

B/ Limites de la force probante de la *blockchain*

100. Néanmoins, plusieurs limites à cette solution « féérique » peuvent se trouver. La première réside dans les capacités techniques propres à une *blockchain*, dans le sens où toute transaction subit une fonction de hachage, c'est à dire que tout dépôt se retrouve condensé en une suite normée de caractère. Un *hash* étant propre à toute opération ou information, il suffit qu'un changement, aussi infinitésimal soit-il pour que le résultat *hash*é soit différent. Forçant ainsi tout créateur désireux de se créer une preuve idéale de sa création d'enregistrer perpétuellement la moindre modification de son œuvre au sein d'une *blockchain*.

101. La seconde limite réside encore dans la nature d'une *blockchain*, notamment prise en ses différentes déclinaisons (publique, hybride ou encore privée). Une *blockchain* pouvant être partagée entre une multitude d'acteurs, la possibilité pour qu'un tel réseau soit en réalité tenu par des acteurs poursuivant le même but (légitime ou non), remet en cause l'intégrité même d'une chaîne de blocs ainsi supportée. Même si une nouvelle fois, en reste la possibilité de

[240] FAUCHOUX V., GOUAZÉ A., *Pourquoi la blockchain va révolutionner la propriété intellectuelle ? Application pratique au secteur de la mode*, Propriétés intellectuelles, Oct. 2017, n°65

[241] « L'EUIPO se connecte (…) via une chaîne de blocs », disponible à : https://euipo.europa.eu/ohimportal/fr/news (consulté le 05/06/2021)

[242] Cf. *Supra*, p.65

[243] Art. L113-1, CPI : « La qualité d'auteur appartient, sauf preuve contraire, à celui ou à ceux sous le nom de qui l'œuvre est divulguée. »

[244] MALAURIE-VIGNAL M., *Enjeux et défis de la blockchain dans ses relations avec la propriété intellectuelle*, Dalloz IP/IT 2018 p.531

l'hybridation d'une *blockchain*, notamment écrite par les seuls offices de propriété intellectuelle[245,246], qui auraient alors la possibilité de moderniser leurs activités actuelles en faisant supporter par une *blockchain*. Cette architecture particulière permettrait une mise à jour constante et quasi immédiate de l'ensemble des travaux de ces offices et aurait, sans nul doute, de forts attraits que ce soit en termes de sécurité informatique, de scalabilité, ou encore de fiabilité.

102. La troisième est corollaire de la notion de divulgation d'une œuvre sur une *blockchain*. Force est de se poser la question de la divulgation d'une œuvre en tant que *hash* sur une *blockchain*. En tant que condensat informatique, un *hash* ne saurait être analysé en tant que divulgation d'une œuvre, celle-ci restant non-identifiable. Or, en l'absence de divulgation et donc de mention de l'auteur en tant que tel sur une œuvre, la preuve de la titularité des droits s'en voit affaiblie [247] . Et manière parallèle, en cas de contrefaçon de l'œuvre et de détermination d'éléments d'antériorité de création, compte tenu des différents régimes de preuve applicables, le juge ne pourra s'en tenir à une seule preuve apportée grâce à une *blockchain*, il s'en devra étudier tout un ensemble d'éléments, sans pour autant placer les éléments rapportés et constitués par une *blockchain*[248] en priorité.

103. Il reste que, même si les attraits probatoires d'une *blockchain* puissent paraître limités pour la propriété littéraire et artistiques, une telle technologie a, une nouvelle fois, le mérite de bousculer et d'inviter à une réflexion plus globale sur l'usage de technologies de l'information et de la communication pour des actions juridiques et classiquement bien entendues. Si la *blockchain* permet bien de s'aménager plus facilement tout un faisceau de preuves (ou à défaut, d'indices), elle permet une dynamisation qui sortirait du champ de la présente étude, notamment sur les impacts purement technologiques reliés à la mise en place d'une *blockchain*, par exemple pour les offices de propriété intellectuelle, ou même, dans une autre mesure possible, sur la gestion des droits d'auteurs ou d'autres attraits reliés à la culture ou d'autres aspects économiques[249].

---

[245] BARSAN I., *Blockchain* et propriété intellectuelle, Revue Communication et commerce électronique, Lexisnexis, Avril 2020, n°4

[246] SELLET E, *Blockchain : vers une ubérisation des Offices de propriété industrielle ?*, Mémoire de recherche, CEIPI, Université de Strasbourg, 2018

[247] CANAS S., *Blockchain et preuve. Le point de vue du magistrat*, Dalloz IP/IT, 01/02/2019, 2, pp81-84

[248] *Ibid*.

[249] GIRAUD T., précité.

104. D'autant plus que l'ordonnance du 28 avril 2016 valide l'utilisation de la *blockchain* en tant que mode de preuve pour le transfert d'actifs[250], démontrant une certaine volonté du législateur à considérer l'usage de la technologie *blockchain* comme pouvant être un moyen de preuve déjà dans le transfert d'actifs. Au-delà, pour revenir à la notion de registre telle que définie précédemment[251], l'intervention du législateur a été nécessaire afin de valider l'utilisation de la *blockchain* pour la tenue de registres officiels, comme a pu le démontrer l'adoption d'un décret de 2019 sur la dématérialisation des registres de société[252]. Démontrant ainsi que toute modernisation de nos fonctionnements sociaux ou juridiques doit dans tous les cas passer par la case « législateur ».

105. Compte tenu des développements précédents, aucune contrariété intrinsèque à l'utilisation de la *blockchain* n'apparaît au regard du droit positif de la preuve français. Néanmoins, l'ensemble des propos tenant à la consécration de la *blockchain* comme mode de preuve « ultime », dans le sens où tout acte enregistré dans une *blockchain* bénéficierait d'un contenu avec une validité incontestable, doivent être modérés. D'une part, en raison des attributs techniques de la *blockchain* prise en tant que telle (en tant protocole de gestion de données dépendant tout aussi bien de la pertinence des différents nœuds ou encore de la fiabilité technique de sa mise en place). D'autre part, en raison du fait qu'il n'existe en tout état de cause aucune validation normative de la consécration d'une telle valeur à tout élément enregistré sur une *blockchain*.

106. D'ailleurs, l'analyse d'une telle technologie doit se faire de manière concomitante à l'analyse des jurisprudences contemporaines et passées, notamment pour permettre une analyse plus large qu'une lecture seule de la Loi. Or, si l'attrait d'une telle technologie reste indéniable, force est de constater qu'il n'existe, au moment de l'écriture de la présente étude, aucune décision jurisprudentielle sur la valeur probatoire d'actes passés *via* une *blockchain*. Espérons seulement qu'une future décision viendra éclairer ces propos tout en n'occultant pas la distinction entre l'outil et la preuve en tant que telle.

---

[250] Ordonnance n°2016-520, précitée, modifiant l'article L223-13 du Code monétaire et financier : « Le transfert de propriété de minibons résulte de l'inscription de la cession dans le dispositif d'enregistrement électronique mentionné à l'article L. 223-12, qui tient lieu de contrat écrit pour l'application des articles 1321 et 1322 du code civil. »

[251] Cf. *Supra*, p.13

[252] Décret n° 2019-1118 du 31 oct. 2019 relatif à la dématérialisation des registres, des procès-verbaux et des décisions des sociétés et des registres comptables de certains commerçants.

107. En définitive, si la *blockchain* possède le potentiel de devenir un nouveau mode de preuve, fiable et sécurisé, il n'en reste pas moins qu'elle ne demeure qu'un outil. Ainsi, elle demeure appréhendable par le droit positif, tout en gardant son potentiel disruptif. Les différents modes de preuve ainsi modifiés techniquement par la *blockchain* invitent alors à concevoir une modernisation des rapports contractuels, mais qui reste partielle compte tenu de la nature même des *smart contracts*.

Section 2 : Une modernisation partielle des rapports contractuels

108. Si l'utilisation de la *blockchain* doit être reliée à l'intervention du législateur pour pouvoir bénéficier d'une quelconque valeur légale probante supérieure à celle d'un simple outil, les démonstrations précédentes ont éclairé le fait que cette technologie a comme premier attrait - une nouvelle fois - de bousculer des acquis. Peut-être à tort, la *blockchain* soulève de nombreuses réflexions partant du principe qu'elle serait quasi miraculeuse pour nos règles de droit, en premier lieu pour le droit de la preuve. L'un des seconds mérites avancés par les partisans de cette technologie est son avancée pour la modernisation de l'automatisation de processus contractuels, à savoir la mise en œuvre des smarts contrats. Rappelons que la notion de « rapport contractuels » sera entendue ici de manière littérale, pour reprendre la définition du Code civil[253], prise dans une approche pragmatique découlant de la réalisation successive ou non de contrats entre deux ou plusieurs personnes.

109. La notion de modernisation invite à de premières réflexions. Cette notion, nom commun dérivé du verbe moderniser est « rajeunir quelque chose, lui donner une tournure moderne[254] », mais est aussi entendu comme « organiser quelque chose d'une manière conforme aux besoins d'aujourd'hui[255] ». L'un des fils rouges propre à toute réflexion autour de la *blockchain* mettant en avant toutes ces possibilités d'évolutions pour notre Société, de manière aussi hétéroclite que l'arrivée d'Internet en son temps. Un premier paradoxe dans la mise en avant d'un caractère « modernisateur » est encore une fois ce rapport au temps, tel

[253] Art. 1101, C. Civ : « Le contrat est un accord de volontés entre deux ou plusieurs personnes destinées à créer, modifier, transmettre ou éteindre des obligations. »

[254] Larousse. (s.d.). Moderniser. Dans LAROUSSE *en ligne* : https://www.larousse.fr/dictionnaires/francais/moderniser/51950 (consulté le 20/08/2020)

[255] *Ibid*.

qu'il peut être compris dans la définition du terme moderniser. Comment définir les besoins d'aujourd'hui, et comme les distinguer de ceux d'hier et de demain ? Comment les mettre en perspective avec les nouvelles technologies, censées répondre à de nouveaux besoins mais qui seront intrinsèquement liées au passé dès leur avènement ? En réalité, la notion de moderniser telle qu'entendue en tant que réponse aux besoins d'aujourd'hui revêt un décalage incompatible avec celui de l'évolution de la norme juridique. Là où la norme juridique va tenter soit de réguler soit d'anticiper de nouveaux besoins, le concept de modernisation répond à un impératif pris à l'instant T, là où toute réponse à l'apparition d'un nouveau besoin va devoir se concrétiser à ce même instant. À défaut, toute nouvelle réponse - trop - postérieure sera en décalage avec ces besoins qui continueront d'évoluer.

110. En réalité, parler de modernisation de rapports contractuels par suite de l'essor d'une technologie comme la *blockchain* invite à une réflexion une nouvelle fois hétéroclite. Il est toutefois possible de l'incarner *via* l'étude de l'apport de la *blockchain* sur les rapports contractuels d'aujourd'hui, afin de pouvoir déterminer et en réalité apprécier le régime applicable à un *smart contract* à l'aune de notre droit. Comme le souligne le professeur Mekki [256], une approche spéculative ne doit pas se faire au détriment d'une approche descriptive à des fins de compréhension d'une notion nouvelle comme le *smart contract*. C'est ainsi que la notion même de *smart contracts* devra être approfondie, notamment pour déterminer ce qu'elle est, et ainsi apprécier une adaptation des rapports contractuels grâce à eux (§1), pour pouvoir seulement entériner sa validité dans nos rapports contractuels contemporains (§2), et donc ses conséquences en termes de modernisation de nos rapports contractuels.

§1 : Une adaptation des rapports contractuels grâce aux *smart contracts*

111. L'avènement de la *blockchain*, notamment avec la montée en puissance de la *blockchain* Ethereum[257], a permis la mise en lumière d'un protocole informatique particulier : le *smart contract*. Paradoxalement, cette notion n'est pas nouvelle et ne coïncide pas avec

[256] MEKKI M., *Le contrat, objet des smart contracts (Partie 1)*, Dalloz IP/IT 2018, p.409

[257] La *blockchain* Ethereum, reposant sur la technologie *blockchain* approfondi les usages possibles de cette même technologie. Développée en open-source, la *blockchain Ethereum* permet notamment le support d'application tierces tout en profitant des caractéristiques techniques d'une *blockchain*. https://ethereum.org/fr/what-is-ethereum/, (consulté le 16/09/2020).

l'avènement de la *blockchain*. Il convient ainsi de réaliser les présentations techniques (A) pour pouvoir réaliser les appréciations juridiques (B) du *smart contract*.

A/ Présentations techniques

187. Sans entrer dans une conception purement théorique, un *smart contract* répond à une double condition informatique de type « *IF/THEN*[258] », et a été théorisé dès les années 90, notamment par l'auteur, juriste et informaticien, Nick Szabo[259]. Une nouvelle fois, il s'agissait, en utilisant les caractéristiques fondamentales de méthodes de chiffrement[260], de créer un protocole informatique permettant de sécuriser la réalisation de conditions préalablement définies une fois un objectif atteint. Par exemple, l'une des premières applications « démocratisées » d'un *smart contract* a été mis en place par la société Axa au bénéfice d'une plus rapide indemnisation en cas de retard d'avions[261]. Le principe est relativement simple : Un client, possédant la référence « 1234 » prend le vol AZ567, dont le contrat d'assurance associé comporte une clause d'indemnisation en cas de retard supérieur à une heure ;

- Le vol AZ567 est équipé d'un capteur électronique (type IoT[262]) qui relève automatiquement l'heure à laquelle les roues quittent le sol et l'heure à laquelle les roues touchent le sol à l'atterrissage, relié à une *blockchain* et à un *smart contract* ;

- La mise en œuvre de la clause d'indemnisation est prévue par ce smart contract, dont les termes prévoient le versement d'une indemnité dès la constatation d'un retard supérieur à une heure, sur le compte bancaire du client[263] ;

[258] Une fonction de type IF/THEN est une fonction qui exécute un groupe d'instructions soumises à une condition, en fonction de la valeur d'une expression ; https://docs.microsoft.com/fr-fr/dotnet/visual-basic/language-reference/statements/if-then-else-statement (consulté le 16/09/2020).

[259] SZABO N., *Formalising and securing relationships on public networks*, *First Monday*, Volume 2, Number 9 - 1 September 1997, disponible à https://firstmonday.org/ojs/index.php/fm/article/view/548/469, (consulté le 10/09/2017)

[260] À savoir sécuriser les échanges, qu'ils soient électroniques ou non.

[261] https://www.axa.com/fr/magazine/axa-se-lance-sur-la-*blockchain*-avec-fizzy, consulté le 13/10/2020

[262] IoT : Internet of Thing, « est l'interconnexion entre l'Internet et des objets, des lieux et des environnements physiques », https://fr.wikipedia.org/wiki/Internet_des_objets, (consulté le 15/10/2020).

[263] NB : l'ensemble des informations bancaires étant naturellement déjà en possession de la société d'assurance ; l'objet du présent exemple est d'illustrer simplement la mise en œuvre d'un *smart contract*, dans le cadre d'une relation contractuelle purement fictive et idéale.

- Le vol AZ567 est prévu pour un décollage à 14h00 (heure de Paris) et une arrivée à 19h00 (heure de Paris) ;

- Le vol AZ567 atterrit à 23h00, soit un retard constaté à l'arrivée de quatre heures ;

- Le capteur électronique envoie un signal, interprété par le *smart contract* comme déclencheur automatique de l'indemnisation du client ;

- Le client reçoit, compte tenu des délais de transactions bancaires son indemnisation en 48h.

La mise en œuvre d'un tel *smart contract* évitant ainsi l'ensemble des mesures habituellement prévues pour la mise en œuvre d'une clause d'indemnisation en raison d'un quelconque sinistre (ici, un retard d'avion). Une autre métaphore possible est de considérer le *smart contract* comme une version purement informatique du distributeur automatique[264]. Si le principe de fonctionnement d'un *smart contract* est effectivement simple, et se rapproche ainsi d'un algorithme relativement peu élaboré[265], le séquençage précédent met en avant plusieurs notions revêtant chacun leur importance :

- L'existence d'un contrat préexistant ;

- La possibilité de compléter ce premier contrat avec une *blockchain* et un *smart contract* dont les termes seront adaptés[266] ;

- La possibilité de relier l'exécution de ce *smart contract* à un événement extérieur (dans l'exemple, une heure d'arrivée) ;

- Une exécution automatique des termes contractuels préalablement convenus.

[264] MOUNOUSSAMY L., *Le smart contract, acte ou hack juridique ?* LPA 20 févr. 2020, n° 150t0, p.12, citant notamment les travaux de Nick Szabo sur les *smart contract*s.

[265] On rappellera que l'algorithme reste une suite logique d'instruction.

[266] Ceci mettant en exergue le fait qu'un *smart contract* complètement autonome ne présente aucun intérêt technique ou juridique tant il reste dépendant d'une *blockchain*.

188. En reste un dernier élément, l'Oracle[267], qui peut être également intégré à cette appréciation du smart contract. Outil tiers à un *smart contract* (et donc à une *blockchain* préexistante), l'Oracle est le tiers de confiance numérique et fantôme d'une *blockchain* ; il permet de rattacher une *blockchain*, théoriquement coupée et autonome du monde extérieur, à des jeux de données préalablement certifiés[268], permettant d'instruire une perméabilité limitée et sélectionnée à une *blockchain*. Un oracle pouvant, pour reprendre l'exemple précédent, se représenter dans le capteur IoT. L'oracle devenant ainsi partie intégrante du processus contractuel préalablement mis en place à travers une *blockchain* et permettant ainsi de fournir les informations nécessaires au fonctionnement du *smart contract* visé[269].

L'explosion - ou plutôt l'exposition - de ces éléments constitutifs d'un *smart contract* permettent le parallèle entre cette appréciation technique des *smart contract* et leur appréciation juridique.

B/ Appréciations juridiques

189. Apprécier, juridiquement, ou encore donner une qualification juridique à un objet ou encore à un événement reste un fondamental du travail du juriste. L'appréciation d'une situation de fait au prisme de règles juridiques établies (ou à établir) demeure un moyen de sécuriser nos relations et, dans une certaine mesure, faire perdurer l'état de droit dans lequel nous sommes.

190. Dans le cadre d'une conception juridique du *smart contract*, force est de séparer la matérialité de l'objet visé (même si cette matérialité est en soi immatérielle du fait de son application) et ses effets juridiques. La matérialité d'un *smart contract* est résumée à quelques lignes de code, le plus souvent dans un langage de programmation aujourd'hui plutôt répandu, le langage *Solidity*, un « langage orienté objet[270] ». Les effets juridiques peuvent, cependant,

[267] POLROT S. Les oracles, lien entre la blockchain et le monde, Ethereum-France, 13 sept. 2016, disponible à : https://www.ethereum-france.com/les-oracles-lien-entre-la-*blockchain*-et-le-monde/ (consulté le 19/10/2020).

[268] Ici, le sens du mot certifié prendra sa notion la plus souple, à savoir l'octroi d'une confiance particulière, soit entre les parties à une *blockchain*, soit par un organe certificateur.

[269] POLROT S., Smart contrat » ou le contrat auto-exécutant, *Ethereum* France, 20 mars 2016, https://www.ethereum-france.com/smart-contract-ou-le-contrat-auto-executant/ (consulté le 19/10/2020)

[270] https://fr.wikipedia.org/wiki/Solidity (consulté le 13/10/2020)

être particulièrement divers, comme l'indemnisation dans le cadre d'un contrat d'assurance, ou même l'accès à une chambre d'hôtel[271].

191. Outre la simplification intellectuelle née de la séparation artificielle entre objets et effets de droit, la matérialité d'un *smart contract* nous renvoie à une appréciation parallèle de la matérialité de suites de caractères à vocation informatique, un langage de programmation. La conception juridique d'un tel langage n'est guère éloignée d'une définition classique de ce qu'est un code, à savoir un « ensemble cohérent de(s) règles qui gouvernent une matière[272] ». Et c'est exactement ce qu'est un *smart contract*, une suite logique et ordonnée de caractères, de règles, y compris grammaticales, un ensemble cohérent de règles. La compréhension de cette matérialité est essentielle pour pouvoir apprécier les effets juridiques d'un objet ; en somme, comprendre le *smart contract* pour mieux l'apprécier, en particulier juridiquement.

Un *smart contract* reste indubitablement rattaché à un contrat primordial, fondamental. Si l'existence du principe de liberté contractuelle[273] peut permettre l'appréciation du *smart contract* comme contrat classique, elle pourrait être l'illustration de la tradition littérale d'un terme anglo-saxon dans la langue de Molière. Si la traduction littérale[274] donne effectivement pour traduction à « *contract* » le terme « contrat », l'inverse doit être moins affirmative. Notre terme français de « contrat » peut se traduire par le vocable « *agreement* », ou encore « *undertaking* [275] ». Ces subtilités découlant des matières dans lesquelles on souhaite converser. Ces nuances sont importantes, et si le terme contract doit être manié avec une certaine prudence, la notion de *smart contract* ne peut se réduire à une appréciation unique.

192. Là où il apparaît une carence du législateur quant à la prise en compte du *smart contract* à la lumière de son initiative pour la consécration juridique de la *blockchain* dans notre droit positif, celle-ci n'apparaît pas pour autant poser quelconque problème. La notion de langage de programmation est en soi déjà connue par le droit, sous l'égide du logiciel. En effet, si le logiciel n'a, en soi, pas de définition légale[276], il ressort des conceptions européennes que le logiciel, ou plutôt le programme d'ordinateur est un ensemble d'instructions qui a pour but de

[271] Exemple « slock.it », précité.
[272] G. CORNU, précité.
[273] LATINA M., *Contrat : généralités – Principes directeurs du droit des contrats*, Répertoire de Droit civil, Dalloz, Mai 2017
[274] https://www.larousse.fr/dictionnaires/anglais-francais/contract/572168 (consulté le 13/10/2020)
[275] https://www.larousse.fr/dictionnaires/francais-anglais/contrat/18588 (consulté le 13/10/2020)
[276] On rappellera que l'article L112-2, 13° du CPI ne fait que citer le terme « logiciel » sans pour autant le définir.

faire accomplir des fonctions par un système de traitement de l'information appelé ordinateur[277] ; et en reste seulement une définition donnée en 1981[278], qui définit le logiciel comme « l'ensemble des programmes, procédés et règles, et éventuellement de la documentation, relatif au fonctionnement d'un ensemble de traitement de données ». Le *smart contract*, pris comme une série d'instruction destinée à être comprise par un ordinateur (même relié à une *blockchain*) pourrait s'affilier effectivement au logiciel. Néanmoins, cette définition n'apparaît pas comme suffisante, tant le régime propre au logiciel se trouverait inadapté, en particulier pour l'ensemble des conditions relatives à la cession ou à la propriété, tant le *smart contract* reste fondamentalement un programme particulièrement court (par rapport à un logiciel classique), ou tant à sa qualité accessoire et dépendant d'une *blockchain*[279]. D'autant plus que la notion d'algorithme, se rapprochant bien plus de la conception d'un *smart contract*, en tant que tel, ne peut bénéficier d'une protection au titre du logiciel[280].

193. Ce premier parallèle avec l'algorithme nous invite alors à nous poser une question déterministe sur le *smart contract* et étudier si ce dernier ne s'apparenterait pas simplement à un contrat. Pour une partie de la doctrine, le *smart contract* serait « plutôt un code de programme informatique qui automatise la vérification, l'exécution et l'application de certaines conditions d'un accord[281] ». Rappelons que le contrat reste la rencontre d'une offre et d'une acceptation, destinée à créer, modifier ou encore éteindre des obligations[282].

Cela étant, l'exécution d'un *smart contract* met principalement en avant une vélocité dans son exécution par rapport à un contrat classique. Là où il est possible de trouver l'expression de « contrat à exécution automatique[283]», qui peut faire écho à la notion de contrat à exécution instantanée[284] et qui tendrait à faire émerger une nouvelle catégorie de contrat, le *smart contract* ne saurait être étendu à une telle notion, tant les conditions de réalisation (au

[277] Livre vert de la Commission des Communautés européennes sur « Le droit d'auteur et les droits voisins dans la société de l'information », 1995

[278] Arr. du 22 déc. 1981 relatif à l'enrichissement du vocabulaire de l'informatique, JONC 17 janv. 1982, p. 624

[279] Cf. *Supra*, p.74

[280] BENSAMOUN A., GROFFE J., *Création numérique – L'influence du numérique sur l'objet du droit*, Répertoire Dalloz IP/IT et Communication / Création numérique Civ., oct. 2013

[281] FINCK M., *"Blockchain Regulation",* Max Planck Institute for Innovation and Competition Research Paper Series No 17-13 SSRN Network (2017) 4.

[282] cf. Titre III, Code civil

[283] BARRAUD B, *Les blockchains et le droit*, Revue Lamy droit de l'immatériel, n° 147, avr. 2018, pp. 48-62.

[284] Par opposition au contrat à exécution successive, à savoir un contrat dont l'exécution s'effectue en un instant.

sens large) sont fondamentales pour sa bonne exécution. Surtout, considérer le *smart contract* comme une nouvelle catégorie de contrat reviendrait à considérer un élément de langage informatique comme équivalent à un contrat classique, à savoir, notamment, un accord de volonté entre deux ou plusieurs personnes, au même titre qu'il aurait été possible d'avoir la même réflexion pour les contrats issus de distributeurs automatiques. Renforcé par les premiers travaux parlementaires sur la question[285], il est alors possible de comprendre que si le *smart contract* n'est pas un contrat, il n'en demeure pas moins qu'il possède effectivement des effets juridiques[286], découlant directement de l'application qu'il peut revêtir.

194. L'approche globale utilisée pour la définition d'une *blockchain* peut s'appliquer en aval pour le *smart contract*. S'il est entendu que le *smart contract* n'est en réalité qu'une application ordonnée et informatique d'une condition particulière d'un rapport contractuel, toujours est-il qu'il en fait fondamentalement partie. Cela étant, la nécessité d'une définition juridique, dans le sens où, un *smart contract* ne reste qu'un morceau de code, n'apparaît pas comme nécessaire. Pis, la construction d'un régime *sui generis* de contrats passés à travers une *blockchain* et un *smart contract* n'apparaît pas comme nécessaire non plus, en raison d'une validité apparente du *smart contract* dans nos rapports contemporains. Enfin, le *smart contract* ne reste qu'une décomposition nouvelle d'un rapport contractuel, un nouveau moyen d'exprimer une partie d'un accord de volonté entre deux ou plusieurs personnes pour créer des effets de droit.

§2 : Un entérinement relatif des *smart contracts* dans nos rapports contractuels contemporains

195. Validant le fait qu'un *smart contract* peut avoir des effets juridiques (transfert d'actifs, blocage de serrure, etc.), il reste acquis que le *smart contract* possède déjà une place dans nos rapports contractuels contemporains. Une dichotomie entre leur validité juridique et leur appréciation doit de nouveau être réalisée à des fins de meilleure conceptualisation. Reprenant le parallèle entre matérialité et effets juridiques, il conviendra de distinguer « contrat source » et *smart contract* : le contrat-source reste le seul vrai contrat et le *smart contract* n'est

[285] DE LA RAUDIERE L., MIS J.-M., Assemblée Nationale, *Rapport d'information sur les chaînes de blocs*, n°1501, mai 2018

[286] CLÉMENT-FONTAINE M., précité.

finalement qu'une modalité d'exécution automatique du contrat source[287] ». Permettant et imposant dès lors une première intégration du *smart contract* dans nos rapports contractuels.

196. Entendu comme élément faisant partie intégrante d'un ensemble contractuel, le *smart contract* devra naturellement reprendre la loi applicable à l'ensemble contractuel de base. Pour reprendre l'exemple du *smart contract* de la société Axa[288], la loi applicable sera celle de l'ensemble contractuel de base ; et si le contrat d'assurance est régi exclusivement par la loi française, alors le *smart contract* sera lui aussi, par voie de conséquence, régit par cette même loi (cette réflexion pouvant s'appliquer également dans le cas où le *smart contract* revêtait un caractère international[289]). Là où la célèbre maxime « *Code is Law*[290] » pourrait parfaitement s'appliquer au smart contract, il conviendrait de simplement rappeler la dépendance certaine entre le *smart contract* et le reste de l'ensemble contractuel s'y rattachant.

197. Cela étant, confirmer la validité du *smart contract* peut se faire *a contrario*, en l'étudiant à partir de différents bornages déjà posés par la loi pour n'importe quel contrat. Selon le professeur Mekki[291], toute considération relative au *smart contract* présente un certain bornage, en particulier avec l'ordre public. Outre l'opportunisme - réel et justifié - pour cette question, la question de l'applicabilité de notions aussi extensibles que l'ordre public et les bonnes mœurs soulève, à notre sens, deux points fondamentaux. Le premier est la capacité du juriste à posséder une prise de recul sur tout objet juridiquement identifié (ou non), et sa capacité à appliquer de manière quasi distributive et complémentaire, différentes notions juridiques. La conception de notre droit positif reposant permet d'encadrer toute nouvelle notion, même à défaut de régulation *ex ante* ou *ex post*. Il s'agit, à propos des nouvelles technologies, de s'interroger sur l'applicabilité de ces « conceptions frontières ». S'agissant des bonnes mœurs et de l'ordre public[292], ces notions revêtant un caractère intimement lié aux pratiques sociétales et visent à maintenir un certain ordre social. À cela se rajoute le caractère général de ces notions, qui permet une application large, et par voie de conséquence à tout ensemble contractuel et au *smart contract,* ces réflexions pouvant s'appliquer à l'ensemble

[287] DARDAYROL J.-P., MARTIN J., ASTOFLI C.-P., BEAUFILS C., CSPLA, Rapp. *L'état des lieux de la blockchain et ses effets potentiels pour la propriété littéraire et artistique*, fév. 2018

[288] Cf. *Supra* p.74 et suiv.

[289] THEOCHARIDI E., *La conclusion des smart contracts : révolution ou simple adaptation ?* Revue Lamy Droit civil, n°161, 1er juil. 2018

[290] LESSIG L., précité

[291] MEKKI M., *Le smart contract, objet du droit (Partie 2),* Dalloz IP/IT 2019, p27.

[292] Art. 6, C. Civ.

des dispositions, par exemple, relatives aux clauses abusives dans le contrat de consommation[293].

198. L'intangibilité du *smart contract* est souvenu décriée notamment pour ce qu'il est de l'exécution forcée du contrat. Sans pour autant réfuter ou non l'appréciation du *smart contract* comme élément indépendant ou faisant partie d'un ensemble contractuel plus vaste, il apparaît qu'« il s'agit d'une régulation « *ex ante* »[294] », à savoir que le *smart contract*, non d'empêcher une telle exécution a plutôt tendance à vouloir l'éviter, pouvant ainsi traduire de manière informatique une nouvelle volonté de s'écarter du pouvoir d'un tiers de confiance, à savoir ici, l'intervention d'un pouvoir judiciaire. Au-delà, cette imbrication dans nos rapports contractuels en tant que solution presque préventive à des risques d'inexécution contractuelle reste une nouvelle fois un élément à prendre en compte au bénéfice d'une validité du *smart contract* dans nos sphères contractuelles, tout en l'excluant d'une définition autonome contractuelle.

199. Les questionnements sur la validité du *smart contract* peuvent également découler de la réalité - brutale - de différents événements dans la vie de l'ensemble contractuel lié. En effet, la rigueur du *smart contract*, à savoir l'incrémentation de conditions contractuelles préétablies, est à double tranchant pour sa pérennité. Si le *smart contract* présente bien des avantages pour la rigueur de son exécution (rapidité, fiabilité, exécutabilité, vélocité), elle présente aussi de potentiels freins voire obstacles ; comme l'appuie le professeur Mekki, reprenant les propos du professeur Mousseron[295], le contrat reste un outil primordial pour la gestion des risques, et si la rigueur du *smart contract* ne peut, aujourd'hui, régir les différentes caractéristiques habituelles retenues dans toute étude des risques, à savoir l'exhaustivité des scénarios à risques et leur probabilité d'occurrence. Dans des termes plus juridiques, le *smart contract* ne peut, à lui seul et sans pour autant réduire sa validité dans nos rapports contractuels, prévoir l'imprévisible ou l'irrémédiable[296]. Dès lors, sa conception technique en devient son bornage, et contribue au fait, d'une part, de considérer le *smart contract* comme simple nouvelle expression contractuelle, et d'autre part, de rappeler que le *smart contract* ne peut se suffire, en l'état actuel de la technique, à lui-même. Il en reste, de manière expectative, la

[293] RODA J.-C., *Smart contracts, dumb contracts ?*, Dalloz IP/IT 2018, p397.

[294] FAVREAU A., *L'état au défi des blockchains, régulations (s) et usages publics de la technologie blockchain*, RFPI - Numéro spécial - Fév. 2021

[295] MOUSSERON J.-M., *La gestion des risques par le contrat*, RTD civ. 1988. 481

[296] MEKKI M., *Le smart contract, objet du droit (Partie 2)*, précité.

possibilité de la promesse de l'avenir algorithmique, et de ses facultés à réduire l'expression de nos rapports contractuels à une suite logique d'opérations informatiques.

200. De manière concomitante, la question de la relation entre *smart contract* et responsabilité peut être étudiée. Si le *smart contract* ne pose en réalité que guère de difficultés dans le cadre d'une appréciation qualificative purement juridique (outre son caractère nébuleux quant à son caractère principal ou accessoire en l'état actuel de la technique), il n'en reste pas moins qu'un potentiel engagement de responsabilité subséquent à un *smart contract* peut être plus délicat. Sans faire état des différents régimes de responsabilités et les problématiques classiques liées au logiciel potentiellement appliquées au *smart contract*, qui apparaissent ici comme applicables faute de régime plus adéquat, nul doute que les aspects pragmatiques contractuels[297] du logiciel se retrouveront dans toute exploitation de *smart contract*.

201. Il convient de mentionner que le *smart contract*, si cette notion a été démocratisée de manière parallèle avec une adoption de la *blockchain*, peut très bien être considéré comme entité informatique autonome, à savoir un « morceau de code » pouvant être utilisé hors de toute *blockchain*. Une nouvelle fois, une approche globale et même une méthodologie d'approche globale des différents éléments gravitant autour d'une *blockchain* doit être préférée pour mieux en saisir les tenants et aboutissants, faute de quoi certains éléments ne pourront bénéficier d'un régime adéquat et rendront délicate toute position procédurale offensive ou défensive dans la pratique et autres contentieux liés à un *smart contract*. Cette automatisation des rapports contractuels, du moins en partie, dont la réalisation sera l'apanage de juristes spécialisés, et dont la résolution des litiges sera sans doute particulière car faisant appel à des experts spécifiques est un premier pas vers un numérisme juridique[298] de plus en plus exacerbé. Ce même numérisme conduisant d'ailleurs à d'autant plus de spécialisation, et de modernisation des pratiques contractuelles mettant en œuvre une *blockchain* et/ou un *smart*

[297] D'ASSIGNIES R., LECARDONNEL M. *Responsabilités et logiciels libres*, Agence pour la Protection des Programmes, 2021, disponible à :https://www.app.asso.fr/centre-information/publications/responsabilite-et-licences-libres (consulté le 19/10/2020). À titre d'exemple, les différentes obligations d'information ou encore de mise à disposition des codes sources (en fonction des licences libres utilisées) seront de mise lors de toute utilisation de *smart contract*.

[298] Sur ce mouvement, v. not. MEKKI M., *L'intelligence artificielle et le contrat, in Le droit de l'intelligence artificielle*, Lextenso, 2019, p.70 et suiv.

contract, compte tenu du fait que tout contrat n'est pas, aujourd'hui, adapté à une telle modernisation[299].

202. Le *smart contract* ne reste que l'expression informatique d'un choix juridique préalable ; il n'est qu'un résultat[300] et non un moyen d'obtention. Il conviendra de constater que cette affirmation est déjà partagée par une partie de la doctrine[301], et doit, à notre sens, être validée. Il s'agirait plutôt d'une émanation numérique d'un contrat, dont le formalisme conduit à être inscrit sur une *blockchain*. Il n'est qu'une application technique et automatique d'un contrat ou d'une relation contractuelle au sens juridique du terme.

[299] TOUATI A., *Tous les contrats ne peuvent être des smarts contracts,* Revue Lamy Droit civil, n°147, 1er avril 2017

[300] CLÉMENT-FONTAINE M., *Le smart-contract et le droit des contrats* : dans l'univers de la mode, Dalloz IP/IT 2018, p.540

[301] RODA J-C, MEKKI M., précités

Conclusion du Chapitre 2

203. L'appréhension du *smart contract* conduit à l'appréhension d'un monde économique, social et juridique de plus en plus numérique, voire digitalisé[302]. Toutefois, l'apparition de tels protocoles informatiques si particuliers que sont les *blockchain*s mettent en évidence une modernisation de nos rapports civils, qu'ils soient entendus au moment de leur formation (via un *smart contract*) ou via leur exécution (et donc les rapports que peut avoir la *blockchain* dans les différents modes de preuve).

La récente analyse de la FFBP[303] met en avant le fait que l'une des réticences dans une démocratisation de ce nouvel outil informatique réside notamment dans les incertitudes légales liées au droit de la preuve[304] et les possibilités offertes pour la *blockchain*, en particulier la valeur légale d'enregistrements produits grâce à une *blockchain*. Or, les précédentes démonstrations ont su mettre en avant que la *blockchain*, si elle est parfaitement compatible avec notre système de preuve actuel, n'en reste pas moins intéressante une nouvelle fois pour le moderniser, notamment pour créer un nouveau mode d'enregistrement, fiable, pratique, sécurisé, mais pas pour autant supérieur à un autre mode de preuve[305]. S'agissant des *smart contracts*, le bornage et la souplesse du droit actuel des obligations n'enlève en rien les attributs de la *blockchain* au service de la modernisation de nos rapports contractuels, pris dans un ajout substantiel de l'automatisation et la diabolisation de ces rapports. L'inscription en *smart contract* de différents termes ou conditions faisant ainsi pencher la balance vers un « *Code is Law* [306] », immédiatement contrebalancée par les différents bornages et autres règles découlant de notre droit des obligations, inscrivant un équilibre subtil mais nécessaire, un *« Balance is Code and Law »* assumé et de plus en plus nécessaire dans cette constante évolution numérique de notre société.

---

[302] Pour les nuances entre numérique et digital, dont le second terme invite à une transformation en profondeur, voir : MOATTI A. *Le numérique rattrapé par le digital ?. Le Débat,* Gallimard, 2016.

[303] Fédération Française des Professionnels de la *Blockchain*, https://www.federation-*blockchain*.fr/accueil/

[304] Rapport FFPB - Chiffres clés - Oct. 2020, disponible à https://drive.google.com/file/d/1sfhwYcjJOcPRRSrzvnTTjv_QiwGLKxa0/view, consulté le 29/10/2020

[305] Rappelons que l'inscription des actes passés par *blockchain* ne saurait avoir un caractère authentique tant ce caractère est déterminé par la qualité de l'agent signant l'acte plutôt que par la méthode utilisée.

[306] LESSIG L., précité.

Conclusion du Titre 1

204. Depuis 2015, la démocratisation de la technologie *blockchain* a pu passer par différents stades d'appropriation. Aujourd'hui visée par un cycle de désillusion[307]. La *blockchain* a su, dans un premier temps, être considérée comme ayant un caractère hautement disruptif, dans le sens sa première réalisation, le *Bitcoin*, a été créé en réaction à un système financier jugé améliorable, ayant causé de forts ravages économiques et sociaux. Appréhendée ensuite par ses facultés de désintermédiation, tout en garantissant fiabilité et sécurité des échanges (*via* l'apparition d'*Ethereum* majoritairement), ses caractéristiques techniques font l'objet de différentes expérimentations (gestion de droits d'auteurs[308], horodatage de diplômes[309], etc.) poussant ainsi à un éclatement extrêmement fort des différents cadres applicables et surtout à appliquer pour l'appréhension de cette technologie. Invitant ainsi à se poser la question de savoir ce qu'est, aujourd'hui, un « expert *blockchain* », tant les domaines d'application sont vastes. En réalité, cet éclatement n'est que conséquence de l'essence même de la technologie, et comprendre la philosophie sous-jacente à cette dernière parait bien plus opportun que la recherche - quasi fantasmagorique - de la maîtrise de l'ensemble des pans techniques et juridiques reliés à la *blockchain*.

205. L'appréhender dans une démarche souple et globale, en se focalisant sur les contours stratégiques de cette technologie, comme sa place dans notre système de preuve ou encore la validité des *smart contracts* apporte plus à sa compréhension. Dès lors, une invitation à une réflexion plus large, notamment sur l'essor de nouvelles technologies fondées sur l'architecture et la gouvernance de données, entendues comme étapes indispensables à l'étude d'une *blockchain* s'impose naturellement. S'il est entendu classiquement que les données sont le nouvel or noir [310] de ce siècle, cette approche stratégique, et non plus purement opérationnelle, de l'utilisation de données s'impose. La *blockchain* n'a pas simplement créé

[307] PANETTA K., *5 Trends Emerge in the Gartner Hype Cycle for Emerging Technologies*, Gartner, 05 nov. 2019, disponible à : https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/, consulté le 03/11/2020. Le cabinet de conseil Gartner a publié, en 2018, un graphique cherchant à modéliser les différentes phases d'appropriation d'une technologie ; on pourra constater que la technologie *blockchain* entrait, en 2018, dans une phase de désillusion.

[308] Par exemple : https://ujomusic.com/

[309] Par exemple : https://www.bcdiploma.com/index-fr.html

[310] FONTAINE M., *La donnée numérique : l'or noir du XXIe siècle ?* LPA 8 sept. 2017, n° 129, p.90

ou détruit des systèmes de données (actuels ou à venir), elle n'a fait, en réalité, que transformer l'approche que nous pouvons en avoir.

Titre 2 : Une émergence perturbée d'un nouveau modèle de gouvernance

« Celui qui doit s'acquitter dans un temps à venir, et à qui on fait confiance, est dit tenir sa promesse, être fidèle à sa parole, et, s'il ne s'acquitte pas, dans le cas où c'est volontaire, on dit qu'il viole sa parole. »

Léviathan, 1651, Thomas Hobbes (1588-1679)

206. En France, la notion de gouvernance est plutôt récente, et pour réaliser une adaptation de ce concept historiquement anglo-saxon, les rapports Viénot I et II[311] ont pu définir la notion de « gouvernement d'entreprise », dans le sens où il s'agit d'une doctrine impliquant « qu'une société est gérée dans l'intérêt commun de l'ensemble des actionnaires et non dans celui du groupe majoritaire ou des organes dirigeants »[312]. Cette notion de gouvernement d'entreprise a pu évoluer vers la notion, plus générale, de gouvernance. Comme le précise le professeur Supiot, « le propre de la gouvernance est en effet de reposer non pas sur la légitimité d'une loi qui doit être obéie, mais sur la capacité commune à tous les êtres humains d'adapter leur comportement aux modifications de leur environnement pour perdurer dans leur être[313] ». Dans une application récente aux données (personnelles ou non), la Commission Européenne fait référence à « l'existence de structures et de processus permettant de partager les données de manière sécurisée, notamment par l'intermédiaire de tiers de confiance[314] ».

207. *De facto*, la gouvernance tend vers la capacité d'acteurs - le plus souvent privés et d'une taille importante - à s'autoréguler à travers la mise en place de documentations

[311] Ces missions de rédaction de rapports ont été confiés par le Conseil national du patronat français (CNPF) et l'Association française des entreprises privées (AFEP) début 1995. Ces réflexions ayant été affinées avec le Rapport Bouton (2003).

[312] Gouvernement d'entreprise, Fiche d'orientation, juil. 2019, Dalloz

[313] SUPIOT A., précité.

[314] Règlement sur la gouvernance des données – Questions et réponses, Bruxelles, le 25 nov. 2020, disponible à https://ec.europa.eu/commission/presscorner/detail/fr/QANDA_20_2103 ; à ce sujet, on pourra regretter l'absence d'une telle définition au sein de la proposition de règlement sur la gouvernance européenne des données (Proposition de Règlement du Parlement Européen et du Conseil sur la gouvernance européenne des données (acte sur la gouvernance des données), 25/11/2020, COM/2020/767 final, disponible notamment à https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A52020PC0767)

spécifiques, comme la gestion de l'éthique,, la rémunération des dirigeants, ou encore les stratégies d'entreprise. Il s'agit d'un mécanisme d'autocontrôle, dans le sens où une entreprise édictant des documentations de gouvernance va, d'elle-même, se soumettre à ces mêmes documentations.

208. Éclatant une nouvelle fois les différents cadres d'appréhension et dépassant ainsi une possible compréhension globale simple, liée à l'omniprésence numérique, la technologie *blockchain* bénéficie d'un cadre actuel particulier, lié à sa matière première, les données. Propres d'un univers numérique à portée quasi universelle, dans le sens où il est présente des difficultés d'appréhension « à la fois épistémologique, institutionnelle et sociale, voire économique et politique (presque tous les secteurs – publics ou privés, institutions culturelles, etc. – sont concernés)[315] », ces données et leurs utilisations font apparaître des schémas disparates d'utilisation, pouvant être liés aussi bien à des matières purement économiques (gouvernance financière liée aux transactions par cryptoactifs), ou purement numériques (gouvernance autour de la protection des données personnelles par exemple).

En réalité, l'appréciation de cette technologie paraît une nouvelle fois désordonnée dans le sens où n'importe quel chercheur ou essayiste se retrouverait confronté à une multitude de secteurs d'applications et donc d'appréciations toutes aussi différentes. Toutefois, dans une mesure propre au domaine numérique, certaines constantes peuvent être identifiées. En premier lieu, il va être aisé de constater une lacune étatique sur la gouvernementabilité des données (Chapitre 1) lacune qui a pu permettre aux grands acteurs du numériques d'imposer leurs pratiques et leurs méthodes de gouvernance des données (Chapitre 2), bien que la *blockchain*, si elle est utilisée par ces acteurs[316], ne reste qu'un outil au service de cette gouvernance.

[315] DOUEIHI M., *Qu'est-ce que le numérique ?*, Presses Universitaires de France, 2013
[316] VERGARA I., *Facebook fait une première acquisition dans la blockchain*, Le Figaro, 05/02/2019

Chapitre 1 : Des lacunes étatiques sur la gouvernementabilité des données

209. Les récentes innovations législatives (française ou européennes) reliées à l'univers numérique (et en particulier sur l'usage de la donnée au sens large) ont été rendues nécessaires par le constat d'un accroissement du pouvoir d'acteurs privés - pour ne pas les nommer, les GAFAMI[317] ou encore les BATX[318] - au détriment d'un constat d'une lacune d'un pouvoir étatique sur la gouvernance des données personnelles en particulier. L'absence de ce pouvoir de gouvernance étatique n'est pour autant une condamnation des politiques publiques en ce sens, néanmoins, l'étude de ce favoritisme de prérogatives étatiques *a priori* (Section 1) nous permettra de mettre en exergue la nécessaire question de la portée des certifications et autres codes de conduites que les acteurs de droit privé sont invités à mettre en place en contrepartie, permettant un contrôle *a posteriori* de la gouvernance des données (Section 2).

Section 1 : De l'abandon de prérogatives étatiques *a priori*

210. L'avènement de technologies telles que la *blockchain*, prise au sein d'un environnement numérique de plus en plus proéminent pousse notamment le législateur à s'ouvrir vers « de nouvelles formes de régulation, dans lesquelles l'État et les institutions administratives, judiciaires et financières vont occuper une nouvelle place, une place différente[319] ». Cette place différente peut être comprise dans le sens où il serait possible de considérer l'État dans une position d'état-gendarme[320] poussé à l'extrême[321], occupant ainsi

[317] Cet acronyme est utilisé pour identifier les plus grandes puissances numériques actuelles, à savoir Google, Apple, Facebook, Amazon, Microsoft et IBM, qui sont des acteurs américains.

[318] Compte des positions politiques chinoise, en réponse à l'omniprésence américaine dans l'univers numérique, la Chine a su soutenir des entreprises nationales, les BATX désignent alors des entreprises chinoise particulièrement puissantes (et grandissantes) dans l'univers numérique, à savoir Baidu, Alibaba, Tencent et Xiaomi.

[319] FAVREAU A., *L'état au défi des blockchains, régulation(s) et usages publics de la technologie blockchain*, RFPI, numéro spécial, fév. 2021

[320] Sur la théorie de l'état-gendarme : MARTIAL M., *État-gendarme*, dans : KADA N., éd., *Dictionnaire d'administration publique.* FONTAINE, Presses universitaires de Grenoble, « Droit et action publique », 2014, p. 209-210. URL : https://www.cairn.info/dictionnaire-d-administration-publique--9782706121371-page-209.htm

[321] Par opposition à la théorie de l'état-providence : MERRIEN François-Xavier, *L'État-providence.* Paris cedex 14, Presses Universitaires de France, « Que sais-je ? », 2007

une place plus en retrait, intervenant seulement en cas de contrôle ou de manquement flagrant au droit positif. L'univers numérique, dont le basculement vers un abandon de prérogatives étatiques *a priori* se tient en raison de l'évolution même de la société à travers l'émergence de technologies toujours plus poussées et invitant même à les considérer « non plus comme (un) objet de régulation, mais comme (un) outil de la régulation[322] », la technologie *blockchain* en étant le parfait exemple, en raison de ses attraits et applications diverse[323]. Cet abandon de prérogatives *a priori* se démontre d'une part à travers une dévolution de prérogatives étatiques dans le monde numérique (§1) mais également dans une nécessaire inertie législative comme axe d'évolution (§2).

§1 : Une dévolution de prérogatives étatiques dans le monde numérique

211. L'abandon (ou la perte) de prérogatives étatiques de contrôle *a priori* ne doit pas être entendu comme un abandon pur et simple de tout contrôle (en dehors de celui du Juge). La réalité est qu'il possible de partir du postulat suivant : il est plus facile de contrôler que de mettre en place. Ce postulat pourra être vérifié par la revue et la mise en œuvre de nouvelles dispositions législatives et réglementaires adéquates autour de la manipulation de données personnelles ou non personnelles.

212. S'il est possible d'avancer qu'il s'agit d'une facilité de la part du législateur de laisser le soin au juge de contrôler *a posteriori* des usages technologiques et en ne réalisant qu'une initiative législative pour contrôler également *a posteriori* des comportements se retrouvant litigieux par l'essor de leurs pratiques, il en ressort un certain art de la part du législateur de poser des principes qui ont vocation à être suffisamment efficaces seuls pour pouvoir se limiter à cette conception *a priori*. Cet art restant conséquence de l'affaiblissement du pouvoir étatique face à la gouvernance d'Internet[324]. Le droit de la protection des données personnelles est un parfait exemple pour une démonstration d'abandon de prérogatives *a priori*. En effet, le droit des données personnelles, marqué en premier lieu par le Code civil[325] et la loi

[322] FAVREAU A., précitée.

[323] On rappellera que la technologie *blockchain* peut trouver attrait aussi bien dans le transfert d'actifs que dans la gestion de données *stricto sensu.*

[324] FAVRO K., *Introduction, Open Data : une révolution en marche,* Legicom 2016, p.3

[325] Art. 9, al. 1 C. Civ : « Chacun a droit au respect de sa vie privée. »

Informatique et Libertés[326], reposait en premier lieu sur une logique déclarative. À savoir que tout responsable de traitement[327] devait respecter une série d'obligations déclaratives afin de soumettre au contrôle de l'autorité de contrôle compétente[328] tout traitement de données personnelles, afin d'en avoir validation (ou non) préalablement à sa mise en place. À l'aune du droit positif[329], la quasi-totalité[330] de ces obligations préalables a disparu, pour laisser la place à une mouvance beaucoup plus actuelle et adaptée à l'univers numérique qui est un régime de conformité[331].

213. Au-delà de conceptions d'un point de vue purement juridique, l'avènement de technologies toujours plus complexes dans l'univers numérique imposant des changements de paradigmes dans la conception même de la norme juridique, est corroboré par l'importance grandissante des GAFAMI et autres acteurs puissants dans cet univers. En témoigne par exemple la nomination d'un ambassadeur auprès de ces derniers au Danemark[332]. Au surplus, toute étude de l'impact d'une technologie comme la *blockchain* ne doit pas omettre une réalité purement scientifique : un protocole informatique ne reste qu'une expression littérale de théories et applications mathématiques.

Comme le rappelle John Law[333], dès le XVIIIème siècle, tout fonctionnement monétaire reposant sur les mathématiques, il paraît illusoire de vouloir interdire ces

[326] Loi n° 78-17 du 6 janv. 1978 relative à l'informatique, aux fichiers et aux libertés, dite LIL ou Loi informatique et libertés

[327] Loi n° 78-17 du 6 janv. 1978, précitée, art. 3 ; sachant que la définition du responsable de traitement a été reprise au sein du « RGPD », et est défini comme « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre »

[328] À savoir ici, la Commission Nationale de l'Informatique et des Libertés (CNIL).

[329] Constitué notamment par la loi n°78-17 du 6 janv. 1978 (précitée) et du RGPD.

[330] On notera que certaines obligations déclaratives ont été conservées, notamment quand un traitement de données personnelles présente des risques importants pour les droits et libertés des personnes concernées. Pour plus d'informations à ce sujet : https://www.cnil.fr/fr/declarer-un-fichier.

[331] La notion de conformité à des règles préétablies est partie intégrante de l'application du RGPD ; il est possible de retrouver plusieurs occurrences de ce terme au sein de ce règlement, dès son considérant 74. Le principe de conformité - en matière de protection des données personnelles - imposant à un responsable de traitement de pouvoir justifier à tout moment du respect des dispositions en vigueur, et non plus à prouver la validité de ses actions comme ce fut le cas avec l'ensemble des obligations déclaratives réalisées auprès des autorités de contrôle compétentes.

[332] The Local, *In world first, Danemark to name a « digital ambassador »*, 27 janv. 2017

[333] Économiste et banquier écossais, il est considéré, en France, comme le père de la finance et de l'utilisation du papier-monnaie à la place des espèces métalliques.

dernières[334]. S'oppose alors au législateur une impossibilité matérielle de régulation de telles technologies. Par extrapolation, toute tentative de régulation d'une technologie devrait se concrétiser en une expression tout aussi technologique de cette dite régulation. Pour prendre une métaphore tout aussi cinglante, toute norme voulant contredire une addition (par exemple « 1+1=2 ») devrait être elle-aussi une addition (par exemple : « 1+1=3 »). Or, il paraît logiquement, et sans jugement de valeur, illusoire de demander au législateur d'être également fin mathématicien.

214. L'univers numérique n'est pas la première matière à avoir pu subir les critiques d'un potentiel abandon de prérogatives étatiques. Comme le mentionnait le professeur Loquin[335], qui faisait état de réflexions sur la nature de l'arbitrage par rapport à la *lex mercatoria*. Ce dernier notait notamment que l'existence de l'arbitrage, sans être un abandon de prérogatives étatiques sur le règlement des litiges, restait un seul moyen alternatif de règlement des litiges et qu'à ce titre, le pouvoir régalien ne perdait rien de ses prérogatives souveraines (à savoir notamment le pouvoir de rendre justice). En ce sens, certains auteurs[336] corroborent la montée en puissance d'une *lex electronica,* permise notamment par un potentiel règlement des litiges de manière automatique, à travers l'utilisation de *smart contracts* adaptés. Non seulement l'émergence d'une telle *lex electronica* n'a rien de préjudiciable pour le pouvoir étatique, mais au contraire, il peut témoigner d'un gain de maturité par rapport à cette matière[337]. De manière parallèle, l'apparition de juridictions et autres institutions particulière destinées à certaines matières exclusives, à l'instar des procédures Syreli pour les noms de domaines, témoigne en premier lieu d'une adaptation du cadre légal applicable[338] plutôt que comme un abandon d'une quelconque prérogative étatique. C'est en ce sens qu'une inertie apparaît comme nécessaire, le temps d'éprouver les usages du monde numérique afin de mieux en réguler les aspects.

---

[334] LAW J., *You can't beat the numbers, signs of the times, and full marx for bitcoin*, Coindesk, 28 fév. 2014. En l'occurrence, il s'agit ici d'un article éponyme reprenant les différents travaux de l'économique John Law.

[335] LOQUIN E., *L'amiable composition en droit comparé et international*, Litec, 1980, pp. 308-309

[336] À ce sujet, notamment : JEAN B., DE FILIPPI P. *Les Smart contracts, les nouveaux contrats augmentés ?*, Conseils et Entreprises, Avocats Conseils d'Entreprise, 2016, disponible à https://hal.archives-ouvertes.fr/hal-01676878 ou encore LESSIG L., précité

[337] Il est d'ailleurs possible de constater l'émergence d'une dualité entre lex mercatoria et lex electronica ; pour exemple : MAKROUM N., FONTAINE C., *La prise en compte de la blockchain par l'arbitrage international en ligne*, 7 oct. 2020, disponible à *https://www.clubdelarbitrage.com/post/makroum-fontaine-la-prise-en-compte-de-la-blockchain-par-l-arbitrage-international-en-ligne*

[338] On rappellera que la procédure SYRELI a été instituée par l'AFNIC (Association Française pour le Nommage Internet en Coopération) en novembre 2011.

§2 : L'inertie législative apparemment contrôlée comme axe d'évolution

215. L'univers des nouvelles technologies, qui, de manière littérale, ne cesse d'évoluer nécessite une constante adaptabilité du cadre légal applicable. Sans retracer dans le cadre de cette étude l'immensité des évolutions légales induites par l'émergence de technologies poussant le législateur à réagir d'une manière plus ou moins prompte et surtout efficace dans certains domaines[339, 340]. L'émergence de la technologie *blockchain* pousse dès lors à s'interroger sur l'opportunité ou non de règles de droits nouvelles et novatrices.

216. Au-delà, comme le souligne le courant réaliste du droit, la simple existence d'une norme ne garantit en rien son aptitude à remplir sa fonction première qui est de garantir le respect des principes fondamentaux qui sont à l'origine de la norme[341]. S'agissant d'une application à la technologie *blockchain*, le professeur Yeung décrivait qu'il était primordial d'étudier la motivation intrinsèque dans l'utilisation d'une telle technologie, motivation qui peut être triple : « échapper délibérément aux contraintes de fond des *blockchain*s (évasion hostile), compléter le droit conventionnel pour le rationaliser (alignement efficace), et coordonner les actions entre et parmi les multiples participants en évitant les inefficacités procédurales (atténuation des frictions transactionnelles)[342] ». Au demeurant, le respect de principes et droits fondamentaux doivent également être indispensables à tout tentative de régulation. D'une manière plus générale, et appliquées à d'autres secteurs de hautes technologies, la Commission Européenne, s'agissant de l'IA, invite également à ce que la

[339] DEJEAN S, PENARD T. et SUIRE R., *Une première évaluation des effets de la loi Hadopi sur les pratiques des internautes français*, 2010 (http://www.marsouin.org)

[340] A l'inverse, la création de la HADOPI (Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet) en 2009, a été fréquemment décriée pour son manque d'efficacité, par exemple : LELOUP D., *Dix ans après la loi Hadopi, que reste-t-il du téléchargement illégal*, Le Monde, 12 juin 2019

[341] Le réalisme est un courant de la théorie générale du droit, qui se définit comme une attitude ou, comme aurait dit Bobbio, une approche, consistant à vouloir décrire le droit tel qu'il est réellement. Tel qu'il est et non tel qu'il devrait être selon telle ou telle philosophie morale ou politique. TROPER M. *Le réalisme et juge constitutionnel,* Cahiers du Conseil constitutionnel, n°22 juin 2007

[342] LOCKETT-YEUNG, K, *'Regulation by blockchain : the emerging battle for supremacy between the code of law and code as law'* Modern Law Review, 2018

régulation en la matière s'attache notamment à la protection de ces droits fondamentaux[343] avant tout, sans pour autant emporter une régulation précise et appliquée à tel ou tel domaine.

217. À l'heure actuelle, et prenant compte de la spécificité de la technologie *blockchain*, le législateur n'a pas réglementé autrement qu'à travers la gestion d'actifs financiers (et de manière plus générale, sur des aspects fiscaux liés à l'exploitation de la technologie *blockchain*, à travers, notamment, de l'imposition des plus-values réalisées sur la cession de cryptoactifs, ou actifs numériques[344]).

218. Cette position, outre l'opportunisme flagrant pour la mise en place d'une nouvelle source d'imposition basée sur des revenus d'un nouveau type, est à saluer. En effet, et comme rappelé précédemment, la régulation - en soi - de la technologie *blockchain* n'aurait aucun sens tant elle viendrait seulement être une tentative vaine de la régulation des mathématiques. Seul l'usage de la technologie peut être régulé ; ce faisant, le législateur s'efforce, dans un premier temps, de combattre ce que le professeur Yeung considérait comme une volonté d' « évasion hostile ». Cela étant, le législateur a su également réguler les acteurs du marché des cryptoactifs, en particulier les prestataires de services sur actifs numériques[345], régulation instaurée par la loi PACTE[346], mettant en avant le respect d'une fiscalité étatique comme droit fondamental avant même la protection de la liberté économique ou la protection de la vie privée. De part cette protection d'intérêts fondamentaux, le législateur peut apparaître comme contrôlant une certaine inertie législative, mettant en avant des choix prioritaires plutôt que de faire le choix d'un ensemble exhaustif de réglementations.

En réalité, il convient, en particulier pour la *blockchain*, de s'interroger sur le caractère dispensable ou non de la création ou l'évolution d'une norme. Cette réflexion, au demeurant

---

[343] «*Against this political context, the Commission puts forward the proposed regulatory framework on Artificial Intelligence with the following specific objectives: • ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values ; (…) ; enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems (…)* » - Proposal for a regulation of the european parliament and of the concil laying down harmonised rules on artificial intelligence act and amending certain union legislative acts, 2021/0106 (COD), 21 avril 2021

[344] BOFIP-BOI-BNC-CHAMP-10-10-20-40, 03/02/2016

[345] https://www.amf-france.org/fr/actualites-publications/actualites/prestataires-de-services-sur-actifs-numeriques-le-dispositif-pacte-en-detail (consulté le 19/12/2019)

[346] Loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises (1)

nécessaire, nous renvoie aux réflexions sur l'inflation législative qu'ont pu être étudiés précédemment[347], comme le rappelait l'auteur Isaac Asimov, dans une appréciation restant parfaitement contemporaine, « si je vous comprends bien, nous sommes sur la bonne voie : il est urgent d'attendre »[348]. Renvoyant bien à un abandon, quoique provisoire, de prérogatives étatiques au profit de la montée en puissance des techniques de gouvernance.

Section 2 : Vers un contrôle de la gouvernance *a posteriori*

219. La montée en puissance de technologies nouvelles, permettant l'hégémonie de systèmes organisationnels et financiers distincts, et voués à échapper à une norme préétablie[349] est d'autant plus problématique que « leur encadrement par le droit pose d'autant plus de difficultés qu'elles sont en partie conçues pour lui échapper[350] ». Un changement de considération du législateur pour ces technologies, passant donc notamment par un changement de paradigme du contrôle (passant d'un contrôle *a priori* à un contrôle *a posteriori*) est donc naturellement nécessaire pour permettre une régulation de ces dernières. Néanmoins, la méthode de régulation de ces technologies, en particulier celle de la *blockchain*, ne nécessite pas la consécration de nouvelles méthodes ou techniques. En effet, les techniques et théories autour de la gouvernance et de la conformité sont d'ores et déjà connues par le droit positif ; au-delà, la *blockchain* peut être devenir un maître outil en la matière car ces attributs techniques permettent de concrétiser un lien fondamental et immuable entre des comportements et les données qu'ils peuvent produire[351]. La *blockchain* permet alors d'être témoin d'un nouveau concept de gouvernance au sein de l'univers numérique (§1), mais elle devient surtout un outil de gouvernance pour la gestion de données (§2).

[347] Cf. note n°160

[348] ASIMOV I., *Le cycle de Fondation, tome 1 : Fondation*, Galimard-Jeunesse, 1951

[349] Nous rappellerons ici la volonté initiale de Satoshi NAKAMOTO à vouloir s'émanciper du système financier actuel, marqué par les précédentes crises monétaires, dans une démarche quasi anarchiste en rejet du système monétaire actuel.

[350] LAVAYSSIERE X., *L'émergence d'un ordre numérique*, AJ Contrat 2019, p.328

[351] Étant entendu que la notion de donnée est entendue ici comme produit informationnel d'un comportement considéré.

§1 : Un nouveau concept de gouvernance au sein de l'univers numérique

220. La prise de position régalienne tendant à laisser une place importante aux acteurs de l'univers numérique pour leur propre régulation n'est pas une nouveauté intrinsèquement liée à cet univers. La faculté des acteurs à entrer dans une démarche d'autorégulation, et de se conformer aux décisions *a posteriori* d'une autorité de contrôle est déjà bien connue dans le monde de la finance[352]. Cette faculté répond dans une certaine mesure à une définition de la conformité[353], qui peut demeurer aujourd'hui empirique[354], à savoir un comportement interne et positif d'un acteur souhaitant s'approprier un corpus réglementaire afin de réduire un risque juridique[355] en amont de tout contrôle.

Cette démarche d'autocontrôle, rattaché à une gestion d'un risque juridique peut être résumé au respect d'un principe de conformité qui, au demeurant, peut être défini comme « un ensemble de techniques, juridiques et de gestion, dont la mise en œuvre est imposée aux entreprises de taille significative dans le but de contrôler l'application effective des règles juridiques et éthiques qui leur sont applicables et de diminuer le risque d'infraction à ces règles[356] ». Comme rappelé précédemment[357], le principe de conformité a déjà sens dans l'univers financier[358], imposant aux acteurs concernés de mettre en place une série de verrous de contrôles internes pour réduire un tel risque. En reste d'ailleurs que les concepts de conformité au sein de l'espace financier sont basés notamment sur des objectifs de transparence et d'efficacité[359].

---

[352] Il est fait ici référence à l'Autorité des Marchés Financiers.

[353] Étant entendu, ici, que la notion de conformité ne se confond pas avec la notion homonymique du défaut de conformité tel qu'il peut être défini au sein du code de la Consommation (articles L217-4 et suivants).

[354] SOUTY F., *Entreprises, concurrence, conformité : définition empirique de la compliance*, Revue Lamy de la concurrence, Nº 55, 1er nov.2016

[355] BENSSOUSSAN A., *Risque juridique, conformité, diversité et classification des risques*, https://www.alain-bensoussan.com/wp-content/uploads/22919251.pdf

[356] GAUDEMET A., *Qu'est-ce que la compliance ?*, Revue Commentaire 2019/1 (Numéro 165), pages 109 à 114, disponible à https://www-cairn-info.scd-rproxy.u-strasbg.fr/revue-commentaire.htm

[357] BOCQUILLON S., CAMUS R., *L'opportunité d'une gouvernance transverse des données*, Revue Banque, n°810, Juil.-Août 2017 ; notamment pour faire le lien entre conformité bancaire et aux règles de protection des données

[358] LEVY-GARBOUA V., *La compliance : au-delà des sentiers bancaires*, SciencesPo, 5 fév. 2016, disponible à : https://www.sciencespo.fr/executive-education/la-compliance-au-dela-des-sentiers-bancaires (consulté le 15/12/2019)

[359] Directive 2004/39/CE du Parlement européen et du Conseil du 21 avril 2004 concernant les marchés d'instruments financiers, modifiant les directives 85/611/CEE et 93/6/CEE du Conseil et la directive 2000/12/CE du Parlement européen et du Conseil et abrogeant la directive 93/22/CEE du Conseil

221. Au-delà même de l'application de ce concept à l'univers numérique, il convient de noter le plaidoyer de plus en plus répandu en faveur l'émergence d'une telle responsabilité *a priori* pour l'ensemble des acteurs de l'univers numérique[360]. La prise en compte de ces nouveaux acteurs reste une démonstration du renforcement de régimes de gouvernance et de conformité, témoignant une nouvelle fois d'un certain favoritisme pour les opérations de contrôle *a posteriori*, déléguant la vérification de la conformité au droit positif non plus à l'État mais aux acteurs directement concernés. Cela permettant des délégations stratégiques et opérationnelles, nécessaire à l'essor de nouvelles technologies comme la *blockchain*. En témoigne notamment les projets de règlement dits « DMA/DSA[361] », qui, dans une tendance propre à la conformité, invitent les acteurs visés dans une démarche d'autocontrôle et de respects de principes simples, comme la limitation des pratiques déloyales ou encore la preuve de la mise en place de mécanismes permettant aux utilisateurs de signaler du contenu illicite.

En particulier, l'émergence des problématiques sous-jacentes à l'adoption de la technologie *blockchain* (en particulier pour ses avantages pour le transfert d'actifs), comme celles relatives au suivi des opérations ou encore à la lutte contre le blanchiment font écho à des volontés de transparence. En ce sens, le secteur financier paraît de plus en plus relié à l'univers numérique [362] et ne font que témoigner d'une prise de conscience nécessaire permettant de faire le lien entre cet univers numérique et l'univers financier. Cela étant, la montée en puissance de régimes de conformité numérique n'est pas sans rappeler une volonté de dresser une « responsabilité numérique[363] » des acteurs. Ces débats ont d'ores et déjà lieu sur la responsabilité liée aux robots[364].

Ces développements autour de la responsabilité de ces acteurs, et en conséquence des outils au service de leur régulation ne sont pas uniquement fondés sur une simple responsabilité ou une nécessaire transparence sur l'utilisation des données et des autres outils

[360] LAVAYSSIERE X., précité.

[361] *Proposal for a Regulation of the european Parliament and of the Concil Council on contestable and fair markets in the digital sector, Digital Markets* Act, 15 déc. 2020, COM/2020/842 final

[362] DIALLO, M., *L'intelligence artificielle et le dispositif de conformité des banques*, RISF, 01/01/2020, 2020-1, pp.88-94

[363] G'SELL F., *Vers l'émergence d'une « responsabilité numérique ?*, Dalloz IP/IT 2020. p.153

[364] Par exemple : NEVEJANS N., *Le robot, responsable ? À propos de la Première Loi de la Robotique d'Asimov,* RFPI, 01/03/2020, pp.15-29

d'exploitation de ces données[365] (notamment les algorithmes utilisés pour leur véhiculer leur véritable valeur ajoutée), la « question du contrôle de ces données et du système technique qui les gère est ainsi devenue une question cruciale des stratégies géopolitiques en recomposition[366] » et en corollaire, une question importante en terme de souveraineté numérique[367].

222. Néanmoins, parler de nouveaux modèles de conformité au sein de l'univers numérique ne doit pas pour autant sous-entendre la création d'une gouvernance d'Internet. En effet, le concept même de conformité appelle de manière subséquente le concept de gouvernance. Aujourd'hui considéré comme réseau quasi universel, bien que pensé dans une approche restreinte[368], Internet ne demeure qu'une compilation de réseaux tout aussi différents et hétéroclites. Il pourrait être plus juste de parler d'internets, au pluriel, plutôt que de parler d'un seul et même réseau, tant les utilisations peuvent être diverses et variées. En ce sens, la technologie *blockchain* ne demeure qu'un réseau *P2P*, pouvant être considéré en marge d'un réseau mondial[369]. Dès lors, l'émergence de nouveaux concepts de gouvernance, adapté à la technologie *blockchain* ne serait être qu'un exemple de gouvernance et de régime de conformité, tant « les enjeux et les sujets abordés sont différents[370] ». Plus loin encore, il conviendrait alors de considérer la *blockchain* non pas comme objet de gouvernance des données, mais bien comme outil, tant la structuration des données et intimement rattachée à la mise en œuvre d'un tel réseau.

§2 : Le caractère utilitaire de la *blockchain* au service de la gouvernance

223. En amont de tout développement analysant la *blockchain* comme outil et non pas comme objet de droit, il est important de comprendre qu'une *blockchain*, ne reste qu'une

---

[365] DE POORTERE C., *Gouvernance algorithmique : 3 questions à Antoinette Rouvroy et Hugues Bersini*, Pointculture, 2 déc. 2019, disponible à : https://www.pointculture.be/magazine/articles/focus/gouvernementalite-algorithmique-3-questions-antoinette-rouvroy-et-hugues-bersini/ (consulté le 15/12/2020)

[366] BYK C., *La souveraineté numérique à l'heure de la gouvernance mondiale*, Dalloz IP/IT 2020 p.337

[367] NAVARRO P., ZANNOTTI F., précité

[368] https://fr.wikipedia.org/wiki/Internet (consulté le 30/12/2019)

[369] On rappellera qu'une *blockchain* permet la mise en place d'un réseau P2P, pouvant être configurée aussi bien pour être publique (et donc disponible avec une simple connexion internet classique) ou pour être fermé, et donc accessible qu'à un nombre restreint d'acteurs.

[370] NOCETTI J., *La gouvernance mondiale d'Internet à la croisée des chemins*, Enjeux numériques, n° 4, Annales des Mines, déc. 2018, pp. 31-36

simple base de données, néanmoins, son architecture, sa transparence et son caractère distribué se trouvent constituer un mode de fonctionnement aujourd'hui de plus en plus plébiscité, au point que l'on considère aujourd'hui des organisations autonomes décentralisées, à savoir une entité fonctionnement grâce à un programme informatique, fournissant des règles de gouvernance[371], mettant en avant, à travers l'utilisation d'une seule technologie, le choix d'une gouvernance autonome. Sachant que ce choix de gouvernance découlera également de la typologie de la *blockchain* choisie (privée, publique ou encore hybride) et devra porter, de manière parallèle aux actions de gouvernance classique, sur « les conditions d'accès, le fonctionnement, la sécurité[372] ». Cela a été notamment soulevé par l'organisation France Stratégie[373], la *blockchain* relève « bien ici d'un enjeu de gouvernance[374] ». Poussant ainsi la *blockchain* à pouvoir être considéré comme axe fondateur d'une gouvernance particulière.

224. Néanmoins, et pour reprendre une critique souvent formulée à l'encontre de la *blockchain*, critique basée sur le retour d'expérience du *Bitcoin* : *Bitcoin* est une monnaie virtuelle, c'est-à-dire une monnaie créée non par un état ou une union monétaire mais par un groupe de personnes (physiques ou morales) et destinée à comptabiliser, sur un support virtuel, les échanges multilatéraux de biens ou services au sein de ce groupe[375]. *Bitcoin* a souvent été décriée comme favorisant les financements terroristes ou plus largement illégaux, du fait de son fonctionnement anonyme et rapide. La difficulté d'identifier les personnes qui se trouvent derrière les pseudos utilisés pour les transactions fait de la monnaie *Bitcoin* un moyen simple

[371] FAVREAU A., *L'état au défi des blockchains, régulation(s) et usages publics de la technologie blockchain*, RFPI, numéro spécial, fév. 2021

[372] LE TROCQUER A-H., *Blockchain, gouvernance d'entreprise et infrastructures de marché*, Revue Lamy droit des affaires, n°129, 2017

[373] France Stratégie, anciennement le Commissariat à la Stratégie et à la Prospective, est une institution rattachée au Premier ministre et a, notamment, pour objectif concourir à la détermination des grandes orientations pour l'avenir de la nation et des objectifs à moyen et long terme de son développement économique, social, culturel et environnemental.

[374] TOLEDANO J. France Stratégie, *Les enjeux des blockchains*, présidé par, Juin 2018, p. 10, v. la définition du *Protocole de consensus* : « Qui a accès à la *blockchain*, qui définit les modalités d'un ajout sur la chaîne, comment décider d'une évolution du protocole ? Le choix du « protocole de consensus distribué » est une question éminemment stratégique. La *blockchain* peut être publique, avec une architecture ouverte, ou privée, avec un nombre volontairement limité de participants et la réintroduction d'une forme d'autorité centralisée. L'enjeu technique se fait ici enjeu de gouvernance ».

[375] Tracfin, Rapport d'activité, ministère de l'Économie et des finances, 2011. NB : Il s'agit de la cellule française de lutte contre le blanchiment de capitaux et le financement du terrorisme. Il concourt au développement d'une économie saine en luttant contre les circuits financiers clandestins, le blanchiment d'argent et le financement du terrorisme. Le Service est chargé de recueillir, analyser et enrichir les déclarations de soupçons que les professionnels assujettis sont tenus, par la loi, de lui déclarer.

et efficace de blanchir de l'argent ou financer des malversations. C'est pour ces raisons que cette technologie est critiquée pour son anonymat.

À ce titre, « la régulation des monnaies digitales est inévitable »[376], et de nombreux projets de régulation sont en cours. Néanmoins, la création de régimes spécifiques, s'agissant de ces « monnaies digitales » portent essentiellement sur les prestataires en tant que tels, et le système de certification, ou plutôt d'approbation de ces nouveaux acteurs économiques que sont les prestataires de services d'actifs numériques ne font que démontrer qu'il n'est pas question de réguler en tant que telles ces monnaies, mais seulement les acteurs les utilisant. Néanmoins, cette intervention démontre surtout une possible immixtion de l'appareil étatique dans la gouvernance même d'une *blockchain* visée. Dans l'exemple de la *blockchain Bitcoin*, le but n'a donc pas été de réguler la *blockchain* en tant que telle, mais de renforcer les axes de gouvernance portant sur la lutte contre la criminalité, et ce en créant un régime de conformité pour lesquels les prestataires de service sur actif numérique[377].

225. Dans une autre mesure, et afin de démontrer les impacts de la *blockchain* comme outil de gouvernance, pour les *blockchain*s publiques[378] ; ce trait particulier n'est pas non plus s'en affirmer qu'il existe en réalité un caractère janusien (en référence au dieu Janus, à deux visages) à la technologie *blockchain*. Traduisant ainsi une prise en compte, d'une part, des créateurs de *blockchain*s publiques des influences à la fois politiques et législatives, et d'autre part, du législateur, préférant instaurer - à juste titre - des garde-fous juridique ou d'autres encadrements légaux de l'utilisation de *blockchain*[379].

De manière parallèle, l'utilisation de la *blockchain* peut se trouver complémentaire à d'autres axes de gouvernance, comme celui ayant trait à la gestion d'un processus créatif et la

[376] CHARPIAT V., *Le Bitcoin devient monnaie courante : les monnaies digitales entre transparence, régulation et innovation,* Revue des Juristes de Sciences Po, n°9, Juin 2014, 96

[377] Désignés également par l'acronyme « PSAN », ces derniers, depuis l'adoption de la loi PACTE du 23 mai 2019, doivent notamment mettre en place toute une série de règles sur le KYC (*Know Your Customer*), bien connu des acteurs bancaires traditionnels.

[378] LÊMY G., *La gouvernementalité de blockchains publiques,* Dalloz IP/IT, 01/09/2019, 9, pp497-502

[379] À noter que ces encadrements peuvent être positifs (comme l'introduction du statut de PSAN) ou négatifs (par exemple, en refusant la caractérisation d'acte authentique pour les actes passés via une *blockchain*).

gestion d'actifs immatériels[380] ou encore pour aider à la facilitation de l'arbitrage en matière internationale[381].

La *blockchain*, en tant qu'outil incorruptible théoriquement, se mue ainsi comme outil de gouvernance ; et là où il est possible d'y percevoir une re-féodalisation du droit[382], il est possible au contraire d'y voir un asservissement de nos rapports à un registre décentralisé, composé de seules entités numériques, au sens le plus caricatural, une suite logique de 0 et de 1.

[380] BOUNOT V., *La blockchain, outil de gouvernance et de traçabilité du processus créatif (R&D)*, Revue Lamy Droit des affaires, 1er sept. 2019, n°151, pp.41-48

[381] MAKROUM N., FONTAINE C., *La prise en compte de la blockchain par l'arbitrage international en ligne*, 7 oct. 2020, Club de l'arbitrage, disponible à : https://www.clubdelarbitrage.com/post/makroum-fontaine-la-prise-en-compte-de-la-*blockchain*-par-l-arbitrage-international-en-ligne, (consulté le 02/09/2020)

[382] LAURENT-BONNE N., *La re-féodalisation du droit par la blockchain*, Dalloz IP/IT 2019, p.416

Conclusion du Chapitre 1

226. L'essor des nouvelles technologies a su devancer la création d'un appareil législatif dédié à la gouvernance des données. En dépit d'une notion de gouvernance d'ores et déjà connue des organisations sociétales classiques, elle paraît encore ténébreuse pour les systèmes d'information et, par extension, pour les données. Néanmoins, il est possible d'assister à un certain lâcher-prise de la part du législateur, pris comme organe premier de toute régulation, dans cet univers numérique, avec pour conséquence directe une impression générale d'un abandon du législateur pour réguler sans cesse de nouveaux sujets. L'exemple des premières régulations tardives autour du *Bitcoin* peuvent être témoin, de cette faiblesse. Cette inertie législative apparaît comme nécessaire, tant les évolutions technologiques sont rapides, afin de garder une efficacité de la norme sur de tels sujets. Toutefois, le pendant de cette approche, est de laisser la place de la régulation aux acteurs les mettant en œuvre. Il est cocasse de rappeler que YouTube et Facebook ne sont que des adolescents numériques, le premier ayant 15 ans, et le second, 14, alors qu'il paraît aujourd'hui difficilement imaginable d'avoir un téléphone ou un ordinateur sans ces acteurs. Mais il est empirique de reconnaitre l'importance du caractère déterminant de ces acteurs pour les pratiques de l'univers numérique. Avec pour conséquence directe une omniprésence des règles de gouvernance des données de ces grands acteurs, au détriment de la latitude décisionnels d'opérateurs plus réduits.

C'est l'intérêt des protocoles *blockchain* que de pouvoir lutter contre cette omniprésence. En effet, étant donné les caractéristiques de la *blockchain*, la mise en place d'un tel protocole devra suivre ses propres règles, préalablement définies. Ainsi tout système informatisé basé sur une *blockchain* possédera alors, aussi bien administrativement que techniquement, une série de règles que tout utilisateur devra suivre, peu importe son importance, sans mettre à défaut l'ensemble d'un système d'information. Empiriquement, toute entreprise se pilote de plus en plus grâce aux données, qu'elles portent sur les données personnelles (prospect, salarié, etc.) ou les données non personnelles (production, retours sur investissements, capital, etc.). Dès lors toute règle servant ces données sert alors l'entreprise, cette dernière se plaçant dans une logique d'autocontrôle. L'utilisation de la *blockchain* devient alors outil de gouvernance. Toutefois, les seules caractéristiques organisationnelles de la *blockchain* ne permettent pas à elles seules une mise en place complète d'une gouvernance efficace et pérenne. Il en reste que le droit positif, en son état actuel, continue de stimuler cette gouvernance par les données, et la *blockchain* peut devenir un outil à part entière de cette dernière.

Chapitre 2 : Au profit des stimulations de la gouvernance privée des données

227. Si une carence du législateur peut se retrouver à l'égard de la latitude des acteurs de l'univers numérique, alors cela laisse une place à une gouvernance par la *blockchain*, et donc, de manière extensive, à une gouvernance algorithmique[383] plus grande encore. Dès lors, les grands consommateurs ou « organisateurs » de données[384] créent d'eux-mêmes leur propre gouvernance basée sur l'utilisation de ces mêmes données. Outre certains contrôles et affaires actuelles[385] portant sur des pans juridiques d'ores et déjà connus (comme le droit de la concurrence), ces acteurs mettent, sur leur propre initiative, des axes de gouvernances dédiés à la gestion de leurs données. Parmi ceux-ci, il est possible de trouver différentes « simili-institutions », comme le Conseil de surveillance[386] de Facebook, ou encore la mention de portails internes thématiques et dédiés[387]. Au-delà, il est plus commun de trouver des codes de conduite internes.

228. Les codes de conduite interne peuvent trouver une influence anglo-saxonne[388], et peuvent comprendre des règles de fonctionnement de l'entreprise, des axes de gouvernance ou encore des dispositions relatives à la mise en œuvre d'une stratégie d'entreprise. De manière parallèle, notamment pour en assurer son efficacité et son application, de tels codes de conduites sont mis en place avec des instruments de contrôle interne, via de l'audit ou encore avec la création d'un comité *ad hoc* créé pour contrôler son application.

Pour réaliser un parallèle avec cette même notion, cette fois rencontrée en droit du travail, l'élaboration d'un code de conduite est le plus souvent unilatérale, sauf en cas

---

[383] Cf. note n°17

[384] Par exemple, les GAFAMI

[385] Par exemple : Jugement Google/UFC-que-choisir, TGI Paris, 12 fév. 2019, n° 14/07224

[386] Sur le Conseil de Surveillance de Facebook, https://www.facebook.com/help/711867306096893 (consulté le 14/09/2021)

[387] FAURE L., *Google va mettre en place un nouveau portail permettant aux employés de signaler les problèmes sur leur lieu de travail*, ITsocial.fr, 26 avr. 2019, disponible à : https://itsocial.fr/actualites/google-va-mettre-place-nouveau-portail-interne-permettant-aux-employes-de-signaler-problemes-lieu-de-travail/ (consulté le 24/09/2019)

[388] PEREIRA B., *Chartes et codes de conduite : le paradoxe éthique*, *La Revue des Sciences de Gestion*, 2008/2 (n° 230), pp. 25-34. DOI : 10.3917/rsg.230.0025. URL : https://www.cairn.info/revue-des-sciences-de-gestion-2008-2-page-25.htm

d'engagements forts dans le dialogue social où il peut être conçu de manière conjointe avec les Institutions Représentatives du Personnel. La valeur juridique d'un code de conduite interne est d'ores et déjà prise en compte par la pratique et par le juge[389], et d'une manière résumée, en fonction de son contenu, il va pouvoir être assimilé au règlement intérieur d'une entreprise. On pourra retrouver ainsi des dispositions relatives aux relations internes l'entreprise, et plus largement, des composantes sociétales, environnementales ou encore économiques en ce qu'elles touchent les relations externes à l'entreprise.

229. Également, ces codes de conduite se retrouvent dans le cadre de la lutte contre la corruption[390], et doivent d'ailleurs être mis obligatoirement en place[391]. Cette tendance au renforcement d'un certain contrôle interne se trouve de plus en plus fréquemment, comme peut en témoigner la mise en place du RGPD[392] et du règlement les données non-personnelles[393], au point d'ailleurs, que la mise en place de tels codes est fortement encouragée, de manière parallèle avec la mise en place de certification.

230. Du latin médiéval *certificatio*, la notion de certification renvoi à une notion d'assurance, de vérification, et peut être définie comme « l'action de certifier » et comme le « résultat de cette action », comme une « assurance donnée par écrit[394] ». La notion de certification dans l'univers numérique a été fortement dynamisée avec l'entrée en vigueur du RGPD. Cette dernière repose sur plusieurs éléments, mais reste « classiquement définie comme un mécanisme permettant d'attester la conformité à des obligations en se conformant à un référentiel »[395] dont l'initiative appartient aux acteurs la souhaitant, laissant alors la place

[389] CAUSSÉ N., *La valeur juridique des chartes d'entreprises au regard du droit du travail français,* Thèse droit, Université d'Aix-Marseille, 1999

[390] Loi n°2016-1691 du 9 déc. 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique

[391] Loi n°2016-1691 du 9 déc. 2016, précité. art. 17

[392] Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 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), dit RGPD.

[393] Règlement (UE) 2018/1807 du Parlement Européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, dit RGNP.

[394] CORNU G., *Vocabulaire juridique,* PUF, collec. Quadrige, 8e éd., 2007

[395] TAMBOU O. *L'introduction de la certification dans le règlement général de la protection des données personnelles : quelle valeur ajoutée ?,* Revue Lamy Droit de l'Immatériel, Nº 125, 1er avril 2016

aux initiatives privées (Section 1), de telles initiatives démontrant une montée en puissance de la gouvernance par la donnée (Section 2).

Section 1 : Un encouragement des initiatives privées de gouvernance

231. La place de la loi sur la gouvernance, outre un certain nombre de règles sur le volet organisationnel [396], laisse une place importance à un auto-déterminisme des axes de gouvernance, notamment sur la gestion des donnés, actuel actif primordial des entreprises. Toutefois, la puissance des autorités de contrôles indépendantes, soutenues par l'appareil législatif, encourage une détermination interne de mécanismes visant à satisfaire des principes à portées générales. Initiés notamment par la loi Sapin II[397] et la lutte contre la corruption, ou encore la protection des données personnelles, les acteurs visés mettent alors en place, sur leur propre initiative, ces codes de conduites et autres certifications. Pour autant, en tant qu'actes individuels et unilatéraux (car édictés et visant une entreprise ou un groupement d'entreprises seules), leur valeur peut être discutée, même si en définitive la montée en puissance d'un droit de la conformité[398] en reste une expression pragmatique. Cette auto-détermination induit alors la prise d'engagements, unilatéraux et encouragés, dont la forme et la portée ne sauraient être contestés au nom du principe de liberté contractuelle (§1), pouvant être matérialisées en application du concept de conformité (§2).

§1 : La validité logique d'un consensualisme privé

232. Habituellement centré sur une typologie d'homologation de processus industriels, managériaux ou encore informatiques, le Marché a permis l'apparition de différentes certifications et autres codes de conduites, dans le but, une nouvelle fois, de garantir une certaine confiance (aux yeux du consommateur, de l'usager, ou encore du client) à une entreprise. Aujourd'hui, deux typologies d'acteurs sont positionnées sur le marché de la certification : les autorités indépendantes (telles que la CNIL ou l'AMF) et les organismes

[396] On pourra ici citer les dispositions des articles L225-17 et suivants du Code de commerce s'agissant de la société anonyme.

[397] Précité.

[398] FRISON-ROCHE M.-A., *Du Droit de la Régulation au Droit de la Compliance*, Working Paper, http://mafr.fr/fr/article/du-droit-de-la-regulation-au-droit-de-la-complianc/, consulte le 21/05/2021

privés. Qui eux-mêmes vont tenir leur légitimité de certification d'un organisme, le plus souvent international, tel que l'ISO. L'ensemble de la présente section se focalisera sur les certifications possibles dans l'univers numérique, en faisant ainsi fi des certifications de produits ou de services particuliers, comme on peut en retrouver à la lecture du code de la consommation[399].

233. S'agissant des codes de conduite, la question de la valeur légale d'un tel document s'est d'abord trouvée dans les conflits relatifs à l'ordre social et leur valeur est appréhendée[400]. Le juge a pu rappeler plusieurs fois que la violation d'un tel code de conduite pouvant suffire à justifier un licenciement[401]. En l'espèce, le code de conduite étant une prérogative du pouvoir hiérarchique de l'employeur, il est aisé de comprendre que la violation d'un tel code suffise à justifier une sanction. Dès lors, l'incorporation d'un tel code de conduite dans un ordre pseudo légal interne paraît justifiée dans la mesure où il reflète l'expression de ce pouvoir hiérarchique, et doit être alors considéré comme part entière de l'environnement de contrôle d'une entreprise, au même titre qu'un règlement intérieur ou une charte informatique. On rappellera d'ailleurs qu'une telle charte, en cas de conséquences pour les conditions de travail[402], doit être soumise à avis des institutions représentatives du personnel ; c'est notamment cette procédure d'avis qui donne force exécutoire à un tel document.

De manière analogue, le Code de conduite va donc produire ses effets intra-entreprise, et possède alors une valeur légale en tant que tel ; mais l'on pourra rappeler le principe d'effet relatif du contrat[403]. Ce principe n'est pas anodin pour la valeur, cette fois, extra-entreprise. En effet, compte tenu de ce principe simple qu'est l'effet relatif du contrat, on est en droit de

---

[399] Art. L115-27, C. Conso. ; « Constitue une certification de produit ou de service soumise aux dispositions de la présente section l'activité par laquelle un organisme, distinct du fabricant, de l'importateur, du vendeur, du prestataire ou du client, atteste qu'un produit, un service ou une combinaison de produits et de services est conforme à des caractéristiques décrites dans un référentiel de certification. Le référentiel de certification est un document technique définissant les caractéristiques que doit présenter un produit, un service ou une combinaison de produits et de services, et les modalités de contrôle de la conformité à ces caractéristiques. L'élaboration du référentiel de certification incombe à l'organisme certificateur qui recueille le point de vue des parties intéressée ».

[400] DOISY M., DAOUD E., *La violation des règles éthiques internes peut justifier un licenciement pour faute grave*, Editions Législatives, juil. 2020, disponible à https://www.village-justice.com/articles/violation-des-regles-ethiques-internes-peut-justifier-licenciement-pour-faute,35985.html (consulté le 24/09/2020)

[401] CA Versailles, 4 déc. 2019, n° 17/01989, ou encore CA Paris, 21 févr. 2018, n° 15/01893, voir com. DOISY M., DAOUD E., précité

[402] Art. L1321-4 C. du Tr. ; l'assimilation de la charte informatique, en ce qu'elle peut avoir des conséquences sur les sanctions disciplinaires doit suivre les mêmes conditions de validité que le règlement intérieur.

[403] Art. 1199, C. Civ.

se questionner sur la portée d'un tel code de conduite, notamment pour sanctionner des pratiques enfreignant un tel code, en particulier quand la pratique ne subordonne nécessairement pas la conclusion d'une quelconque convention portant sur l'application d'un tel code. Pour apporter des éléments de réponses, il est possible de reprendre les développements tenus lors de l'élaboration de la loi « Sapin II », en ce qu'elle traite des codes de conduite internes[404]. Si l'élaboration de tels codes fait partie intégrante des obligations des entreprises concernées, deux typologies d'effets juridiques peuvent être identifiées : les conséquences dues à son absence et les conséquences dues à leur violation. Si l'absence d'un tel code va pouvoir être sanctionnée directement, la violation d'un tel code ne répond pas nécessairement à la même logique. Il s'agit ici, notamment, des cas des lanceurs d'alerte, ou autres aviseurs fiscaux[405] qui dénoncent des atteintes à des codes de conduite. Ce type de dispositifs entérine la valeur extra-entreprise de tels codes de conduite, permettant aux personnes y ayant intérêt à pouvoir dénoncer tout manquement interne à de tels dispositions inhérentes au pouvoir discrétionnaire de l'employeur. Une logique est rapidement discernable : si un acteur s'engage, aussi bien en interne que sur la place publique, alors il répond de ses engagements, plaçant ainsi un engagement unilatéral à un niveau quasi multilatéral indifférencié.

Au-delà, la jurisprudence semble tendre vers une telle solution ; dans deux arrêts rendus par la Cour d'appel de Paris[406] viennent appuyer la possibilité de justifier la rupture de relations contractuelles au motif de la violation d'un code éthique, quand bien même un tel code n'est pas l'objet principal des relations contractuelles. Outre les engagements pris par un acteur grâce à un tel code, c'est une nouvelle fois la notion de confiance qui trouve une place importante voir fondamentale ; un acteur souhaitant s'engager vers un code de conduite engage alors la confiance que son public place en lui. Toute violation de cette confiance emportant alors sanction (financière, économique ou encore potentiellement juridique). Ces codes de conduite contiennent alors des lignes directrices « qui doivent permettre de tendre vers de

[404] Cf. *Infra*, p.184 et suiv.

[405] Pour plus d'informations : https://www.economie.gouv.fr/cedef/aviseur-fiscal-remuneration (consulté le 15/02/2021)

[406] CA Paris, 24 mars 2021, n°19/15565 et CA Paris, 5 mai 2021, n°19/15680

l'autorégulation[407] », dans un objectif de respect de normes à vocations plus larges, par exemple, la lutte contre la corruption.

234. La portée d'un tel engagement est alors multiple, tout acteur s'engageant avec un engagement de ce type produit ses effets aussi bien envers son organisation interne (que ce soient des entreprises d'un même groupe, ou plus simplement des préposés) qu'envers sa sphère publique (ses clients, ses autorités de contrôles compétentes, etc.).

S'agissant des certifications, d'un point de vue individuel (pour les rapports entre deux personnes physiques pour l'exemple le plus simple), un défaut de certification ou le retrait d'une certification peut entraîner une rupture du contrat, pour défaut d'*intuitu personæ*[408]. D'un point de vue concurrentiel (notamment dans le cadre d'une relation *BtoB*), la présence ou non d'une certification va principalement conférer un avantage concurrentiel ; par exemple, l'obtention d'une certification de type « ISO 27001 » va assurer à un cocontractant la maitrise d'un état de sécurité satisfaisant par rapport aux standards établis. Au-delà, les mêmes réflexions que précédemment peuvent être tenues, et encore une fois, la confiance est le maître mot de la portée de telles certifications ; là où elle va se distinguer, c'est par l'implication d'un organisme tiers certificateur.

L'encouragement, dans l'univers numérique du développement de tels codes (par exemple encouragés à travers les deux règles majeures en termes de protection des données personnelles et non personnelles) pousse les acteurs visés à « s'auto-engager », et dédouane les acteurs étatiques classiques de cette responsabilité. L'État n'a plus à régler les affaires internes d'une entreprise, c'est à cette dernière d'anticiper de prévoir les modalités de règlement de manquement à des principes établis. Au point que les autorités de contrôle, pour prendre exemple de la CNIL, a notamment pour prérogative d'étudier et de rendre un avis sur les codes de conduite que les entreprises peuvent lui soumettre[409].

235. D'un point de vue plus concret, il existe alors une nécessaire étude qui ressemble de près à une pure étude contractuelle ; chaque clause ou engagement d'un tel code de conduite devra être étudiée *in concreto*, ne serait-ce que pour en déterminer sa légalité ; une telle analyse

---

[407] BOUGEARD A., *Les dispositions relatives à l'accès et au portage des données : code de conduite et bonnes pratiques*, Dalloz IP/IT 2020 p.408

[408] Pour un exemple d'i*ntuitu personae* dans le contrat : Cass. Com., 8 nov. 2017, n°16-17.296

[409] Pour plus d'information : https://www.cnil.fr/fr/comment-faire-approuver-un-code-de-conduite

ayant déjà été retenue, en droit social, par la Cour de cassation[410], mais aussi, plus largement en droit des affaires[411]. De manière opposée à la vérification de la portée juridique d'une telle « norme », ces axes de régulations doivent être mis en balance par ce que l'on pourrait nommer une carence - volontaire - du législateur en ces domaines. Par exemple, le domaine de la sécurité informatique faisant appel à de nombreuses compétences souvent qualifiées de niche, et, logiquement, à des compétences peu nombreuses, l'opportunité de créer un dispositif légal précis et centré uniquement sur des facettes technologiques éparses est moindre. Ce faisant, le choix du législateur, comme il l'a été fait, par exemple, avec la mise en œuvre du RGPD, sera portée sur la mise en œuvre de principes directeurs et appelant à la création de certification[412] appelant à une montée en puissance des régimes de conformité, permettant aux entreprises de ne pas se trouver confrontées à l'application de normes juridiques potentiellement diluées, illisibles, ou pis, non efficientes.

236. Ceci n'est sans rappeler les exigences de rédactions de *smart contracts* et l'inscription de règles techniques pour l'application de conditions contractuelles. En effet, la rédaction de tels protocoles informatiques, et plus largement, la conception de *blockchain* va de pair avec la conception et l'application de règles internes. Par exemple, l'utilisation d'une *blockchain* pour la gestion de données personnelles, si elle est possible[413], va s'inscrire dans le respect de règles internes tendant à l'application du RGPD ; or, si la validité de tels codes de conduites est affirmée, leur expression technique à travers un protocole informatique ne semble pas être un obstacle à leur application. Ces initiatives privées de gouvernance pouvant aussi bien s'appliquer aux comportements humains que techniques. Au surplus, il en ressort même un apport du concept de conformité pour les initiatives privées.

§2 : La matérialisation des initiatives induite par le principe de conformité

237. Pris dans une conception propre aux propos de cette étude[414], le concept de conformité doit être entendu comme un principe visant à créer, alimenter et pouvoir produire (en cas de

[410] Cass. Soc., 8 déc. 2009, n°08-17191, Bull. 2009 V n°276

[411] DE QUENAUDON R., *Un « code de conduite des affaires » en quête de statut juridique*, commentaire de l'arrêt rendu par la Cour d'appel de Versailles, 17 avril 2008, RDT 2009, pp.311-315.

[412] TAMBOU O. précité.

[413] Cf. *Infra*, p.142 et suiv.

[414] Excluant ainsi les notions de conformité au sens civil du terme (par exemple, le « défaut de conformité »), la notion de conformité telle qu'elle issue du droit de la consommation, ou encore celle rencontrée en droit de la concurrence.

contrôle), toute une série de documentations visant à prouver la bonne application d'une règlementation en vigueur. Dans un domaine propre aux données, on peut ainsi concevoir la conformité comme un véritable management documentaire[415], et va ainsi soumettre une entreprise à tout un ensemble normatif (ayant valeur légale ou non, notamment dans le cadre d'une appréciation de la *soft law*[416]). Il reste que cette notion est « propre à tout chacun[417] », et peut être potentiellement bornée par le « totalement volontaire et le totalement contraint[418] », ce qui résume l'esprit même du principe de conformité. C'est-à-dire l'engagement, unilatéral mais profondément encouragé par les autorités de contrôle compétentes (CNIL, etc.) ou même par le législateur, d'acteurs économiques pour démontrer d'eux-mêmes la bonne application d'une règlementation particulière.

238. On peut y voir un parallèle, avec la gestion de la déclaration « 2042 » pré-remplie par l'administration fiscale, pour laquelle la charge de la preuve appartient au contribuable. Ce dernier devant alors « fournir tous éléments, comptables ou autres[419] » à l'appui de sa déclaration en cas de contrôle de la part de l'administration. Cette charge de la preuve est, au demeurant, brutale. Il appartient à un non-technicien fiscaliste, la démonstration, à une autorité compétente et formée, d'une situation fiscale particulière, la sanction restant potentiellement élevée[420]. C'est une logique similaire que l'on peut trouver dans la gestion de la conformité, par exemple aux règles de protection des données personnelles, provoquant un « changement de paradigme[421] ». Un opérateur ne pouvant démontrer sa conformité pourra être affublé de sanctions tout aussi dissuasives[422].

239. Pour autant, le principe de conformité ne doit pas être vue comme un piège pour les acteurs concernés, au contraire, la latitude laissée peut-être un véritable atout pour les entreprises amorçant des initiatives particulières en ce sens. Pour rappel, la démonstration du respect du principe de conformité doit notamment se faire au regard des mesures mises en œuvre par un acteur concerné, ces mesures devant « tenir compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que du risque que celui-ci présente pour les droits

---

[415] https://www.cnil.fr/fr/les-outils-de-la-conformite (consulté le 03/03/2019)
[416] Cf. *Infra*, p.114
[417] FRISON-ROCHE M.-A, *Le Droit de la compliance*, *D.*2016, Chron., 29 sept. 2016, n°32
[418] *Ibid*.
[419] Art. R191-1, LPF
[420] Art. 1727, CGI
[421] FAVRO K., *La démarche de compliance ou la mise en œuvre d'une approche inversée*, Legicom 2017, p.21
[422] Art. 83, RGPD, précité

et libertés des personnes physiques[423] ». En pratique, il existe une multitude de moyens de démontrer une « bonne conformité » autant qu'il existe de situations. En conséquence, parler d'une démonstration unique de conformité n'a autant de sens que de parler d'usage unique de données. La conformité d'une entreprise, prise dans sa dimension de gouvernance, c'est-à-dire dans sa dimension organisationnelle, doit alors se mettre en parallèle de ses activités, et devient alors un moyen de légitimer ses initiatives autant qu'un moyen de les contrôler en interne ; notion écrite au singulier, elle doit s'entendre dans un sens parfaitement pluriel.

240. Il en reste que le concept de conformité appelle la rédaction de nombreuses documentations, preuves de ces engagements volontaires. Il est possible d'y concevoir une application fondamentalement sociale, dans le sens où le concept de conformité va en premier lieu s'appliquer à des personnes physiques et morales. Or, et la protection des données tend vers cette solution, le concept de conformité peut inviter également à une soumission des techniques. La *blockchain* n'a pas de raison d'échapper à cette soumission. Compte tenu de l'importance grandissante des technologies pour la gestion des données, prise comme actif fondamental de toute activité économique, le concept de conformité trouve d'ailleurs de premiers échos avec la sécurité des systèmes d'information[424]. L'encouragement des initiatives privées de gouvernance s'élargit, partant de la gouvernance d'entreprise vers la gouvernance des données. La conception d'une architecture *blockchain* doit ainsi répondre à ce concept, dans le sens où la seule implantation d'une *blockchain* ne se suffit pas à elle-même pour démontrer un bon état de conformité.

Section 2 : Le soutien des régimes de conformité des données

241. Les régimes de *data compliance*[425] doivent donc être entendus comme multiples, et « face au dépérissement de l'État et aux formes nouvelles d'aliénation qu'il engendre, une structure juridique réapparaît, de facture typiquement féodale : celle des réseaux d'allégeances,

[423] Considérant 74, RGPD, précité

[424] ANSSI, *Guide agilité & sécurité numériques – méthode et outils à l'usage des équipes projets*, Oct. 2018, disponible à https://www.ssi.gouv.fr/uploads/2018/11/guide-securite-numerique-agile-anssi-pa-v1.pdf

[425] La notion de *data compliance* littéralement « conformité des données » est difficilement traduisible, en raison, d'une part de la notion ambivalente de la conformité et d'autre part de les considérations actuelle autour des données, prises aussi bien pour leur essence purement informatique que pour leur valeur intrinsèque et valorisée en entreprise.

au sein desquels chacun cherche la protection de plus fort que soi ou le soutien de moins fort que soi[426] ». En effet, s'il est entendu une multiplicité de régimes de *data compliance*, propres à chaque entreprise, alors ces régimes vont pouvoir, du moins intellectuellement, être hiérarchisés. L'importance et l'avènement des GAFAMI démontrent que la gestion de leurs données a des répercussions sur des entreprises plus faibles économiquement. De manière caricaturale, il est difficilement imaginable qu'une entreprise moyenne puisse lutter contre les politiques de gestion des données d'un Google ou d'un Microsoft[427]. Une structure féodale, telle qu'entendue par le Professeur Supiot[428] peut décrire alors une soumission du « plus petit que soi », mais sans forcément la protection du seigneur, telle qu'entendue traditionnellement[429]. Au point que le seul garant d'une éventuelle protection ne peut que se trouver dans un acteur tiers, ou un autre seigneur. Ainsi, les régimes de conformité des données vont découler de deux aspects : le premier en tant qu'expression d'un acteur économique, et le second, en tant qu'expression des moyens technologiques mis en place. Ce second aspect reste important dans une économie de la donnée. En effet, si un nouveau seigneur est apparaît, il voudra faire appliquer, d'une part ses règles, et d'autre part, ces outils ou ses techniques. La *blockchain* se démocratisant de plus en plus, les acteurs puissants l'ayant choisie, capables d'imposer leur vision, pourront dès lors assujettir son usage, et ce même dans des activités publiques. Dès lors, une immersion critiquable du pouvoir privé dans la sphère publique (§1) est constatable, immersion pouvant, en partie, être contrebalancée par le droit souple. (§2).

§1 : L'immersion critiquable du pouvoir privé dans la sphère publique

242. Le développement d'initiatives privées autour de la gouvernance des données, comme peuvent en témoigner les pratiques des « géants du web », si elles possèdent un impact déjà fort pour les acteurs privés, ne sont pas sans conséquences pour au regard de la sphère publique, à savoir notamment pour les autorités régulatrices (CNIL, Autorité de la concurrence, AMF, etc.) mais également pour les intérêts étatiques.

[426] SUPIOT A, précité

[427] Ceci n'étant pas sans conséquence, par exemple dans le cadre d'une maitrise des données d'une entreprise, soumise nécessairement au bon vouloir de ses hébergeurs.

[428] Précité.

[429] Dans le système féodal traditionnel, si les vassaux étaient soumis à l'autorité de leur seigneur, ce dernier n'avait pas pour autant de responsabilité envers eux, notamment une obligation de sécurité et de protection.

Dans un premier temps, les intérêts étatiques deviennent de plus en plus sujets de cette féodalisation du monde numérique. L'ensemble des tenants et aboutissants autour, par exemple, du Health Data Hub[430] (HDH), est un excellent exemple[431]. La création du HDH est une plate-forme destinée à faciliter le transfert et le partage d'informations de santé, dans le but, notamment, de renforcement et de facilitation de la recherche. Les développements d'une telle plateforme possèdent des enjeux cruciaux pour le développement de la recherche dans le domaine de la santé (favorisant le croisement d'information, le développement de données massives ou encore l'utilisation de l'intelligence artificielle pour l'exploitation des données). Néanmoins, pouvoir supporter de tels enjeux possèdent des répercussions fortes d'un point de vue technique ; quel hébergeur de données est capable de supporter un tel afflux de données. Après la constitution d'un appel d'offre, la solution d'hébergement Microsoft Azure a été retenue. Or, outre les qualités techniques de la solution retenu, un problème majeur fut simplement identifié par la CNIL[432] : la localisation potentielle des données issues de la recherche française sur des serveurs soumis à la souveraineté américaine. En réalité, il faut également comprendre que ce sont les caractéristiques de cet hébergement, expression de capacités techniques et politiques d'un opérateur privé étranger qui ont pu faire chanceler la sphère publique, au point que de cette espèce a permis de mettre en lumière les enjeux d'une souveraineté numérique[433].

243. L'univers numérique, et l'omnipuissance des acteurs privés grâce au pouvoir de la donnée dépasse les seuls enjeux de conformité, au point que des régimes de *data compliance* deviennent des attributs pouvant alimenter des débats sur la notion même de souveraineté numérique[434]. Face à cette puissance, presque irrésistible compte tenu de la puissance économique des acteurs concernés, peu de contre-pouvoirs sont aujourd'hui présents. Et le droit positif permet d'ailleurs à ces acteurs d'être « plus à même d'élaborer un cadre juridique propre et répondant précisément aux pratiques à avoir sur un marché et une concurrence

[430] https://www.health-data-hub.fr/page/mentions-legales et https://www.cnil.fr/fr/la-plateforme-des-donnees-de-sante-health-data-hub (consultés le 20/03/2021)

[431] D'autres exemples démontrant l'importance des initiatives d'opérateurs privés ayant des répercussions politiques auraient pu être cités : par exemple l'importance du développement de l'ordinateur quantique de Google.

[432] NAVARRO P., ZANNOTTI F., *Souveraineté et surveillance, les enseignements tirés de l'affaire du Health Data Hub*, Revue Lamy Droit de l'immatériel, 176, 01/12/2020

[433] On rappellera que le concept de souveraineté peut se définir comme « capacité, pour une entité, de se donner ses propres règles », et pour un état, le fait de « définir par elle-même les normes auxquelles elle se soumet, et non de se voir imposer ces règles de l'extérieur ».

[434] DERIEUX E., *Souveraineté à l'ère du numérique*, Revue Lamy Droit de l'immatériel, 156, 01/02/2019

donnée, plutôt que de subir une norme juridique qui viendrait les contraindre[435]». Si certaines autorités de contrôle tentent de prendre le pas contre ces acteurs, en droit de la concurrence[436] ou encore la CNIL[437], la présence quasi systématique des outils issus de ces derniers reste un témoignage de la difficulté pour la sphère publique de s'en passer, même si des initiatives en ce sens existent[438].

244. Dans une logique propre à la *blockchain,* cette immersion du pouvoir privé peut dans la sphère publique peut être d'autant plus marquée. En effet, la force d'une *blockchain* réside dans son partage, et dans son utilisation partagée par les participants au réseau. L'affaire du HDH, si une solution *blockchain* avait été retenue, aurait eu pour conséquence de forcer l'adoption d'une telle technologie par l'ensemble des acteurs souhaitant utiliser l'HDH. Cette adhésion forcée, si elle n'a pas lieu dans le cadre de la gestion des données de santé, emporte pourtant réalité dans le secteur financier. En effet, l'adoption du *Bitcoin* par le Salvador en 2021 comme monnaie ayant cours légal[439] témoigne du pouvoir privé s'immisçant dans la sphère publique. Toutefois, cette immixtion dans la sphère publique ne peut se faire en dehors de toute régulation. Et à défaut de solution claire et univoque, qu'elle soit issue de régulations nationales ou européennes, l'encadrement de la conformité de ce pouvoir peut passer par des produits dérivés législatifs.

§2 : Le contrepoids insuffisant par le droit souple

245. Le droit souple, ou *soft law*, a pu faire l'objet de différentes études, et reste issu du droit international et d'un besoin de régulation alternatif à un droit dit « dur ». Le Conseil d'état

[435] BOUGEARD A., *Les dispositions relatives à l'accès et au portage des données : code de conduite et bonnes pratiques*, précité.

[436] SCHREPEL T. *Ententes algorithmiques et ententes par blockchain*, Recueil Dalloz, D. 2020, 1244

[437] Délibération SAN-2020-012 du 7 déc. 2020, CNIL/GOOGLE IRELAND LIMITED

[438] Par exemple : https://solutions-opensource-pour-collectivites.fr/solution/visioconference, (consulté le 21/02/2021)

[439] RANDALL P. *Le Salvador devient le premier pays à adopter le bitcoin comme monnaie légale*, Les Numériques, 07/06/2021, disponible à https://www.lesnumeriques.com/pro/le-salvador-veut-etre-le-premier-pays-a-adopter-le-bitcoin-comme-monnaie-legale-n164665.html

a pu, dans un rapport en date de 2013, dégager trois critères[440] pouvant conférer une qualité de droit souple à une norme. Si l'enjeu de la conformité est notamment la confiance, alors il convenait de trouver une typologie normative capable d'appréhender une notion aussi abstraite. La réponse potentielle apportée par le droit « dur » peut être jugée comme insuffisante[441], et l'absence de régulation n'est pas non plus une solution efficace. La place laissée à la *soft law* est alors d'autant plus facilitée, en particulier dans l'univers numérique, et notamment dans un univers propre à la *blockchain*[442].

246. Néanmoins, le rappel des critères avancés par le Conseil d'État en 2013 fut lapidaire, pour la CNIL, à l'occasion de l'étude des « murs de cookies[443] » *ou cookies wall*[444]. En l'espèce, les directives de la CNIL, notamment depuis un premier arrêt du Conseil d'état en 2016[445]. Depuis, la CNIL a pu édicter un certain nombre de règles et autres lignes directrices sur les cookies[446], notamment en prévision et en réaction à l'adoption du RGPD. Or, un arrêt de 2020[447] vient encadrer les pratiques de la CNIL, rappelant qu'un acte de droit souple n'emporte pas de « droit ou d'obligations pour leurs destinataires[448] », et qu'en conséquence, les directives de la CNIL, en tant que droit souple, ne peuvent, à elles-seules imposer un comportement particulier à un responsable de traitement de données à caractère personnel.

---

[440] CE, *Le droit souple*, Étude annuelle 2013 ; dans cette étude, le Conseil d'état détermine trois critères cumulatifs : « – ils ont pour objet de modifier ou d'orienter les comportements de leurs destinataires en suscitant, dans la mesure du possible, leur adhésion ;
– ils ont pour objet de modifier ou d'orienter les comportements de leurs destinataires en suscitant, dans la mesure du possible, leur adhésion ;
– ils ne créent pas par eux-mêmes de droit ou d'obligations pour leurs destinataires ;
– ils présentent, par leur contenu et leur mode d'élaboration, un degré de formalisation et de structuration qui les apparente aux règles de droit dur ».

[441] On pourra renvoyer notamment aux développements et études sur l'opportunité et les résultats de la Hadopi, précités.

[442] MARRAUD DES GROTTES G., Preuve blockchain : et si la soft law était une première étape ?, Wolters Kluwer, 9 déc. 2019, disponible à : https://www.actualitesdudroit.fr/browse/tech-droit/*blockchain*/24918/preuve-*blockchain*-et-si-la-soft-law-etait-une-premiere-etape, (consulté le 15/11/2020)

[443] On rappellera qu'un cookie est un fichier informatique déposé, lors d'une navigation sur internet, permettant, potentiellement, de se souvenir des choix de l'utilisateur, le suivi de son activité sur un site internet, ou encore la sauvegarde d'un panier pour un site de e-commerce.

[444] La pratique du *Cookies Wall* est une pratique consistant à bloquer l'accès à un site internet à un utilisateur tant qu'il n'a pas donné son consentement au dépôt de cookies sur son terminal.

[445] CE, 10ème - 9ème ch. réunies, n°412589, 6 juin 2016, Publié au recueil Lebon

[446] Voir notamment https://www.cnil.fr/fr/cookies-et-autres-traceurs, consulté le 19/05/2021

[447] CE, 19 juin 2020, n°434684, voir com. HAAS G., TORELLI M., *Annonceurs et RGPD : faux amis, frères ennemis, l'exemple des cookies publicitaires*, Revue Lamy Droit des affaires, n°168, 1er mars 2021

[448] CE, étude annuelle, 2013, précitée

247. Appliqué à la *blockchain*, l'encadrement par le droit souple est une demi-vérité. Comme a pu le noter le LINC[449], plusieurs points d'attentions doivent être pris en compte dans le développement de projets *blockchain*. Or, en conséquence des critères du Conseil d'état rappelés précédemment, si de tels propos ne peuvent s'appliquer *de facto* à des projets de ce type, ils doivent néanmoins être utilisés à des fins de conformité et vecteurs de confiance. La professeure Frison-Roche décrit notamment l'impact du droit souple comme ne devant pas omettre le droit « dur », conduisant à un droit de la conformité qui doit induire une acculturation de la conformité[450]. Pointant ainsi les lacunes potentielles du droit souple, et démontrant ainsi l'importance de la culture, aussi bien juridique que technique que devrait posséder tout acteur de la conformité, applicable logiquement à la *blockchain*.

Conclusion du Chapitre 2

248. L'émergence de la *blockchain* participe de l'importance actuelle de la montée d'une gouvernance de la donnée. Là où la *blockchain* se distingue c'est par ses caractéristiques techniques particulières, notamment ses possibilités de traçabilité et d'intégrité des données ; les impacts qu'une telle technologie sur la gouvernance d'une entreprise (via, par exemple, l'utilisation d'une *blockchain* sur la traçabilité d'actes) peuvent être importants. Néanmoins, la seule utilisation d'une technologie ne peut, en soi, avoir de répercussion profonde sur l'organisation et le fonctionnement d'une entreprise. C'est là tout l'attrait de ces documentations internes, à vocation « quasi supra » réglementaire, que sont les Codes de conduite et autres règles internes. Ces dernières sont de toutes façons encouragées, voir rendues obligatoires par la loi, et leur valeur devant le juge sont affirmées et deviennent ainsi source de droits et d'obligations Il peut ainsi ressortir, par la stimulation des axes de gouvernance par la donnée, des nouveaux rapports de force, entre les entreprises et des autorités administratives indépendantes. Même si le contrôle du juge reste présent, il se borne de plus en plus à vérifier l'application de principes généraux, à atténuer les ambitions de ces autorités en évitant qu'elles ne s'arrogent un pouvoir normatif. Néanmoins, l'absence de pouvoir normatif des autorités de contrôle[451] n'empêche pas la montée en puissance de régimes de conformité, et ce qui peut être présenté comme une lacune est en réalité une

[449] LINC (Laboratoire d'Innovation Numérique de la CNIL), 02 août 2016, précité

[450] FRISON-ROCHE M-.A., *Compliance : Avant, maintenant, après ?*, MAFR, 12 déc. 2017, disponible à : https://mafr.fr/fr/article/compliance-avant-maintenant-apress/, (consulté le 12/12/2018)

[451] CE, 19 juin 2020, n°434684, précité

invitation à œuvrer à des démarches d'autocontrôle et de conformité. Si le droit souple n'a pas vocation à remplacer le droit « dur », il a cependant vocation à entraîner les acteurs économiques concernés vers des démarches d'autorégulation.

Conclusion du Titre 2

249. L'appareil législatif actuel, pouvant être considéré comme construit au service de l'émergence de nouvelles technologies (sans pour autant favoriser ensuite leur essor[452]), favorise alors l'apparition d'un nouveau modèle de gouvernance par la donnée. Au contraire il nous semble qu'est prônée une régulation minimale, afin de ne pas légiférer de manière précipitée, et ainsi garder une position à tendance libérale, et donc favoriser l'innovation et le progrès économique[453]. La *blockchain* bénéficie aujourd'hui de ce contexte.

Mettant cette dernière au centre des organisation sociétales et autres enjeux économiques, et profitant *de facto* largement à la *blockchain*, en tant qu'outil d'expression de cette gouvernance. Mais l'émergence d'une gouvernance par la donnée ne doit pas se faire en dépit de toute possibilité de contrôle ou d'accompagnement des acteurs économiques. Poussés dans une démarche de conformité, les acteurs concernés se voient dans une nécessaire autorégulation. À la fois encouragée par la pratique d'acteurs puissants du numérique et le droit souple émanent des autorités administratives de contrôle, un nouveau modèle de gouvernance se dessine. Là où le contrat seul pouvait servir de pallier de gouvernance (à travers un contrat de société, des statuts ou encore un contrat d'établissement), la technique devient moteur de la gouvernance des entreprises. La *blockchain* permet le lien entre la technique et le normatif.

250. Cela étant, la *blockchain*, ne demeure une fois de plus qu'un outil au service de cette gouvernance autour de la donnée, et face à un outil, le droit positif doit se trouver appliquer de manière ordonnée, notamment pour éviter toute lacune dans la protection d'une *blockchain*, invitant, dans le cadre de cette étude, à analyser l'applicabilité de différents régimes de propriété intellectuelle à elle. En effet, si l'outil est au service de la gouvernance et, par voie

[452] Par exemple, la France, bien que considéré comme l'un des premiers états à avoir légiférer sur la *blockchain* n'en reste pas moins un état avec l'une des fiscalités les plus dures s'agissant des actifs numériques.

[453] À ce titre, nous pouvons citer une résolution sur les monnaies virtuelles, basées sur des technologies d'organisation décentralisée de type *blockchain* adoptée par le Parlement européen, conscient du potentiel d'une telle technologie et de la nécessité de la laisser arriver à maturation. Proposition de résolution du Parlement Européen sur les monnaies virtuelles, 2016/2007(INI) - 26/05/2016 Texte adopté du Parlement, lecture unique //disponible à : http://www.europarl.europa.eu/oeil/popups/summary.do?id=1438763&t=e&l=fr

de conséquence, au service de l'entreprise, alors protéger l'outil en tant que tel protège l'entreprise.

Conclusion de la Partie 1

251. L'avènement de nouvelles technologies, de manière toujours plus rapide, avec des bénéfices toujours annoncés comme « disruptifs », conduit à une appréciation pouvant être profondément désorganisée. Pouvant accuser une conséquence du « buzz[454] », les nouvelles technologies émerveillèrent autant qu'elles inquiètent. La *blockchain* en devient un parfait exemple ; la *blockchain Bitcoin*, née d'une réaction épidermique aux dérives d'un système bancaire, est aujourd'hui autant une source d'influences que de peurs. La baisse des cours du *Bitcoin*[455], corrélée (de manière réelle ou non, là n'est pas la question) aux déclarations d'Elon Musk[456] ou encore celles de la Chine[457] a créé un certain vent de panique, là où les investisseurs institutionnels[458] ou autres GAFAMI[459] tendent vers une acceptation de plus en plus franche des possibilités de la *blockchain*. Toutefois, ce cadre est bien éclaté en n'étant pas uniquement centré sur la finance. Les réflexions, juridiques, sur l'impact de la *blockchain* dans le droit de la preuve, du brevet ou encore au sein des offices notariaux, son utilisation à titre de gestion énergétique, ou encore pour les contrats d'assurances démontrent à elles seules

[454] LAUF A., *Propagation du buzz sur Internet - Identification, analyse, modélisation et représentation dans un contexte de veille*. Institut National des Langues et Civilisations Orientales - INALCO PARIS - LANGUES O', 2014, disponible à https://hal.archives-ouvertes.fr/tel-01126913/

[455] NDA : le 19 mai 2021, le Bitcoin (BTC) sur les marchés de cryptoactifs a subi une baisse majeure ; pour rester dans une croissance largement positive depuis sa première cotation.

[456] ROCHE L. Elon Musk dans le viseur des autorités US, Journal du Coin, 26 fév. 2021, disponible à : https://journalducoin.com/actualites/elon-musk-dans-le-viseur-des-autorites-us-pour-manipulation-du-marche-crypto/ ou encore DAVID F., *Un économiste accuse Elon Musk d'avoir manipulé le prix du bitcoin*, Clubic, 16 fév. 2021, disponible à : https://www.clubic.com/antivirus-securite-informatique/cryptage-cryptographie/crypto-monnaie/actualite-361924-un-economiste-accuse-elon-musk-d-avoir-manipule-le-prix-du-bitcoin-btc-.html, (consultés le 27/05/2021)

[457] CHICHEPORTICHE O., *La Chine provoque une nouvelle chute du bitcoin*, BFM Business, 24/05/2021, disponible à : https://www.bfmtv.com/economie/economie-social/monde/la-chine-provoque-une-nouvelle-chute-du-bitcoin_AV-202105240013.html (consulté le 27/05/2021)

[458] RENAUDIN H., Des investisseurs institutionnels dans le bitcoin, Finance Mag, 21 oct. 2019, disponible à : https://finance-mag.com/des-investisseurs-institutionnels-dans-le-bitcoin/, consulté le 27/05/2021

[459] À titre d'exemple : https://fr.cryptonews.com/news/l-arrivee-d-apple-dans-les-cryptomonnaies-se-confirme-10740.htm, (consulté le 21/07/2021)

que l'outil en tant que tel doit être déconnecté de son application pour être compris efficacement, appuyant notamment la récente prise de position de l'ADAN sur ce sujet[460].

252. Au-delà, la démocratisation actuelle des usages de la *blockchain* démontre au contraire une volonté de rationaliser, simplifier et améliorer nos rapports à la Donnée. Si le législateur, d'une part pour ne pas freiner l'innovation, et d'autre part, faciliter la démocratisation de l'utilisation de la *Data*, fait un choix de laisser une attitude aux acteurs du numériques, c'est, à notre sens, pour deux raisons. La première pourrait être dans l'impossibilité (matérielle ou encore financière) de générer de nouveaux usages de la donnée, la seconde serait dans l'opportunité de conférer une place plus grande encore à la conformité. Il est aisé de comprendre qu'il plus facile de contrôler des situations novatrices *a posteriori* que d'anticiper toutes ces évolutions possibles.

253. La mise en place de règles et mécanismes d'autocontrôle, dans cette optique de « libéralisme numérique[461] » facilitent la tâche au législateur, qui peut se restreindre à l'édition de principes fondateurs/fondamentaux (lutte contre la corruption, protection de la vie privée par exemple) et à déléguer à des autorités compétente le soin de décortiquer et d'analyser la conformité d'une situation apparaissant comme contraire à ces principes. Donnant ainsi une place malléable, mais restant soumise au potentiel contrôle du juge, au droit « mou » et autres actes de conformité internes. Toutefois, cette libéralisation et cette absence de contrôle *stricto sensu* de ces nouvelles technologies disruptives reste sujet à débat, comme peuvent magnifiquement le démontrer notamment le professeur Supiot[462] ou Madame Antoinette Rouvroy[463] vis-à-vis de leur impact sur les structures sociétales actuelles.

254. Il reste que la *blockchain*, sujet à de multiples fantasmes, sorte de panacée numérique, n'en reste qu'un outil, une magnifique expression d'un art mathématique et informatique. En ce sens, la possible dualité d'approche de cette technologie réside ici : la déconnexion de ses

---

[460] L'ADAN est l'association pour le développement des actifs numériques, et dans une contribution aux travaux de révision de la Directive européenne « Finalité » (https://ec.europa.eu/info/consultations/finance-2021-settlement-finality-review_en), elle appelle à la réalisation du distinguo entre outil et finalité juridique ; pour plus d'informatiohttps://adan.eu/consultation/reglementation-finalite-technologique-juridique, (consulté le 13/05/2021).

[461] SADIN E., *La silicolonisation du monde : l'irrésistible expansion du libéralisme numérique*, L'échappée, 2016

[462] SUPIOT A., précité.

[463] ROUVROY A., BERNS T., *Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ?, Réseaux*, 2013/1 (n° 177), p. 163-196. DOI : 10.3917/res.177.0163. URL : https://www.cairn.info/revue-reseaux-2013-1-page-163.htm

intérêts organisationnels de ses enjeux juridiques. De manière complémentaire à l'approche désorganisée qu'elle provoque, une application ordonnée du droit positif doit trouver expression.

Seconde partie : Pour une application ordonnée

255. Si la réflexion de l'arrêt *Cryo*[464] doit être, dans le cadre de cette étude, entérinée, elle rejoint les développements précédents relatifs à la considération de la *blockchain* comme outil, comme simple objet de droit. Les développements précédents démontrent ainsi que l'appréciation d'une nouvelle technologie, aussi disruptive qu'elle soit, ne peut être exclusive d'une double réflexion : l'appréhension de son contexte, la recherche et l'application ordonnée du droit applicable.

Pris dans sa conception la plus stricte, à savoir l'utilisation d'un logiciel donné couplée à la gestion d'une base de données (même distribuée), l'application des différents régimes applicables fera l'objet, logiquement, d'un pan de la présente étude (Titre 1). Toutefois, cette logique étude sémantique de la *blockchain* ne peut s'opérer sans étudier, dans une logique voisine à celle retenue dans l'arrêt *Cryo*[465] à une étude fonctionnelle du régime applicable aux éléments visés par l'utilisation d'une *blockchain*, les données (Titre 2).

[464] Cass, 1ère Civ., 25/06/2009, n°07-20.387, arrêt dit *Cryo*, précité.
[465] *Ibid.*

Titre 1 : D'une application sémantique des régimes de propriété littéraire et artistiques

« De même qu'il faut d'abord apprendre sa langue pour connaître un peuple étranger, pour comprendre ses mœurs et pénétrer son génie, de même la langue juridique est la première enveloppe du droit, qu'il faut nécessairement traverser pour aborder l'étude de son contenu. »

Vocabulaire juridique, préface, 1836, Henri Capitant (1865-1937)

256. Les termes de l'articles L112-2[466] du Code de la propriété intellectuelle ne tendent pas vers une exhaustivité, « la catégorie des œuvres de l'esprit reste assez ouverte »[467]. On rappellera également les caractéristiques intrinsèques d'une *blockchain*, en ce sens qu'un tel protocole informatique vise à utiliser les caractéristiques d'un logiciel pour la gestion d'une base de données, même distribuée. Dès lors, comme le développait le professeur Capitant[468], la sémantique est une part essentielle de l'étude juridique. La compréhension des spécificités d'une nouvelle technologie doit donc passer logiquement par l'étude de ce qu'elle représente, de façon pragmatique. Si le premier temps de la présente étude vise à comprendre et concevoir la *blockchain* dans notre environnement actuel, son analyse ne peut se passer d'une application littérale, quasi cartésienne, du droit applicable. L'apport de la réflexion sur la qualification distributive est de pouvoir étudier, individuellement, tout élément d'une œuvre complexe. Appliqué à une *blockchain*, l'étude sémantique conduit alors à étudier dans un premier temps le régime de la *blockchain* face à la protection du logiciel (Chapitre 1), puis, dans un second temps, à l'étude de la protection de la *blockchain* grâce à une concordance naturelle du droit des bases de données (Chapitre 2).

[466] Art. L112-2, CPI : « Sont considérés notamment comme œuvres de l'esprit au sens du présent code : 1° Les livres, brochures et autres écrits littéraires, artistiques et scientifiques (…) »

[467] GAUTIER P.-Y., *Propriété littéraire et artistique*, 11ème édition, 2019, éditions PUF

[468] CAPITANT H., *Préface, in.* CORNU G., Vocabulaire juridique, PUF, collec. Quadrige, 8e éd., 2007

Chapitre 1 : L'adéquation de la protection du logiciel à la *blockchain*

257. Si l'application distributive des régimes de propriété intellectuelle tend, pour la *blockchain*, à une application des régimes de protection du logiciel et des bases de données, et dans une vision excluant volontairement les réflexions sur la brevetabilité du logiciel[469], la *blockchain* soulève deux axes particuliers. En effet, le développement d'une *blockchain* repose souvent sur du logiciel libre, et si ce dernier n'est pas exclusif de propriété intellectuelle[470]. Licence libre ne signifie pas absence de droit de propriété intellectuelle, et le logiciel est dit libre lorsque son auteur accorde « aux tiers le droit d'accéder au code source du programme, mais surtout de copier, de modifier et de diffuser librement le logiciel, modifié ou non »[471]. Dès lors, la définition de la titularité des logiciels dits « *blockchain* » peut soulever quelques difficultés (Section 1), mais au-delà de la première détermination de cette titularité, c'est l'exploitation, dans un modèle distribué, de ces logiciels qui peut provoquer des difficultés (Section 2).

Section 1 : La banale titularité des *blockchain*s

258. De manière liminaire, les caractéristiques d'une architecture de type *blockchain* vont avoir une répercussion directe sur la titularité des logiciels *blockchain*, dont certaines sont à exclure des présents développements. En effet, on rappellera qu'une telle architecture peut être à vocation publique, privée ou encore hybride. Ce choix d'architecture dépendant du choix du porteur du projet *blockchain* ; ainsi, une *blockchain* purement privée, et n'ayant donc pas vocation à être utilisé par tout public, doit ici être exclue. En tant que simple projet interne, toute *blockchain* privée répondra aux problèmes classiques de détermination de titularité de la

[469] Cf. *Supra*, p.40 et suiv.

[470] JULLIEN N., ZIMMERMANN J.-B. *Le logiciel libre : une nouvelle approche de la propriété intellectuelle*. In : *Revue d'économie industrielle*, vol. 99, 2e trimestre 2002. Les droits de propriété intellectuelle : nouveaux domaines, nouveaux enjeux, sous la direction de Benjamin Coriat. pp. 159-178, disponible à https://www.persee.fr/doc/rei_0154-3229_2002_num_99_1_3021

[471] GRYNBAUM L., LE GOFFIC C., MORLET-HAÏDARA L., *Droit des activités numériques*, 1ère édition, 2014, Dalloz §631

même manière qu'un logiciel *lambda*[472], et de manière analogue pour les *blockchain* hybrides[473]. En conséquence, la présente étude sera centrée sur les problématiques de *blockchain* dites publiques. Enfin, de manière liminaire, on rappellera également le caractère aménagé du droit d'auteur en ce qu'il concerne les logiciels. Il reste que pour sa facette logicielle, la *blockchain* ne comporte que peu de spécificités pour l'appréciation de son originalité (§1), néanmoins des difficultés, compte tenu que la *blockchain* soit empreinte de l'idéologie du logiciel libre, peuvent être appréhendées (§2).

§1 : L'originalité ordinaire d'une *blockchain*

259. Il convient de rappeler que la valeur inventive, ou informative du logiciel ne sera pas constitutive d'un attribut d'originalité. Pouvant mettre à mal les qualités intrinsèques d'une *blockchain*, notamment mises en avant pour leur caractère disruptif ou novateur[474]. Il reste que la notion d'originalité repose davantage sur la conception et l'architecture conceptuelle que sur l'expression littéralement codée[475]. Sur les éléments protégeables d'un logiciel *blockchain*, et pour reprendre un droit positif établi en la matière, le programme[476], le matériel de conception préparatoire[477] ou encore la documentation[478], et en excluant ainsi les données, ou encore les algorithmes s'y rattachant[479].

260. Sur le point de l'originalité en tant que telle, appréciée à la lumière du logiciel, la directive n°2009/24 limitait la protection d'un programme d'ordinateur lors qu'il est "la création intellectuelle propre à son auteur ». Quant à elle, la jurisprudence, dans un premier

---

[472] On retrouvera alors les problématiques, raisonnements et réponses classiques, aussi bien sur la pluralité d'auteurs que sur les aspects relatifs à la création salariée ; de tels développements sont à exclure dans le cadre de la présente étude.

[473] Ainsi, une *blockchain* hybride, donc développée par un unique opérateur ou nombre réduit de contributeurs, reprendra des solutions parallèles à celles que l'on peut trouver pour les *blockchain*s privées. En effet, la seule différence est que les utilisateurs d'une telle *blockchain* devront bénéficier d'autorisation de la part de leurs producteurs ; toute problématique juridique liée à l'exploitation d'une telle *blockchain* se retrouvant de manière classique dans la gestion de licences.

[474] On pourra penser ici, par exemple, à l'activité inventive résidant dans la création du Bitcoin.

[475] BENSOUSSAN A., *Informatique Télécoms Internet*, 5ème édition, 2012, Editions Francis Lefebvre

[476] Il est à noter que l'expression « programme » fera ici référence au logiciel ; ce terme étant régulièrement employé dans la littérature ou simplement la loi ; la directive n°2009/24 parle de « programme informatique », là où le Code de propriété intellectuelle mentionne bien le « logiciel ». Dans le cadre de ce chapitre, les deux termes seront utilisés de manière uniforme.

[477] Art. L112-3, 13°, CPI

[478] Qui est protégée au titre du droit d'auteur de manière indépendante à la protection du logiciel en lui-même (voir, à ce titre, notamment CA Paris, 1er juin 1994, arrêt GPL Système)

[479] Cf. *Supra*, p.51

arrêt Pachot le logiciel sera original dès que « son auteur a fait preuve d'un effort personnalisé allant au-delà de la simple mise en œuvre d'une logique automatique et contraignante et que la matérialisation de cet effort réside dans une structure individualisée[480] » ; en prolongement, la pertinence des choix ne peut non plus entrer en ligne de compte[481]. Enfin, un arrêt de 2008 rappelait que l'originalité est corollaire des choix de l'auteur, sans prise en compte de simples attributs techniques[482]. Également, point intéressant quant aux logiciels *blockchain*s, les algorithmes ainsi que les fonctionnalités, ne sont pas protégeables par le droit d'auteur, relavant des idées, qui restent de libre parcours. Sur ce point, il sera opportun de simplement rappeler que la jurisprudence reste constante sur ce refus[483,484].

En conséquence, il en reste que pour sa partie logicielle, une *blockchain* pourra bien évidement rechercher son originalité, si tant est que les réflexions précédentes soient respectées. Dès lors, l'application simple des critères retenus par la loi et la jurisprudence ne semblent pas s'opposer à la recherche de l'originalité d'un logiciel *blockchain* et donc à sa protection par le droit des logiciels. En conséquence, l'identification de l'auteur d'une *blockchain* reste un point important.

§2 : L'alternance de l'auteur du logiciel *blockchain*

261. Dans le cadre du droit d'auteur appliqué au logiciel, la durée de protection sera, classiquement, celle prévue par le Code de propriété intellectuelle, soit 70 ans après la mort de l'auteur[485]. Il reste que pour être efficace, la protection d'un logiciel *blockchain* doit avoir son auteur identifié. On rappellera que la *blockchain* est une initiative mise en exergue avec le développement de *Bitcoin* : l'architecture décentralisée mise en place repose sur un logiciel

[480] Cass., ass. plén., 7 mars 1986, précité
[481] GRYNBAUM L., LE GOFFIC C., MORLET-HAÏDARA L., précité
[482] Cass. 1ère Civ, 17 oct. 2012, n°11-21.641
[483] Sur les fonctionnalités : TGI Paris, 4 oct. 1995, JCP 1996, II, 22673, note H. Croze ; T. Com. Nanterre, 9 fév. 2007, RLDI 2008/36, comm. F. Macrez
[484] Sur les algorithmes : Cass. Civ. 1ère, 14 nov. 2013, RLDI 2013, 999, n°3281 ; CA Paris, 23 janv. 1995, LPA, 19 avril 1996
[485] Art. L123-1, CPI

libre[486]. Comme le souligne Hubert de Vauplane[487], il convient de faire une différence entre logiciels protégés par le droit de propriété intellectuelle et ceux dans un format « ouvert », mettant en avant une alternative. La technologie *blockchain* s'est conçue également en réaction de la centralisation du pouvoir sur Internet (on parle ici des GAFA ou GAFAMI[488]), d'où l'utilisation de logiciels sous licence libre de manière privilégiée[489]. Ces regards sur la *blockchain* au travers du droit des logiciels permettent de comprendre les problématiques liées à la désignation du propriétaire de la *blockchain*. L'utilisation de cette politique « du libre » rendant le propriétaire difficile à discerner. Le problème ne se posera guère lors de la conception d'un logiciel *blockchain* purement privée, et les réflexions sur la titularité des droits de droit commun[490] emporteront toutes réponses.

262. Reste que l'alternative d'un l'auteur d'une *blockchain* « publique » reste difficile à cerner. La question de la propriété d'un tel logiciel est à mettre en relation avec la problématique de l'identification du propriétaire. Les pratiques du logiciel libre montrent que les contributeurs sont souvent anonymes, acteurs de diverses communautés informatiques. Si l'on prend l'exemple de la licence libre « GNU[491] », le code source sera transmis avec chacun des octrois d'une telle licence de logiciel. Or, un transfert de licence n'emporte pas transfert de toute l'entière propriété, même quand le logiciel s'accompagne de son code source. Cet anonymat peut rendre donc difficile, voire impossible l'identification du réel propriétaire d'un logiciel concédé sous licence libre. C'est d'ailleurs l'objet de quasi-fantasmes sur une *blockchain* comme *Bitcoin*[492].

---

[486] « Les logiciels dits « libres » sont des programmes d'ordinateur, protégés par le droit d'auteur, qui peuvent être, à titre gratuit et parfois à titre onéreux, copiés, distribués et modifiés selon les termes d'une licence-type. Ce phénomène s'appuie sur le droit d'auteur, tout en contestant nombre de ses principes fondamentaux. » - CARON C., *Les licences de logiciels dits ''libres'' à l'épreuve du droit d'auteur français*, Recueil Dalloz 2003, p.1556

[487] DE VAUPLANE H., *La Blockchain et la loi*, 14 fév. 2016 http://alternatives-economiques.fr/blogs/vauplane/

[488] Cet acronyme représente les géants du web, à savoir Google, Amazon, Facebook, Apple, et selon les utilisations du terme, Microsoft.

[489] On pourra préciser que *Bitcoin* a été publié sous licence « MIT », à savoir un modèle très permissif dans sa réutilisation.

[490] Différents développements, très classiques, peuvent être cités ici : la désignation de l'auteur personne physique, ou encore le cas de la dévolution automatique vers l'employeur.

[491] http://www.gnu.org - GNU : General public License ; il s'agit d'un des modèles les plus répandus de licence libre.

[492] BOSSARD O., *Que savons-nous de Satoshi Nakamoto, l'inventeur du Bitcoin ?*, Forbes, 23 avr. 2019, disponible à : https://www.forbes.fr/finance/que-savons-nous-de-satoshi-nakamoto-linventeur-du-bitcoin/?amp, (consulté le 13/09/2019)

Toutefois, compte tenu des difficultés dans la gestion des licences libres, surtout quand la *blockchain* aura pour objet de gérer des réseaux institués entre plusieurs grandes sociétés (on peut ici citer le cas du consortium R3), sans nul doute que ces conglomérats d'entreprises choisiront de développer leurs propres logiciels propriétaires *blockchain*, et au-delà il appartiendra à l'auteur du logiciel de déterminer en amont les choix de gestion de sa propriété intellectuelle.

263. Dès lors, et sans entrer dans le détail ici, l'exercice des droits moraux[493] sera bien souvent particulièrement difficile pour tout créateur de logiciel *blockchain*, outre les actuelles difficultés présentes nativement dans le droit des logiciels[494]. Néanmoins, s'agissant du droit à la paternité, des problématiques peuvent être intéressantes. Dans un premier temps, on pourra rappeler la maxime « divulgation vaut titre[495] », néanmoins, si cette maxime s'apprête facilement à d'autres objectifs concernés par le droit d'auteur (tableau, sculptures, etc.), le cas d'un logiciel, partagé directement sur Internet, de manière pouvant être anonyme, fait apparaître plus de difficultés. Dans le cadre d'une *blockchain*, publiée par un organisme ou autre personne physique, si la volonté de la publication du nom de son auteur est présente, alors peu de soucis pratiques apparaîtront[496]. Néanmoins d'autres situations peuvent apparaître.

D'une part, l'éventualité, même si limitée, d'un auteur d'une *blockchain* qui souhaiterait que son droit à paternité soit respecté pour une *blockchain* déjà distribuée (au public) depuis un certain temps. Même si le caractère immuable d'une *blockchain* est avéré, le nom de l'auteur ne pourrait pas forcément être apposé sur tous les blocs[497]. En reste la

[493] Sans aire état de développements plus poussés, on pourra se borner à rappeler que les droits moraux, sont réduits dans le cadre du droit des logiciels, conformément à l'article L121-7 du CPI.

[494] On se bornera ici à mentionner le fait que les droits moraux de l'auteur d'un logiciel sont réduits (art. L121-7, CPI).

[495] RAYNARD J., *Le tiers au pays du droit d'auteur*, JCP, 1999 I 138, n°7 et suiv.

[496] Outre des potentiels conflits classiques sur la paternité, d'ores et déjà connus par la loi et la jurisprudence.

[497] Qui, rappelons-le, ne demeurent que des amas de données informatiques retraçant des opérations de hachage.

modification du logiciel de base en tant que tel (par exemple, *Bitcoin* Core[498] pourrait bénéficier d'une mise à jour en cas de revendication de la paternité de son auteur). Néanmoins, l'apposition du nom de l'auteur dans la documentation (matérielle ou immatérielle) liée à la *blockchain* est parfaitement envisageable[499] même s'il peut présenter des soucis pragmatiques.

264. Justement, le cas de la *blockchain Bitcoin* et de son mystérieux auteur, Satoshi Nakamoto, peut être un intéressant cas d'école, en particulier pour ce droit à la paternité mais également pour considérer l'application ou non de l'œuvre orpheline ou pseudonyme. Aucun élément matériel ne démontre une quelconque volonté de l'auteur de la *blockchain Bitcoin* d'exercer son droit de paternité, mais est-ce pour autant une œuvre orpheline pour autant ? On rappellera que le CPI défini l'œuvre orpheline comme « l'œuvre protégée et divulguée, dont le titulaire des droits ne peut pas être identifié ou retrouvé, malgré des recherches diligentes, avérées et sérieuses[500] », et que cette notion présente surtout un intérêt pour un exploitant souhaitant échapper à une contrefaçon[501] ; ici, il n'est pas question de la « perte » d'un auteur, mais plutôt la consécration d'une volonté positive de ne pas se révéler. Alors, l'existence des œuvres anonymes[502], licites, permettant la publication d'une œuvre sans révéler l'identité de l'auteur parait plus opportune. Même en l'absence de « publicateur », quoique le pseudonyme de Satoshi Nakamoto, pourrait être considéré comme tel au nom d'une quelconque théorie de l'apparence, on peut alors y voir, de manière fantasque, une brèche pour Satoshi Nakamoto, de se révéler au grand jour le moment venu. Le régime de l'œuvre anonyme permettant à l'auteur de conserver ses prérogatives et de se révéler à tout moment au public.

S'agissant du droit au respect[503], quoique mis à mal par le droit positif sur le logiciel, l'auteur garde la possibilité de s'opposer à toute modification entraînant pour lui une atteinte

---

[498] Bitcoin Core est le client logiciel permettant à n'importe quel ordinateur de se connecter à la *blockchain* Bitcoin et d'en devenir un mineur (pour plus d'informations : https://github.com/bitcoin/bitcoin/releases/tag/v0.21.1).

[499] D'autant plus que la loi ne précise pas le support de ce nom à apposer ; VIVANT M., *Droits moraux sur les œuvres logicielles*, Le Lamy droit du numérique (Guide*)*, n°2631

[500] Art. L113-10, CPI

[501] Or, dans le cadre de Bitcoin, la volonté, quasi anarchiste de se libérer du système bancaire, démontre une volonté de son auteur de partager sa création et d'en avoir une diffusion large, que le système de propriété intellectuelle tendrait, au contraire, à limiter.

[502] Art. L113-6, CPI

[503] Art. L121-7, CPI

à son honneur ou à sa réputation. Néanmoins, s'agissant du logiciel libre, ce droit s'efface d'autant plus car, en pratique, les licences libres ne prévoient pas cette possibilité.

Outres ces développements sur une existence, classique, de droits moraux sur une *blockchain*, c'est surtout l'exercice des droits patrimoniaux (et donc l'exploitation de tels logiciels) revenant à leurs titulaires respectifs et en fonction des contrats de licences accordés, qui font apparaître certaines spécificités.

Section 2 : L'exploitation délicate de logiciels *blockchain*

265. Au-delà des caractères classiques d'un logiciel *blockchain* en ce qu'il concerne la désignation de l'auteur ou encore ses prérogatives liées aux droits moraux, il faut conserver en ligne de mire une spécificité de la *blockchain*, à savoir la réplication au sein du réseau P2P du logiciel *blockchain*. Chaque mineur ou participant à une *blockchain* va, pour participer à son intégrité, partager un même logiciel. Dans le cadre de la *blockchain Bitcoin*, chaque mineur va devoir télécharger *Bitcoin* Core[504]. Si la lecture de la licence MIT se rapproche d'une licence complètement libre, à savoir une large possibilité de reproduction, toute *blockchain* n'est pas forcément soumise à ce type de licence. C'est pourquoi la gestion patrimoniale d'une *blockchain*, en ce qu'elle concerne l'exercice des différents droits patrimoniaux ne doit pas être omise et reste délicate. Néanmoins, à la lumière du droit positif, certaines spécificités d'une *blockchain* vont être mises en avant. La gestion patrimoniale d'une *blockchain* (§1) s'en trouve alors minorée. Également, une certaine précarité des droits d'exploitation, induits par des aménagements liés par les aspects techniques de la *blockchain* doit être analysée (§2).

[504] https://bitcoin.org/fr/telecharger ; Bitcoin Core est le logiciel client, permettant la participation à la *blockchain* Bitcoin ; en l'occurrence, il est également important de rappeler que ce logiciel est publié sous licence MIT (disponible à https://opensource.org/licenses/mit-license.php).

§1 : La gestion patrimoniale émoussée d'une *blockchain*

266. De manière liminaire, le CPI prévoit un certain nombre de règles dérogatoires s'agissant des droits patrimoniaux attachés au logiciel[505]. Il convient de viser deux pans de l'appréhension de cette gestion patrimoniale : une gestion qui pourra être considérée comme classique (comme un logiciel dit propriétaire standard) et une gestion propre au logiciel libre. S'agissant du logiciel libre, il conviendra également de rappeler que des libertés essentielles doivent être accordées aux utilisateurs de tels logiciels, en particulier la liberté d'en étudier le fonctionnement ou encore de le modifier[506]. Cela étant, seules les *blockchain*s ayant un auteur identifié (soit dans le cadre d'un développement propre à une entreprise, ou encore dans le cadre d'une *blockchain* de type BaaS[507]).

267. Le monopole de l'auteur, dans le cadre d'une gestion classique, permet une gestion de la traduction ou de la mise sur le marché par tout procédé, de manière tout à fait « lambda », et n'emportera pas ici plus de développements étant donné que le régime applicable sera celui de l'exploitation du logiciel classique. À l'instar du droit de mise sur le marché à titre onéreux ou gratuit.

La reproduction du logiciel *blockchain* classique mérite plus de développements. En effet, si le CPI prévoit que la reproduction permanente ou provisoire d'un logiciel (comprenant l'affichage, l'exécution, ou encore la transmission) sous seule autorisation de l'auteur[508], cette nécessaire autorisation est mise à mal par la nature même de la *blockchain*. De surcroît, encadré par nature pour le logiciel, visé par la directive dite DADVSI[509], un épuisement du droit de distribution est prévu en cas de première vente pouvant être opérée par téléchargement sur internet[510]. Cela étant, la mise à disposition, par exemple dans le cadre d'un SaaS, ne saurait être considérée comme une vente. Dès lors, comme concevoir la reproduction d'un

[505] Art. L122-6, CPI ; sont visés, notamment, les droits de reproduction (permanente ou provisoire) ; la traduction, l'adaptation ou encore la modification ; et enfin la mise sur le marché à titre onéreux ou gratuit.

[506] À côté de ces deux libertés, celles d'exécuter le logiciel ainsi que celle de le diffuser font partie des critères retenus par la Free Software Foundation, créée en 1985 ; pour plus d'informations : https://fr.wikipedia.org/wiki/Free_Software_Foundation (consulté le 10/09/2020).

[507] Ou *Blockchain as a service*, expression empruntée au SaaS, *Software as a Service.*

[508] Art. L122-6, CPI

[509] Directive n°2001/29/CE relative à l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information

[510] CJUE, 3 juill. 2021, aff/ C-128/11, arrêt dit UsedSoft/Oracle ; *LEFEVRE A. La mise à disposition de copies de logiciels (…) de l'éditeur sur ces copies*, Revue Lamy Droit de l'Immatériel, n°85, 1er août 2012

logiciel *blockchain* à l'ensemble des mineurs souhaitant y participer ? En effet, un protocole *blockchain* repose sur la distribution et la multiplicité des acteurs y participant, plus leur nombre augmente, plus l'intégrité de la *blockchain* est renforcée. Dès lors, par nature, l'auteur d'un logiciel *blockchain* doit concéder, *de facto*, un droit de distribution (comprenant notamment le droit de reproduction permanente ou provisoire) non-exclusif à l'ensemble des participants afin que le réseau mis en place puisse bénéficier des avantages d'une *blockchain*. À défaut d'une telle prédisposition, toute *blockchain* serait vidée de sa substance, car y participer placerait n'importe quel mineur dans une situation de contrefaçon, dans une logique propre au droit des logiciels, d'ores et déjà connue par la jurisprudence[511]. Insistant sur une pratique contractuelle rigoureuse pour toute rédaction de contrat de licence *blockchain*.

268. Adaptée au monde du logiciel libre, la pratique contractuelle aura tout son sens pour l'exploitation et surtout la distribution d'une *blockchain*. Les logiciels libres demeurent originaux dans le sens où ils ont été conçus en opposition avec les systèmes de propriété intellectuelle classique[512]. Le logiciel libre peut se traduire par la faculté laissée aux utilisateurs d'exécuter, partager ou notamment modifier le logiciel visé. L'idée sous-jacente est de favoriser le partage et la réutilisation des logiciels libres, dans une véritable « mise en communauté du logiciel diffusé[513] ». Néanmoins, toutes les licences libres ne se valent pas, et le choix de la licence libre aura également son importance, et cela peut être notamment pour cette raison (pour prendre l'exemple de la *blockchain Bitcoin*) que le choix de la licence MIT[514] a été opéré.

269. La question de la validité d'une licence libre sur une *blockchain*, notamment en ce qu'elle concerne la délimitation des droits cédés demeure également intéressante. Certaines licences libres comprennent par nature l'autorisation de l'auteur de distribution des copies de programmes, à titre onéreux ou non, ou encore de recevoir le code source du logiciel visé[515]. Néanmoins, le logiciel libre n'est pas exempt de l'application des règles du droit de la propriété

[511] CJUE 18 déc. 2019, C-666/18, *IT Development c. Free Mobile ;* HADDAD S., CARLER F., CASANOVA A., *Le débat est (enfin) tranché : le non-respect des termes du contrat de licence de logiciel est une contrefaçon*, Revue Lamy Droit de l'Immatériel, n°167, 1er fév. 2020

[512] BITAN H., *Droit des créations immatérielles*, Lamy 2010

[513] VIVANT M., *Lamy droit du numérique*, Wolters Kluwer, 2021, §2314

[514] Cf. *Supra*, p.130

[515] Par exemple, c'est le cas de la licence GNU GPL.

intellectuelle, en particulier les dispositions de l'article L131-3 du CPI[516]. Formalisme d'ordre public, la transmission des droits concédés doit faire l'objet d'un écrit[517] (quoique le support de l'écrit n'est pas précisé) et nombre de licences libres méconnaissent cette disposition, les frappant de nullité relative[518]. En ce sens, la *blockchain* ne fait pas exception, et cette problématique y trouve application également.

270. Afin de déterminer le régime applicable à une *blockchain*, plusieurs situations doivent être identifiées. Dans un premier temps, la détermination de la typologie de la *blockchain* doit être effectuée (publique, privée, hybride, ou encore en type BaaS). Dans un second temps, le choix de gouvernance et, corrélativement, de licence retenue est nécessaire. S'agissant de la typologie de *blockchain*, une nouvelle fois, il convient d'exclure toute analyse de *blockchain* purement privée, qui restera l'apanage d'un acteur identifié, et donc la seule spécificité sera d'utiliser un protocole *blockchain* en lieu et place de n'importe quel autre protocole informatique, renvoyant ainsi toute problématique aux développements existants pour le logiciel dans le cadre du droit positif.

S'agissant d'une *blockchain* hybride et sous format BaaS, un raisonnement similaire pourra être retenu. La particularité d'une telle *blockchain* résidant dans le fait que ses utilisateurs (à l'exception des nœuds de validation qui seront préalablement choisis par l'éditeur de la *blockchain*, et donc soumis au régime de licence logiciel classique) ne peuvent disposer qu'un droit d'utilisation ou d'accès à la *blockchain*, sans pour autant emporter épuisement du droit de distribution rattaché au logiciel[519]. S'agissant d'une *blockchain* purement publique, force est de constater que le régime applicable aux logiciels libres, dans tout son esprit communautaire, sera appliqué, la spécificité résidant principalement dans le fait que le partage d'un logiciel *blockchain* est prévu par nature.

---

[516] Art. L131-3, CPI, 1er al. « La transmission des droits de l'auteur est subordonnée à la condition que chacun des droits cédés fasse l'objet d'une mention distincte dans l'acte de cession et que le domaine d'exploitation des droits cédés soit délimité quant à son étendue et à sa destination, quant au lieu et quant à la durée. ».

[517] LE GOFFIC C. *Licences libres et copyleft : la contractualisation du droit d'auteur*, Revue Lamy Droit de l'immatériel, n°77, 1er déc. 2011

[518] MACREZ F., *Créations informatiques : bouleversement des droits de propriété intellectuelle ? Essai sur la cohérence des droits*, collection CEIPI, 2011, Lexisnexis

[519] Cf. *Supra*, p.121 et suiv.

§2 : Les aménagements d'exploitation nécessaires à la *blockchain*

271. Plusieurs exceptions aux droits des auteurs sont prévues[520], néanmoins, appliquées au droit des logiciels, certaines de ces exceptions sont expressément inapplicables, comme l'exception de reproduction technique transitoire et les exceptions de copie privée. Si certaines d'entre elles sont peu applicables en pratique[521], d'autres sont spécifiques au logiciel[522], tels que le droit d'utilisation et d'auto-maintenance des utilisateurs, d'effectuer une copie de sauvegarde, d'étudier le logiciel et le droit de décompilation.

Concernant le droit d'utilisation et d'auto-maintenance, s'ils permettent, notamment, à un utilisateur légitime le droit de reproduire ou modifier le logiciel visé à des fins de correction d'erreur ou pour respecter sa destination, voient leur application potentiellement modifiée au sein de la *blockchain*. Il convient de faire un rappel sur le fonctionnement d'une *blockchain*, qui repose sur la multiplicité de ses membres (mineurs), et un partage des données et du logiciel de base. Pour fonctionner, la communauté des participants à la *blockchain* est soumise aux mêmes règles, par exemple, tous les mineurs de la *blockchain Bitcoin* sont soumis aux règles du *Bitcoin* Core[523]. Ce dernier décrit les différentes règles de fonctionnement, y compris les règles pour « créer » du *Bitcoin*.

272. Or, en cas de désaccord ou de changement sur les règles de fonctionnement, un *fork* peut paraître nécessaire. De manière simplifiée, la chaîne de blocs, à la suite d'un *fork* se dédouble, et deux chaînes parallèles peuvent coexister, sans pour autant nuire à la pérennité de la *blockchain* visée[524]. Un *fork* pouvant être plus ou moins important pour une *blockchain* ; un *hard fork* résultant de la modification du protocole *blockchain* de base[525] et un *soft fork* résultant de la simple concomitance de création de bloc[526]. La spécificité d'un *hard fork* est qu'il est intentionnel, et résulte de la volonté des participants à une *blockchain* (expliquant notamment pourquoi certains voient dans la *blockchain* une parfaite représentation

---

[520] Art. L122-5, CPI

[521] Sont ici visées notamment le droit à la parodie ou encore les représentations dans un cercle de famille.

[522] Art. L122-6-1, CPI

[523] https://fr.wikipedia.org/wiki/Bitcoin_Core (consulté le 27/06/2021)

[524] Pour exemple, la *blockchain* Bitcoin permet le support deux actifs immatériels par suite d'une *hard fork*, le bitcoin (traditionnel) et le bitcoin cash depuis le 1er août 2017.

[525] ANTONOPOULOS A, « Mastering Bitcoin : Programming the Open *Blockchain* », 2ème édition, 2017, glossaire

[526] *Ibid.*

démocratique). Or, si une majorité de participants ne souhaitent pas de modification du protocole, alors aucun *fork* n'est possible[527]. Soumettant donc toute modification à l'adhésion du plus grand nombre, peu importe sa nature.

En conséquence, le droit d'effectuer une modification du logiciel, notamment en cas d'erreur, peut être mis à mal, de manière pragmatique, avec une *blockchain* non soumise aux différents régimes de licence libre. En effet, si ce droit existe à l'échelle individuelle, cette vision n'apparaît que peu applicable à une *blockchain*, étant donné qu'un utilisateur ne l'est qu'en raison de son appartenance à une communauté. Il est impossible pour un utilisateur de procéder à une modification du logiciel *blockchain*, même pour des raisons de sécurité, tout en restant membre de la communauté ; ayant réalisé une modification du logiciel, il entre dans un conflit de version, et s'isole donc du reste de la communauté. La modification réalisée devant faire l'objet d'un consensus à défaut d'être rejetée.

Néanmoins, cette exception n'est pas d'ordre public et l'auteur (si tant est qu'il est identifié), peut déterminer les modalités spécifiques à un tel droit de modification. En reste qu'en pratique, et surtout pour des mises à jour de sécurité, un consensus au sein de la communauté utilisatrice d'une *blockchain* n'a pas d'apparente raison d'être refusé. Dans le cadre d'une licence libre - de manière pragmatique et majoritaire - les mises à jour de sécurité sont publiées et partagées entre les différents utilisateurs.

273. S'agissant de la copie de sauvegarde, une telle copie est subordonnée à la double condition de nécessité et de bénéfice d'une licence préalable[528]. Néanmoins, le fait qu'un logiciel libre *blockchain* soit partagée entre ses utilisateurs et le plus souvent disponible sur les réseaux Internet, l'application pratique de cette exception n'offre que peu de difficultés. Également, pour le cas d'une *blockchain* visée par une licence classique (quoique présentant peu d'intérêt en cas d'un nombre limité d'utilisateurs), toute difficulté se retrouve purgée par des solutions déjà connues par le droit positif et la jurisprudence[529].

274. Les dernières exceptions tirées du CPI, à savoir le droit d'étudier le logiciel et le droit de décompilation emportent une nouvelle fois un *distinguo* nécessaire entre logiciel libre et logiciel « classique ». Si le logiciel libre, du fait de sa volonté de partage et de publicité

[527] Sous réserve d'une éventuelle « attaque des 51% ».
[528] VIVANT M., *Lamy droit du numérique*, §56, mise à jour de mai 2021
[529] Pour exemple sur la licéité d'une copie de sauvegarde : CA Paris, 13e ch., 20 sept. 2005, no 04/0237

emporte une facilité d'étude et de décompilation (étant donné la disponibilité des codes sources ou encore de la documentation inhérente), le cas commun du logiciel peut emporter d'autres difficultés une fois appliqué à la *blockchain*. Comme le souligne le professeur Gautier[530], l'interopérabilité devient une constante dans les exceptions, permettant aux utilisateurs d'assurer une comptabilité avec d'autres logiciels. Facette importante de la *blockchain*, en particulier celles servant de support à des applications diverses et variées[531], l'interopérabilité est bien souvent nécessaire pour l'exploitation d'une *blockchain*, tant elle a vocation aujourd'hui à se greffer à des systèmes d'information préexistants. Le CPI précisant notamment que les mesures techniques en place ne devant pas empêcher cette interopérabilité[532], cette dernière répond à plusieurs critères, en particulier une relative à l'accès légitime de l'utilisateur au logiciel donné[533]. De plus, les informations issues de ce droit de décompilation, si elles sont limitées à la seule interopérabilité, ne peuvent être communiquées aux tiers, hormis dans le cadre d'une stricte nécessité[534] (d'autant plus que la seule raison d'assurer une mise à jour de sécurité en utilisant les informations issues d'une décompilation ne saurait être une raison légitime et constituerait une contrefaçon[535]).

Dès lors, deux conceptions peuvent trouver à s'opposer : la volonté d'appliquer de manière *stricto sensu* le droit des logiciels, notamment en limitant/se réservant le droit de décompilation (en tant que prérogative de l'auteur d'être seul libre d'en consentir sous toutes ses formes), ou alors à abandonner de manière volontaire un tel droit de décompilation. En effet, si la première solution a le mérite d'illustrer de manière adéquate l'esprit de la technologie *blockchain*, la seconde reste une expression juste et légitime des prérogatives de l'auteur. Pourtant, ce droit à l'interopérabilité, y compris dans le cadre d'une communication à des tiers pourrait être légitime dans le sens où plus une *blockchain* possède de participants, plus sa sécurité et son intégrité est renforcée. Appelant potentiellement à un nécessaire aménagement de ce droit à l'interopérabilité dans le cadre de l'exploitation d'une *blockchain*. Même si en soi, cet aménagement n'a, à notre sens, que peu de chance d'aboutir un jour. De

---

[530] GAUTIER P.-Y. précité.

[531] Pour exemple, la *blockchain Ethereum* a notamment pour but de supporter différentes applications, notamment à travers les *smart contracts.*

[532] Art. L331-5, CPI

[533] On rappellera que les deux autres critères sont l'absence de mise à disposition facile et rapide des informations permettant l'interopérabilité et que la décompilation soit limitée aux parties nécessaires du logiciel.

[534] CA Caen, Ch. Corr., 18 mars 2015, *Skype Ltd.,* RLDI 2015/116, n° 3771, comm. DUPONCHELLE M.

[535] VIVANT M., *Lamy Droit du numérique*, 05/2021 - §2669 - Décompilation du logiciel ou « reverse engineerig »

plus, toute tentative en ce sens serait à l'encontre des prérogatives naturelles de l'auteur et du droit positif, peu importe les caractéristiques disruptives d'une telle technologie.

275. Il est possible d'assister, pour la *blockchain*, à une nouvelle tendance envers la contractualisation des droits d'auteur, comme peut le soutenir une partie de la doctrine[536]. En effet, la nature même d'une *blockchain* appelle à son partage et à une évolution commune (même si seulement sur des aspects techniques), dès lors, cette contractualisation des droits semble même devoir être encouragée au profit de cette technologie.

Parler de contractualisation de droits d'auteur n'est pas sans appeler des développements particuliers sur la contrefaçon. Définie par la loi[537], elle n'emporte guère de particularités s'agissant du logiciel, même si dans le cadre d'une telle logique, il conviendra de rappeler que toute violation d'un contrat portant sur des droits d'auteur est constitutive d'une contrefaçon[538]. Dans une déroulante logique, elle n'emporte pas de spécificités intrinsèques liées à un logiciel *blockchain*. Néanmoins, il conviendra de rappeler que le Professeur Caron identifiait déjà la possibilité de la nullité d'une licence libre, et dans un tel cas, la « contamination » contrefaisante pouvant atteindre l'ensemble des utilisateurs d'un logiciel libre[539]. Dans le cas précis d'une *blockchain*, cette contamination en cascade peut être dramatique tant l'ensemble des utilisateurs sont connectés en réseau, et que leur identification est d'autant plus aisée du fait que l'ensemble des données soit partagé entre tous. Cette spécificité doit, à notre sens, être prise en compte dans toute contractualisation relative à la mise en place d'une architecture *blockchain*, au-delà des potentielles clauses exonératrices ou subrogatoires de responsabilité[540] pouvant être mises en place.

---

[536] LE GOFFIC C. précité*e*

[537] Art. L335-3, CPI « Est également un délit de contrefaçon toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur, tels qu'ils sont définis et réglementés par la loi. Est également un délit de contrefaçon la violation de l'un des droits de l'auteur d'un logiciel définis à l'article L. 122-6. (…) ». Également, peuvent être mentionnés l'importance des éléments matériels ou moraux, en particulier l'indifférence de la bonne foi dans la caractérisation d'une contrefaçon.

[538] En tant que violation des droits de l'auteur ; cf. CJUE 18 déc. 2019, C-666/18, *IT Development c. Free Mobile*, précité

[539] CARON C. précité

[540] LE TOURNEAU P., précité

Conclusion du Chapitre 1

276. Outre les spécificités intrinsèques d'une *blockchain* quant à ses potentielles utilisations, une application sémantique des règles du droit positif arrive à une conclusion simple, voire simpliste : une *blockchain* demeure un objet connu de droit, concerné notamment par les règles du droit des logiciels. Il ressort d'un arrêt de Cour d'appel que « Considérant que si le législateur distingue ainsi le programme d'ordinateur, dont la caractéristique est d'être opérationnel, de la base de données informatique, objet du traitement par le programme et dont la caractéristique est d'être statique, il existe entre ces deux catégories un *continuum*, l'efficacité de la recherche dépendant autant du logiciel que de la mise en forme préalable des données et des règles d'organisation de la base, tous ces éléments étant imbriqués (…)[541]», imposant ainsi de ne pas omettre le lien pouvant être fait entre un programme d'ordinateur (pris dans une conception logicielle, donc dans ses composantes de code source et autres) et une base de données en découlant. Encore une fois, l'application d'une appréciation globale et homogène de notions par nature hétérogène se réalise dans l'univers numérique. Cette solution retenue par la jurisprudence nous indique alors naturellement de procéder à une étude de la protection d'une *blockchain* par le droit des bases de données.

[541] CA Paris, 10 mai 2016, n° 14/08976

Chapitre 2 : La concordante protection de la *blockchain* par le droit des bases de données

277. Une définition retenue de la *blockchain*, outre sa transcription dans le vocabulaire de l'informatique[542], avance le terme de « Mode d'enregistrement de données produites en continu, sous forme de blocs (…) ». Le CPI[543] envisage la base de données comme un recueil d'œuvres, de données, ou d'autres éléments indépendants. Et en tant que moyen d'enregistrement de données, une *blockchain* reste bien alors une base de données, distribuée, partagée et chiffrée qui sert ainsi de répertoire d'informations public, irréversible et incorruptible[544]. Les bases de données ont une conception très utilitaire, le but étant de gérer, compiler, même classer toute une série d'informations. La CJUE, dans une série de trois arrêts, a affiné cette définition en précisant qu'une base de données doit être constituée d'éléments séparables, et organisée d'une manière arbitraire[545]. Cela étant, il est possible d'exclure un simple regroupement naturel d'informations de la qualité d'une base de données. Enfin, la lecture de la lettre de la loi, au regard de la directive de 1996[546] nous indique trois niveaux de protection : sur la structure en tant que telle (le contenant), les éléments de la base de données (le contenu) mais également l'ensemble que représente la base, considérée globalement[547]. Au-delà de la continuité de cette approche sémantique relative à la *blockchain*, il convient dès lors d'étudier une dualité classique, portant aussi bien sur le contenant que le contenu[548]. Les bases de données faisant l'objet d'une dualité de protection, l'étude de l'application du régime inhérent au droit de la propriété littéraire et artistique doit être effectuée d'une part (Section 1) et celui du droit dit *sui generis* d'autre part (Section 2).

[542] JORF n°0121 du 23 mai 2017 - texte n° 20, précité

[543] Art. L112-3, CPI

[544] LEAGEAIS D., *JurisClasseur commercial, Fascicule Blockchain*, LexisNexis, mai 2018

[545] CJCE, 9 nov. 2004, C-203/02, C-46/02 et C-338/092, voir notamment CCE 2005, comm. 2, CARON C.

[546] Directive 96/9/CE du Parlement européen et du Conseil, du 11 mars 1996, concernant la protection juridique des bases de données

[547] SIRINELLI P. *Le Lamy Droit des médias et de la communication*, Wolters Kluwer, Étude 136, màj de fév. 2000

[548] Faisant ainsi écho direct à la caractérisation classique des éléments d'une base de données.

Section 1 : Application légitime du régime de propriété littéraire et artistique

278. Dans le cadre d'une application sémantique et pragmatique des régimes de propriété littéraire et artistique, le droit des bases de données va se focaliser sur le contenant d'une base de données, étant donné que chaque élément doit rester individuellement accessible[549], néanmoins les prérogatives de l'auteur, ainsi que les tenants de l'exploitation d'une telle base de données doivent être étudiés. Pourtant les concepts d'auteur et d'originalité de la base de données *blockchain* induisent une nouvelle fois une application classique (§1) et l'exploitation des droits d'auteurs ressort aussi d'une certain routine s'agissant d'une base de données *blockchain* (§2).

§1 : Les attributs classiques de la base de données *blockchain*

279. Le Code de la propriété intellectuelle prévoit une application du droit d'auteur sur les bases de données en ce qu'elles peuvent être considérées comme des œuvres de l'esprit[550]. En tant qu'œuvre de l'esprit, une base de données doit revêtir la condition d'originalité. En ce sens, les bases de données couvrement par le droit d'auteur seront considérés comme « œuvres d'information », dans une conception retenue par la jurisprudence, dans un arrêt dit Microfor[551].

Le CPI retient, pour la notion d'originalité, un « choix ou une disposition particulière des matières », dans le sens où l'organisation de la base, si tant être qu'elle reflète l'empreinte de la personnalité de son auteur, pourra être originale. La distinguant ainsi de la simple compilation, qui n'est pas protégeable par le droit d'auteur[552]. En réalité, l'appréciation de l'originalité d'une base de données repose sur une logique parallèle à celle en œuvre pour le

[549] Art. L112-3, CPI

[550] Art. L112-2, précité

[551] Cass. Plén., 30 oct. 1987, JCP éd. G 1988, II, no 20932, RIDA janv. 1988, p. 78, RTD com. 1988, p. 57, obs. FRANÇON A., D. 1988, som., p. 206, obs. COLOMBET C.

[552] Cass. 1re civ., 13 mai 2014, nº 12-27.691, « *Originalité d'une base de données caractérisée par la Cour de cassation* », Revue Lamy Droit de l'immatériel, n°105, 1er juin 2014

logiciel, comme a pu le déclarer la Cour de cassation[553], en utilisant notamment l'expression « d'apport intellectuel », corroboré par d'autres arrêts rendus préalablement[554].

Au-delà, doit également être rappelé que seul le contenant pourra bénéficier de la protection au titre du droit d'auteur et que surtout, la présence d'éléments couverts par un tel droit n'emporte pas protection à ce titre de la base pour autant[555]. Dans une situation inverse, la présence d'éléments couverts par le droit d'auteur au sein d'une base de données n'emporte pas non plus pour autant protection de la base en tant que telle à ce titre[556] Également, doit être rappelé que la nature de la base de données ne conditionne pas l'application ou non du critère d'originalité[557], solution heureuse pour une application à la *blockchain*, tant son support demeure particulier, en raison de la mise en réseau et du partage des différentes données afférentes.

280. Sur le critère d'appréciation globale d'une base de données, l'originalité peut être recherchée sur le choix des éléments composant la base. Si la nature des données n'emporte pas d'appréciation sur l'originalité de la structure[558], c'est la recherche, les choix arbitraires des données composant la base qui lui peut revêtir une originalité. Au-delà, une partie de la doctrine aurait tendance à refuser une protection au nom de ces choix[559], en raison que ces choix restent « fonctionnels(s) », une autre partie considère que c'est une recherche de « rationalité[560] » qui s'exprime dans le choix des données, excluant ainsi toute originalité. Dès lors, plus on s'éloigne de ces adjectifs, plus il est possible de retrouver des choix arbitraires, et donc empreints de personnalité. À ce titre, au regard de l'applicabilité du droit d'auteur, la *blockchain* se retrouve une nouvelle fois incluse de manière naturelle dans ces critères.

---

[553] Cass. 1re civ., 13 mai 2014, nº 12-27.691, précité

[554] Par exemple : CA Paris, 18 juin 2003, D. 2003, somm., p. 2756, note SIRINELLI P.

[555] T. com. Nanterre, 7e ch., 16 mai 2000, Rev. Lamy dr. aff. 2000, no 29, no 1843, obs. Costes L.

[556] CJUE, 3e ch., 1er mars 2012, aff. C-604/10, Football Dataco e.a. c/ Yahoo ! UK Ltd e.a, http ://curia.europa.eu, RLDI 2012/81, no 2710, obs. CASTETS-RENARD C.

[557] T. com. Paris, 15e ch., 19 mars 2004, Rev. Lamy dr. aff. 2004, no 73, no 4576

[558] Cf. *Supra*, p.138

[559] GAUDRAT P., *Droits et obligations de l'utilisateur d'une banque de données*, Brise, no 12, CNRS éd., nov. 1988

[560] SIRINELLI P. *Le Lamy Droit des médias et de la communication*, précité

281. Dès lors, où peut se situer l'originalité d'une base de données *blockchain* ? Concernant l'appréciation de ce critère par rapport à une *blockchain*, comme présenté précédemment, une *blockchain* suit une logique propre, fonction des objectifs donnés à cette dernière. Par exemple, lorsqu'une *blockchain* est utilisée dans le seul objectif d'effectuer des transferts d'actifs, il s'agira de démontrer le caractère original des choix effectués dans la disposition des données de la base créée pour effectuer ces transferts de fonds. Dès lors, dans un exemple limitatif d'application du droit positif, lorsqu'une *blockchain* sera créée pour de simples transferts d'actifs, la démarche originale, les choix arbitraires de l'auteur seront difficiles à rapporter. D'autant plus que les choix effectués n'auront que de sens les finalités fonctionnelles de la *blockchain* concernée, et dans ce cas, l'originalité d'une telle base de données a déjà été refusée par la jurisprudence[561].

Il ressort que l'originalité d'une *blockchain* peut être mis à mal par ses caractéristiques techniques, pouvant porter également sur l'ordonnancement chronologique des actions sur les différentes données. C'est l'une des particularités premières de la *blockchain*, enregistrer de manière régulière et cyclique, les différentes actions sur les données visées. Si le simple enregistrement chronologique a déjà pu servir à rejeter l'originalité[562], elle devrait être logiquement être refusée également pour toute *blockchain* dont les données seraient classées pour ce seul critère. Or, rien n'oblige, techniquement, une *blockchain* à orchestrer l'organisation de ses données exclusivement de manière chronologique. Un classement des données en fonction de la nature ou du nombre de transactions, ou encore en fonction de la fonction de hachage choisie pourraient être des facteurs à prendre en compte pour la détermination ou non de l'originalité d'une *blockchain*. Également, si la protection au titre du droit d'auteur est possible, l'exhaustivité peut nuire la démonstration du critère d'originalité. En effet, l'exhaustivité conduisant à annihiler tout choix arbitraire, néanmoins, le choix de la disposition pourra emporter conviction lors du contrôle du juge[563].

[561] CA Paris, 11 mai 2011, RLDI 2011/72, n°2382

[562] CA Paris, 28 fév. 2007, voir com. RIDA 2007, n°212, p.150

[563] Cass. 1ère Civ., 22 sept. 2011, nº 10-23073, com. MALLET-POUJOL N., *La protection des bases de données : un péage pour l'accès aux informations génériques ?*, Revue Lamy Droit de l'immatériel, Nº 93, 1er mai 2013

Toutefois, l'une des possibilités de la technologie *blockchain* est l'introduction de « *smart contracts* », des connecteurs logiques afin d'arriver à un résultat particulier. Un *smart contract* sera nécessairement empreint des choix de son auteur, en fonction de ses finalités et de ses objectifs. À ce titre, le « contrat intelligent », en ce qu'il affectera l'organisation de la base de données *blockchain* créée, répondra à des choix propres à son auteur. Cette analyse rejoindrait d'ailleurs celle effectuée par la Cour de justice de l'Union européenne dans son arrêt « *Football Dataco* »[564]. Néanmoins, la nuance entre les choix originaux découlant de l'application du logiciel et ceux découlant de la base de données en tant que telle pourra être difficile à rapporter.

Par ailleurs, dans l'élaboration d'une *blockchain* hybride, l'auteur devra faire preuve de personnalité, de créativité afin d'élaborer la structure de la *blockchain*, qui aura pour rôle de compiler, d'organiser les données suivant un schéma précis, non banalisé, afin de répondre aux objectifs voulus. Cet apport intellectuel de la part de l'auteur conférera les conditions requises pour accéder à la protection conférée par le droit d'auteur.

282. Aussi, rappelons que la *blockchain* reste l'association d'un logiciel et d'une base de données, et qu'en conséquence, une application distributive doit être appliquée. Pourtant, pris cette fois dans une conception globale, la protection de la base de données pourrait-elle découler de celle du logiciel ? La jurisprudence tendrait vers la négative, en particulier pour donner suite à un arrêt de 2011, portant sur la protection de l'architecture d'une base de données associée à un logiciel[565]. Dans les faits de l'espèce, la partie demanderesse affirmait que sa base de données, pour laquelle elle cherchait à obtenir réparation d'actes de contrefaçon en raison de l'usage de la structure de sa base de données. La Cour a pu rappeler que si la base de données peut être protégée par le droit d'auteur, cette dernière avait son « architecture associée au logiciel », et que devaient être précisés les « choix des matières ou quelle disposition (…) portant l'empreinte de (la) personnalité ». En l'espèce, la Cour rejette alors

[564] CJUE, 1er mars 2012, arrêt Football Dataco c/ Yahoo, précité. Dans cet arrêt, la Cour, saisie d'une question préjudicielle, a précisé certains points :
- l'originalité d'une base de données réside dans sa structure ;
- la liberté créatrice de l'auteur dans le choix ou la disposition des matières est importante.

[565] Cass. 1re civ., 22 sept. 2011, nº 10-23.073, voir com. COSTES L. Revue Lamy Droit de l'Immatériel, n°76, 1er nov. 2011

l'originalité de l'architecture de la base de données tant elle découle non pas de choix arbitraires et originaux, mais du logiciel. Cette solution offre un aspect particulièrement intéressant une fois appliquée à la *blockchain*. La recherche de l'originalité, pour la base de données, devra découler non pas du logiciel créant la base de données, mais bien d'elle-même, en soi. En conséquence, tant la complémentarité du logiciel et de la base de données est forte, et compte tenu de la possible qualification d'une *blockchain* de « système expert[566] », il en ressort une potentielle difficulté pour son appréciation.

283. Enfin, conformément au droit commun, la protection donnée par le droit positif pourra être accordée à l'auteur de la base de données. La qualité d'auteur pouvant faire référence à une seule personne ou à une pluralité. En pratique, compte tenu du fait que les bases de données peuvent être réalisées à plusieurs, la base de données peut avoir le statut d'œuvre collective[567], cette potentielle cotitularité sur les droits d'auteur d'une base de données devra être pris en compte pour l'exploitation de tels droits portent sur une base de données *blockchain*.

§2 : L'exploitation routinière des droits d'auteur d'une base de données *blockchain*

284. Conformément à un droit commun déjà établi, les droits d'auteur sur une *blockchain* répondent à des impératifs et des problématiques classiques. C'est pourquoi le contenu de la protection tirée du droit des bases de données appliqué à la *blockchain* doit être analysé (A), en tant compte ensuite d'exceptions et de particularités (B).

A/ Contenu de la protection

285. La protection tirée du droit d'auteur est accordée à l'auteur d'une base de données originale. Également, le contenu de la protection, en l'absence de toute disposition particulière, est régi par le CPI[568]. La durée de protection restant sans particularité. Ainsi, le titulaire de la protection sur une base de données disposera du monopole conféré à l'auteur, comprenant notamment le droit exclusif de permettre ou de faire une reproduction de la base, ou encore

[566] Cf. *Supra*, p.23
[567] CA Paris, 27 juin 2002, RLDI 2012/85, n°2850
[568] Art. L121-1 et suivants.

permettre ou faire sa communication. S'agissant du point de départ de la protection, sera considéré la jour de la création de l'œuvre[569]. Outre les développements possibles en cas de cotitularité des droits et des conséquences pour les délais de protection (qui restent des applications classiques des durées de protection au regard du droit d'auteur), en reste que la date de création de l'œuvre pourra être considérée comme le jour de création du premier bloc d'une *blockchain* donnée. Néanmoins, des développements supplémentaires, dans le cadre de la notion d'achèvement d'une base de données, seront nécessaires. En effet, si la création d'une œuvre peut être résumé à un point temporel particulier (expression d'une « matérialité, une certaine forme d'expression[570] »), la notion d'achèvement d'une base de données, au titre du droit *sui generis*, qui reste un droit à vocation utilitaire, doit être plus nuancée.

286. Il conviendra de noter qu'il n'existe pas de régime de dévolution classique, tel que prévu par le droit des logiciels au profit de l'employeur. La pratique conduisant, le plus souvent, à la constitution d'une base de données réalisée à plusieurs, il conviendra d'appliquer les solutions portant sur le statut d'œuvre collective ou de collaboration[571].

Toutefois, appliqué à la *blockchain*, la cotitularité des droits exclusifs peut emporter quelques difficultés, qui se retrouveront, d'ailleurs, pour le droit des bases de données[572]. Aucune difficulté ne saurait être trouvée pour une *blockchain* réalisée par un seul auteur (ou entreprise pour faire application du régime de l'œuvre collective, par exemple). Néanmoins, la complexité d'une *blockchain* et l'absence de dévolution automatique au profit de l'employeur nécessite dès lors une contractualisation précise des différents droits sur une *blockchain* réalisée par des salariés (si tant est, bien entendu, qu'elle soit originale). Également, dans le cadre d'une *blockchain* sous licence libre, cette licence devra également porter sur la base de données en tant que telle afin de purger toute problématique inhérente à la gestion de ces droits. Dans une mesure commune au logiciel, une contractualisation des droits d'auteur s'en retrouve renforcée par l'utilisation de la *blockchain*.

[569] Art. L111-1, CPI : « L'auteur d'un œuvre de l'esprit jouit sur cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous ».

[570] GRYNBAUM L., LE GOFFIC C., MORLET-HAÏDARA L., précité, §377 et suiv.

[571] GRYNBAUM L., LE GOFFIC C., MORLET-HAÏDARA L., précité ; CA Paris, 27 juin 2012, RLDI 2012/85, n°2850, obs. COSTES L.

[572] Cf. *Supra*, Chapitre 2, p.137 et suiv.

287. Également, l'ensemble des développements sur le droit de distribution d'une base de données peut mériter d'autres particularités. Si la notion de public[573] reste importante pour l'appréciation de la théorie de l'épuisement du droit de distribution, les spécificités inhérentes à cette théorie restent applicables à la *blockchain*. Toutefois, dans une particularité propre à la *blockchain*, il apparaît, à notre sens, que la notion de public exclut l'ensemble des participants à la *blockchain*, tant leur qualité de participant est fonction technique indispensable à l'intégrité d'une *blockchain*.

B/ Exceptions et particularités

288. Les exceptions classiques au droit d'auteur sur une base de données trouveront application[574]. Une triple particularité trouvera également application pour les bases de données[575], qui restent des exceptions communes au logiciel.

Néanmoins, des limites ressortant du droit de la concurrence doivent également être mentionnées. Ressortant d'un arrêt de la Cour de cassation[576], le droit d'auteur (mais aussi le droit *sui generis*) sur une base de données ne saurait faire obstacle lorsque cette dernière « constitue une ressource essentielle pour des opérateurs exerçant une activité concurrentielle ».

289. Pour conclure, le droit d'auteur peut s'appliquer à la *blockchain*, et ce, de manière logique, tant la *blockchain* n'est pas caractérisée comme une exception particulière aux yeux de la propriété intellectuelle. Une nouvelle fois, la *blockchain* restant un outil - quoique particulier - l'ensemble des développements propres au droit d'auteur tendra à s'appliquer. Néanmoins, force est de constater certaines difficultés, en particulier pour une démonstration du caractère original de la base de données. La pratique démontrant également ces difficultés, elle tend surtout à la recherche de la protection par le droit dit « *sui generis* ».

---

[573] Sur ce sujet, voir notamment : RANÇON E., *Nouvelle précision sur le champ du droit de communication au public*, CJUE, 2avr. 2020, aff. C-753/18, Revue Lamy Droit de l'Immatériel, n°171, 1er juin 2020

[574] Art. L122-5 CPI

[575] Art. L122-5, 2°, CPI ; est fait référence ici à l'exception pour copie privée, l'exception de copie technique, et l'impossibilité d'interdire les « actes nécessaires à l'accès au contenu d'une base de données électronique pour les besoins et dans les limites de l'utilisation prévue par contrat ».

[576] Cass. Com. 4 déc. 2001, n°99-16.642, arrêt France Telecom, voir notamment comm. IDOT L., *Information et droit de la concurrence,* Revue Lamy droit des affaires, n°60, 1er mai 2003.

Section 2 : Reconquêtes du régime *sui generis* au bénéfice de la *blockchain*

290. Les développements autour de la protection au titre du droit d'auteur sur les bases de données doivent donc être doublés par une applicabilité du droit dit « *sui generis* » sur les bases de données. La directive de 1996, sur les bases de données, en ses considérants 38 et 39[577], visait déjà l'importance de la protection du contenu d'une base de données, et la protection nécessaire contre la reprise des contenus que le producteur aurait pu produire. Et comme le mentionne l'article L341-1 du Code de la propriété intellectuelle, les protections conférées par le droit d'auteur et le droit *sui generis* sont indépendantes et cumulatives, sans préjudice l'une de l'autre[578]. Néanmoins, compte tenu des attributs techniques d'une blockchain, la notion de producteur d'une base de données *blockchain* demeure particulier du fait de la potentielle distribution des données à un ensemble de participants au réseau (§1). C'est, en définitive, cet ensemble de participants qui participent à l'exploitation d'une *blockchain*, et c'est pourquoi cela confère un caractère étonnant à l'exploitation d'une telle base de données. Enfin, une approche plus fonctionnelle, prenant compte de la nature des données gérées par une *blockchain* doit être appréhendée (§3).

§1 : Le producteur particulier d'une base de données *blockchain*

291. La notion de gestion des droits est plus intéressante quand elle touche à la protection *sui generis*. Dans le cadre du droit *sui generis*, le producteur d'une base de données, pour être protégé au titre du droit *sui generis*, doit démontrer trois éléments : l'investissement substantiel, l'initiative de la conception de la base de données, et le risque assumé[579]. La lecture du texte semble viser une seule et unique personne.

292. La notion d'investissement regroupe une diversité d'objets dans leur réalisation (humain, financier, matériel). Le terme « initiative » parle de lui-même, mais s'agissant de la

[577] Directive 96/9/CE du Parlement européen et du Conseil du 11 mars 1996 concernant la protection juridique des bases de données, JOCE 27 mars 1996, n° L 77, p.20

[578] Art. L341-1, CPI, précité

[579] SIRINELLI P., *Le Lamy Droit des médias et de la communication*, précité

condition du « risque », il est plus difficile de la cerner. La lecture de la jurisprudence peut nous aiguiller, et on peut alors comprendre que le risque doit être compris comme le fait de supporter le poids principal de l'investissement (au sens financier) ou le fait d'avoir à répondre des dommages que l'utilisation de la base pourrait occasionner[580]. En d'autres termes, la notion de risque renvoi à la détermination de la personne responsable en cas de problème sur la base de données ou la personne qui subira les pertes financières dues à son exploitation. Pour rappel, cette notion d'investissement regroupe les investissements aussi bien financiers, matériels ou humains[581]. À ce titre, la jurisprudence européenne a également précisé que l'investissement pour la création des données (vouées à être dans la base) ne permet pas, à lui seul, de faire bénéficier la protection *sui generis* à son titulaire[582]. Enfin, le coût de la vérification des données, et celui de leur maintien dans la base peut également être admis dans le calcul des investissements qui serviront de base à la démonstration de l'effectivité de la protection *sui generis* d'une base de données[583].

293. Et en pratique, cette personne sera souvent une entreprise, qui financera et assumera les risques de la mise en place d'une base de données. Le titulaire de la protection *sui generis* sur une base de données appartiendrait donc toujours à une seule personne, comme l'avance le professeur Gaudrat[584]. Ainsi, même cette partie de la doctrine peut l'exclure[585], cette hypothèse de la présence de co-titulaires, en ce que plusieurs personnes ont réalisé des investissements substantiels, peut être remise au goût du jour concernant la *blockchain*. Toutefois, une thèse contraire est mise en avant dans la doctrine[586], thèse qui n'exclut pas l'hypothèse de la pluralité de producteurs d'une seule même base de données. Il est vrai que la jurisprudence n'aborde jamais directement la question de savoir si une pluralité de producteurs sur une même base de données est possible, la question principale étant souvent

[580] CA Paris, 20 fév. 2004, jurisdata n°2004-235866, LUCAS A., *Jurisclaseur Propriété littéraire et artistique*, Fasc. 1650

[581] On pourra citer, à titre d'exemple, l'arrêt de la chambre d'appel de Paris (CA Paris, 2 fév. 2021, n° 17/17688) rappelant l'importance de la démonstration des investissements comme fondamental pour la protection *sui generis*.

[582] CJCE, 9 nov. 2004, arrêt Opap, n°C-444/02. Sachant que si l'activité de création des données est mixte, c'est à dire couplé, notamment, avec une activité de compilation, alors l'activité de création des données peut être comptée comme part d'investissement substantiel, nécessaire à la protection *sui generis* ; CJCE, 9 nov. 2004, arrêtt BHB c. William Hill, C-203/02

[583] Cass., 1ère Civ., 13 mai 2014, arrêt Xooloo/Optenet

[584] GAUDRAT P., SARDAIN F., *Traité de droit civil du numérique - Tome 1 - Les biens*, éditions Larcier, 2015

[585] GAUDRAT P., *Droit des nouvelles technologies*, RTD Com. 1999, p. 104

[586] SIRINELLI P., Le *Lamy Droit des médias et de la communication*, précité - §136-57

de savoir si oui ou non les investissements présentés permettent le bénéfice de la protection *sui generis*.

Toutefois, un exemple jurisprudentiel semble aborder la question. Un arrêt de la Cour d'appel d'Aix-en-Provence [587] met en avant une société et une personne physique, qui réclamaient la cotitularité des droits, afin qu'ils soient tous deux considérés comme étant producteurs d'une même base. Les prétentions des parties mettant ceci en avant, la Cour d'appel reprend leurs prétentions dans leur rédaction, n'excluant pas cette possible cotitularité. Même si en définitive, la question sera tranchée autrement par la Cour d'appel en refusant la protection pour défaut d'investissements substantiels, et non pas en précisant que la cotitularité est impossible.

Sachant également que les quatre arrêts de novembre 2004 de la Cour européenne[588] mettent en exergue que la protection *sui generis* a pour vocation « d'encourager le développement de systèmes assumant une fonction de ''stockage'' et de ''traitement de l'information'' » ; à noter que si la Cour utilise le terme de « fabriquant », et non de « producteur », c'est parce que le terme de producteur a été utilisé en droit français pour faire écho aux notions de producteurs de phonogrammes notamment, sans exclure cette possibilité. Cette porte ouverte à cette cotitularité n'a pas été franchie à nouveau depuis l'arrêt de Cour d'appel précité, mais cette possibilité est intéressante surtout dans le cadre de cette étude. En effet, dans le cadre d'une *blockchain*, chacun des nœuds participants a vocation à créer, ordonner, à avoir accès et vérifier des données. Dès lors, chaque nœud assume une part du risque tel que présenté précédemment.

De plus, en cas d'échec dans la mise en place ou dans la gestion de la base, l'ensemble des participants assumera les pertes. En tant que part intégrante et nécessaire au réseau *blockchain* et donc à la base de données prévue, chaque nœud (et donc chaque propriétaire de ce dit nœud) peut donc revendiquer la qualité de producteur, sous preuve qu'il puisse rapporter la preuve desdits investissements. Régulièrement retenue par la jurisprudence française, la

[587] CA Aix en Provence, 28 mars 2012, n°10/21745
[588] Dont fait partie l'arrêtt Opap, précité

notion d'investissement substantiel peut également s'apprécier à la lumière de la jurisprudence, leur appréciation se faisant au biais de « moyens chiffrables […], des efforts non quantifiables, tels qu'un effort intellectuel ou une dépense d'énergie[589] ». Ainsi, étant donné que chaque nœud devra assumer une part des investissements, chaque nœud pourra prétendre à la qualité de producteur de base de données.

Par ailleurs, pour revenir au critère de l'initiative, seconde condition à l'attribution de la protection ; du fait que la *blockchain* est une architecture décentralisée, sa conception peut tout aussi bien revenir à une seule personne, ou à tout un groupe. Groupe qui aurait décidé de partager ses différentes ressources (matérielles, humaines, financières) pour la mise en place d'une *blockchain*, réflexions pouvant être reprises pour la notion de « risque » dans l'élaboration d'une base de données.

294. Ces trois critères considérés, et la possibilité d'avoir plusieurs personnes pouvant répondre à ces différents critères, il existe alors une possibilité dans la consécration d'une cotitularité des droits *sui generis* de protection, à l'instar d'une cotitularité des droits d'auteur. Outre la possibilité que ces investissements soient effectivement réalisés par une seule et même personne, les fonctionnalités d'une *blockchain* poussant à posséder plusieurs nœuds dans son réseau (plusieurs mineurs), l'ensemble des participants participent à l'investissement sur la vérification des données (pour ne prendre que cette facette). En effet, chaque action de minage nécessite un investissement temporel et énergétique (et donc financier), chaque mineur acceptant alors une partie des risques liés à l'exploitation d'une *blockchain*. Et concernant le critère relatif à l'initiative, l'ensemble des mineurs étant *a minima* identifié lors de la constitution de la *blockchain*, c'est bien leur participation mutuelle qui fonde l'initiative de la constitution d'une *blockchain*. Ainsi, dans le sens de la présente étude, la cotitularité de la protection au titre du droit *sui generis* ne doit pas être exclue, de surcroît, elle doit être envisagée.

En poussant plus loin la réflexion, il serait en effet intéressant d'accepter cette possible cotitularité de droits, la présence potentielle de plusieurs producteurs d'une même base de

[589] Une nouvelle fois, ce sont les 4 arrêts de novembre 2004 qui donnent ces précisions sur la nature des investissements substantiels nécessaires à l'octroi de la protection.

données. D'un point de vue du droit positif, aucune disposition n'apparaît comme prenant en compte cette possibilité, il apparaît donc une certaine carence, pouvant nécessiter la modification du Code de propriété intellectuelle, qui viserait non plus « le producteur »[590], mais « le ou les producteurs ». Comme expliqué dans les développements précédents, une simple mise à jour du Code de la propriété intellectuelle permettra de remédier à un risque juridique s'agissant de la titularité des droits sur une base de données. Permettre explicitement une cotitularité des droits sur une même base de données pourra permettre à plusieurs entités de gérer plus efficacement les droits exclusifs conférés par la loi sur une base de données et ne pas créer des situations d'incertitudes dans lesquelles les différents acteurs d'une *blockchain* ne sauraient pas à qui les droits exclusifs, accordées par le droit *sui generis*, appartiennent.

295. Le droit *sui generis*, tel que présenté à l'article L341-1 du Code de la propriété intellectuelle[591] est avant tout un droit d'investisseur, c'est-à-dire qu'il protège le titulaire de la base de données en ce qu'il a réalisé des investissements substantiels sur cette dernière. Il est important de souligner que la protection *sui generis* vise bien le contenu de la base, et non le contenant[592].

La notion d'investissement, notion mesurée de manière économique, a été précisée par la CJCE[593] : « les moyens tenant à la création de données ne sont pas comptabilisés », « seuls les investissements liés à l'obtention, la vérification et la présentation du contenu de la base doivent être pris en compte ». Toutefois, il en reste une difficile appréciation pratique, notamment pour des bases de données continuellement mises à jour et/utilisée, car il peut être délicat de distinguer les phases de lancements, de stockage et de maintenance des données

---

[590] Art. L341-1, CPI ; « Le producteur d'une base de données, entendu comme la personne qui prend l'initiative et le risque des investissements correspondants, bénéficie d'une protection du contenu de la base lorsque la constitution, la vérification ou la présentation de celui-ci atteste d'un investissement financier, matériel ou humain substantiel ».

[591] Art. L341-1, CPI : « Le producteur d'une base de données, entendu comme la personne qui prend l'initiative et le risque des investissements correspondants, bénéficie d'une protection du contenu de la base lorsque la constitution, la vérification ou la présentation de celui-ci atteste d'un investissement financier, matériel ou humain substantiel ».

Cette protection est indépendante et s'exerce sans préjudice de celles résultant du droit d'auteur ou d'un autre droit sur la base de données ou un de ses éléments constitutifs ».

[592] CA Paris 12 sept. 2001, jurisdata n°2001-155210, JCP E 2002, no 888, obs. VIVANT M., MALLET-POUJOL N. et BRUGIERE J.-M.

[593] CJCE, arrêts du 9 nov. 2004, C-46/02, C-203/02, C-444/02, voir notamment CCE 2005, comm. 2, CARON C.

d'une base. La Cour de cassation, dans un arrêt de 2009[594], a précisé que la notion d'investissement ne comprend pas « les moyens mis en œuvre pour la création des données », mais comprend les moyens consacrés en vue « d'assurer la faillibilité de l'information » y compris pendant son « fonctionnement ». Solution qui fut complétée par un arrêt de Cour d'appel, précisant que sont pris en compte les investissements liés au stockage et au traitement des éléments une fois ceux-ci réunis[595].

296. S'agissant du caractère « qualitatif » de l'investissement, apparaît l'usage du qualificatif substantiel. Notion une fois nouvelle floue, il existe une appréciation ayant tendance à être *in concreto*, pour exemple, des investissements de 35 000€ ont pu être retenus[596] ou encore une somme de plus de 850 000€[597], sachant qu'outre l'aspect purement financier, l'investissement peut être également qualitativement substantiel, notamment les efforts intellectuels ou la dépense d'énergie retenue[598]. Enfin, la notion d'investissement doit être rapprochée du risque encouru par l'investisseur, comme le précise la loi[599], pour la constitution de la base de données et permettre l'octroi de la protection par le droit *sui generis*. Notamment un arrêt de la Cour d'appel de Paris retient également la pertinence du risque encouru par l'investisseur pour lui octroyer ou non cette protection[600].

Pour un aspect rattaché à la pratique pour la mise en œuvre du droit *sui generis*, le producteur devra donc se préserver des preuves relatives à l'importance et à la nature des investissements réalisés (pour les investissements financiers, humains ou encore matériels), tout en justifiant que ces investissements portent bien que la vérification, ou encore l'obtention des différentes données de la base, et non leur création.

---

[594] Cass. 1ère Civ, 5 mars 2009, n°07-19.735, publié

[595] CA Paris, pôle 5, ch. 2, 20 déc. 2013, n°12/20260, sté Protagoras, voir com. *La qualification du producteur de données non retenue*, Revue Lamy Droit de l'Immatériel, n°101, 1er fév. 2014

[596] CJCE, 9 oct. 2008, C-304/07, RLDI 2009/43, n°1411, obs. COSTES L.

[597] TGI Paris, 5 sep. 2001, arrêt Keljob, voir com. Legalis Actualité, 21/09/2001, disponible à https://www.legalis.net/actualite/keljob-condamne-a-un-million-de-francs-de-dommages-interets/

[598] CJCE, arrêts du 9 nov. 2004, précités

[599] Art. L341-1, CPI

[600] TGI Paris, 20 juin 2007, arrêt PMU

297. Ces critères rappelés, nous pouvons ainsi déterminer une application positive de la protection *sui generis* des bases de données sur un réseau *blockchain*. En effet, il existera, au moment de sa conception, des investissements humains, matériels et financiers sur la conception de la base (d'autant plus qu'à l'heure actuelle il n'existe que peu de spécialistes *blockchain*s, augmentant drastiquement le coût « homme »), sur la mise en place du réseau, le maintien des données et leur continuel renouvellement. Mais seront donc récompensées la ou les personnes ayant pris « l'initiative et le risque »[601] des investissements inhérents à une *blockchain*. Cette triple condition, sur l'investissement, l'initiative et le risque, est importante, et servira à la détermination du titulaire de la protection.

Toutefois, une attention particulière devra être apportée sur une distinction nécessaire entre les dépenses réalisées pour la création des données et celles réalisées pour leur vérification ou encore leur accès. En effet, l'association du logiciel *blockchain*, permettant de définir les modalités de création et de vérification des données, et de la base de données, consistant à la fois en une activité de création et de vérification des données, se devra d'être particulièrement claire. Si les dépenses, seules, sur la création des données, ne sauraient être utiles pour l'octroi de la protection du titre du droit *sui generis*, elles resteront, en pratique, souvent mêlées aux dépenses relatives à la vérification des données[602]. Une ventilation, en particulier comptable, sera nécessaire ; cette dernière devant être rigoureuse pour pouvoir emporter conviction des juges en cas de litige[603].

298. En pratique, la détermination de la titularité de ces droits est essentielle à une gestion efficace d'une base de données, toutefois, la *blockchain*, dans sa logique première, est fondé sur une logique *open source*. En effet, le cas du *Bitcoin* montre que la technologie *blockchain* repose sur des logiciels et une logique *open source*, et donc un modèle ouvert. D'autant plus que la technologie *blockchain* a pour vocation une décentralisation du pouvoir décisionnel. En conséquence, attribuer la titularité des droits à une ou plusieurs personnes pourrait aller à l'encontre de la philosophie « *blockchain* ». Dès lors, la titularité des droits sera à considérer

[601] Art. L341-1, CPI, précité

[602] En pratique, chaque nouveau bloc d'une *blockchain* comporte plusieurs fonctions, notamment celle de vérifier les données plus anciennes, pour pouvoir, par résolution d'un problème cryptographique, créer de nouvelles données.

[603] Pour des développements au sujet des expertises dans le coût et leur ventilation au bénéfice du droit *sui generis* : CA Paris, pôle 5, ch. 1, 27 oct. 2015, n°14/14239

en fonction des licences choisies par ses participants mais aussi en fonction du type de *blockchain* mis en place (public, privé, hybride). Mais ce point ne peut être écarté pour, par exemple, d'une *blockchain* à but purement financier.

Le consortium R3[604] dont les travaux, à terme, sont de concevoir une *blockchain* pour le transfert d'actifs, et dans un tel cas, la titularité des droits sur la base de données sera une problématique évidente, dans le sens où le titulaire bénéficiera des prérogatives associées, notamment l'accès exclusif aux données présentes dans la base. Il est évident de voir l'intérêt que chaque participant aurait à pouvoir accéder et réutiliser les différentes données issues d'une telle *blockchain*[605].

§2 : L'exploitation étonnante d'une *blockchain*

299. La protection *sui generis* sur les bases de données a une vocation utilitaire et financière. Le producteur, personne(s) ayant investi dans la production d'une base de données doit pouvoir posséder des retours sur investissements pour la création de sa base. Il doit pouvoir également se prémunir contre les utilisations et/ou extractions qui viendraient vider sa création.

Le CPI précise que le producteur d'une base de données, en cas de protection au titre du droit *sui generis*, l'extraction et la réutilisation d'une part substantielle, qualitativement ou quantitativement des données contenues dans la base[606]. Étant précisé que l'accès direct à la base de données n'est pas nécessaire[607], et que la réutilisation peut être indirecte, en utilisant

[604] https://r3cev.com/ ; le consortium R3, créé en 2014, est une réunion de plusieurs acteurs important du monde financier, dont la fonction est d'étudier l'impact de la technologie *blockchain* au sein de la finance. Récemment, c'est la banque BNP Paribas qui a pu le rejoindre, plus d'informations : https://fr.wikipedia.org/wiki/R3_(entreprise)

[605] PERREAU C., *R3, le consortium blockchain qui divise les banques*, Journal du Net, 18 juil. 2017, disponible à : https://www.journaldunet.com/economie/finance/1196309-r3-le-consortium-*blockchain*-qui-divise-les-banques/, consulté le 20/09/2019, Cela étant, à l'heure actuelle, le consortium R3 se vide petit à petit de sa substance ; les aboutissants relatifs à la propriété intellectuelle ne sauraient être exclus des raisons pour lesquelles certains de ces membres ont pu le quitter.

[606] Art. L342-1, CPI

[607] À propos des arrêts du 9 nov. 2004, précités, VIVANT M. et BRUGUIERE J.-M., *Droit d'auteur*, Précis, Dalloz, 2009, 1re éd.

une seconde base de données[608] ces actions nécessitant une reprise intellectuelle et une appropriation des données[609].

Également, a pu être retenu que la réutilisation d'une base de données accessible en ligne peut constituer une atteinte aux droits du producteur, et ce, dès qu'une partie a été reproduite et extraite et l'identique, dans le cadre d'un « usage anormal[610] ». Corollaire logique du droit du producteur d'une base de données, qui reste un droit d'investisseur, protéger le producteur semble logique dans un tel cas, néanmoins, en reste que l'usage anormal doit découler une nouvelle fois d'une appréciation *in concreto*. En effet, dans les faits de l'espèce précédente, il s'agissait de condamner l'extraction d'environ 60% d'une base de données, et si les juges n'ont pas précisé les notions de quantité ou de qualité substantielle, en reste que c'est l'usage anormal qui a été retenu de cette réutilisation (même si, en pratique, 60% d'une base de données peut être considéré comme quantitativement important).

300. Or, si un tel usage peut être qualité d'anormal, le cas d'une base de données *blockchain*, dont l'une des caractéristiques intrinsèques est de répliquer 100% du contenu auprès de l'ensemble des participants au réseau, l'usage anormal ne saurait être retenu. En effet, l'usage anormal pouvant découler d'un usage, d'une part, non pris en compte par le producteur, et d'autre part, contraire aux droits qu'il peut avoir sur sa base de données. Or, cet usage en totalité est lié par nature à la *blockchain*. La réplication de données étant même nécessaire à la pérennité d'un tel réseau. En conséquence, il est possible de voir une nouvelle fois un certain affaiblissement du droit des bases de données en raison de la pratique technologique. Et si un producteur de base de données *blockchain*, publié en ligne, souhaite se protéger contre la réutilisation de ses données, alors il devra prendre en compte la nécessaire réutilisation de ses données par ses utilisateurs.

301. Néanmoins, concernant la durée de protection, une problématique importante applicable à la *blockchain* doit être étudiée. Au demeurant, celle-ci demeure beaucoup plus courte que la durée conférée par le droit d'auteur : quinze ans à partir de l'achèvement ou de la fabrication de la base de données, renouvelable à chaque investissement substantiel[611].

---

[608] CJCE, 9 oct. 2008, C-304/07

[609] CASTETS- RENARD C., *La protection des producteurs de bases de données contre l'extraction des données par un logiciel*, Revue Lamy Droit de l'Immatériel, n°56, 1er janv. 2010

[610] TGI Paris, ch. 3, sect. 3, 6 déc. 2013, arrêt Auto Look Perfect, voir com. Revue Lamy Droit de l'Immatériel, n°103, 1er avril 2014

[611] Art. L342-5, CPI, al. 3ème

Expliqué par la volonté de protection de l'investisseur, le droit *sui generis*, cette durée, plus courte, a l'avantage, d'une part, de prendre en considération la vacation utilitaire d'une base de données, et a, d'autre part, l'intérêt de fournir, au moins théoriquement, une protection à durée illimitée.

Également, on peut remarquer que le CPI conditionne la protection *sui generis* à la réalisation de l'investissement pour « la constitution, la vérification ou la présentation[612] », et qu'il fait débuter cette protection à partir de « l'achèvement[613] » de la base de données, ou de sa « mise à disposition du public ». Le texte de la directive de 1996 précise que la « charge de la preuve de la date d'achèvement de la fabrication d'une base de données pèse sur le fabriquant de celle-ci ». Or, si la démonstration de l'existence d'une base de données classique est déjà qualifiée d'ardu[614], comment l'appliquer à une *blockchain* ? Comment estimer l'achèvement d'une *blockchain* ? Comment apprécier l'achèvement d'une base de données qui a vocation à continuellement s'enrichir de nouvelles entrées et qui ne possèdent de valeur (du moins économique ou technique) qu'une fois un volume - non identifié - de données y sont compilées ? Est-ce que la mise à disposition au public d'une base de données vide, invitant ce dernier à l'alimenter mérite protection au titre du droit *sui generis* ?

302. Cette réflexion porte tout à fait sens dans un environnement où la compilation, l'enrichissement et les futures exploitations de données deviennent d'autant plus importants que la constitution simple d'une base de données, à savoir la création d'un « moule » de données, dans lequel viendraient se déverser un nombre fini de données. Outre l'opportunité d'une telle question pour toute base de données ayant vocation à s'enrichir continuellement, et dont la portée financière n'en serait que plus grande au fur et à mesure de son exploitation, l'actuel droit des bases de données ne semble donc viser que la constitution ou la vérification de données, sous-entendant que les investissements portent en premier lieu sur un volume de données préexistant. La pratique et la quasi-majorité des cas jurisprudentiels ne portent que sur des bases de données déjà constituées, mais dans le cadre d'une *blockchain*, à quelle moment la base est-elle constituée ?

[612] Art. L341-1, CPI
[613] Art. L342-5, CPI, al. 1er
[614] GRYNBAUM L., LE GOFFIC C., MORLET-HAÏDARA L., précité

La jurisprudence est particulièrement pauvre sur la notion d'achèvement d'une base de données. Il est vrai qu'en pratique, les litiges naissent pour donner suite à une réutilisation non autorisée par le producteur, et les faits des différentes espèces font références à des bases de données en cours d'utilisation. Néanmoins, la notion de réutilisation des données peut permettre de saisir cette notion d'achèvement, au-delà d'une définition purement sémantique, renvoyant non forcément à un moment purement temporel, mais à un état[615], démontrant la fin de travaux ou d'un ouvrage.

Un arrêt de la CJUE indique notamment que « la notion de partie substantielle (…) se réfère au volume de données (…) et doit être apprécié(e) par rapport au volume du contenu total de celle-ci[616] ». Une référence et un critère de proportionnalité quant au volume de la base de données doit donc être pris en compte, mais sans pour autant identifier le moment à partir duquel, techniquement, la base est achevée. Un arrêt de la Cour d'appel de Paris, s'agissant de la mise à jour des données, a pu retenir que la simple mise à jour annuelle de données ne suffit pas à caractériser « l'existence d'un nouvel investissement substantiel[617] » ; ce même arrêt renvoyant également aux « documents comptables de nature à démontrer la part réservée dans ses comptes à la constitution, la vérification ou la présentation du contenu de la base de données », excluant ainsi une simple mise à jour des données et insistant sur la production de pièces comptables pour attester d'un investissement substantiel et son renouveau dans le but d'obtenir une protection et un renouvellement de cette protection au titre du droit *sui generis*. D'ailleurs, sur la notion de nouvel investissement substantiel, la CJUE a pu retenir la notion « modification substantielle résultant de l'accumulation d'ajouts, de suppressions ou de changements successifs qui ferait considérer qu'il s'agit d'un nouvel investissement substantiel, évalué de façon qualitative ou quantitative[618] », invitant une nouvelle fois à établir un jalon temporel pour l'appréciation de ce nouvel investissement.

Également, le droit de la concurrence et des obligations, en ce qu'ils portent sur la concurrence déloyale et le parasitisme peuvent nous indiquer des clés de lecture quant à la réutilisation d'une base de données protégées, comme le fait de profiter d'un enrichissement

[615] Le Robert. (s.d.). Achèvement. dans LeRobert *en ligne*, https://dictionnaire.lerobert.com/definition/achevement (consulté le 15/05/2021)

[616] CJUE, 1er mars 2012, aff. C-604/10, précité

[617] CA Paris, 4e ch., Sec. A, 28 fév. 2007, n°06/01801

[618] CJUE, affaire C-203/02, précitée

réalisé dans le sillage d'un concurrent[619], invitant à une approche très économique de la réutilisation de la base de données concernées.

Enfin, rappelons que le droit d'auteur, dans sa dimension applicable aux bases de données, fait référence à la création de l'œuvre, à savoir le moment où une matérialité de l'œuvre est présente et est plus appréciable qu'une simple idée.

303. Dès lors, et en l'absence de réponse précise quant à la détermination de l'achèvement d'une base de données, aussi bien quantitativement que qualitativement, il pourra être opportun d'avoir une approche plus économiste que juridique. Si le droit d'auteur considère la création, l'expression faisant sortir l'œuvre du domaine des idées, rappelons qu'une *blockchain* a pour intérêt d'être une base de données évolutive, créée pour être en constante évolution, et ce, dès le premier bloc miné. Également, ce premier bloc permet les actions de constitution et de vérification constante (opérations qui seront réalisées par les différents nœuds du réseau). Enfin, une *blockchain* présentera un intérêt économique dès le premier bloc miné, attestant de son bon fonctionnement et, potentiellement, de sa future efficacité.

304. En conséquence, s'il est possible de concevoir une approche non pas temporelle mais fonctionnelle de l'achèvement d'une *blockchain* (et donc d'une base de données), son achèvement pourrait être considéré comme concomitant à la création et à la distribution du premier bloc miné au sein de la communauté des participants au réseau. Ainsi, il conviendra, notamment pour la détermination des investissements substantiels requis pour l'octroi d'une protection au titre du droit *sui generis*, de réaliser une démonstration aussi bien comptable que technique de ces investissements jusqu'au moment du minage du premier bloc. Une telle hypothèse reprenant ainsi la solution donnée par le droit d'auteur, qui reste intimement liée au droit *sui generis*, ne serait-ce que par son objet.

Aussi, pour la prise en compte du renouvellement de la protection au titre du droit *sui generis*, l'architecture d'une *blockchain* peut attester d'évolutions majeures, avec des *forks*. Ces dernières pourront servir de jalons probatoires à la réalisation de nouveaux investissement substantiels, compte tenu du rejet de la simple mise à jour d'une base de données. Effectivement, une *blockchain* étant en perpétuelle évolution, la solution de considérer chaque

[619] CA Versailles, 11 avr. 2002 : LPA 2003, n° 105, p. 11, obs. DAVERAT X.

fork (et plus particulièrement les *hard forks*) comme jalon temporel à un nouvel investissement substantiel, tant ces *forks* conduisent à un renouveau d'une *blockchain*.

305. Compte tenu des évolutions technologiques informatiques, le droit *sui generis* des bases de données présente alors une lacune, qui réside dans la définition du point de départ de la protection. Si ce point de départ ne saurait poser de réelles difficultés pour le droit d'auteur[620], le point de départ de la protection d'une base de données ayant vocation à évoluer constamment au-delà de la simple mise à jour, et pouvant être considérée comme un actif important d'une entreprise présente donc une fragilité. Par exemple, les bases de données massives, actif important des acteurs de l'Intelligence artificielle, peuvent être protégées, logiquement, par le droit des bases de données. Mais en cas de litige sur la protection de telles bases, comment déterminer, si ce n'est que par une vision économique, la durée de sa protection ? Sachant également qu'une telle base ne présente que plus de valeur plus sa pérennité et son exploitation sont continues dans le temps. En ressort que l'expression « d'achèvement » pourrait être modifiée, au bénéfice d'une expression de « première utilisation », la rapprochant ainsi de la conception de création tirée du droit d'auteur, mais conservant le caractère utilitariste du droit *sui generis* des bases de données.

§3 : Limites fonctionnelles de la protection d'une *blockchain*

306. Si l'applicabilité du droit des bases de données ne semble guère faire de doute pour ce qui concerne la *blockchain*, certaines limites tendant à la réutilisation, l'extraction et l'utilisation de la *blockchain* pour des données publiques sont à noter.

307. Les exceptions tirées du régime de la protection *sui generis*, outre leur applicabilité certaine à la *blockchain* présente néanmoins des difficultés pratiques, liées à la nature même d'une *blockchain*. Le droit d'interdire la réutilisation d'une base de données paraît clairement affaibli dans le cadre d'un tel protocole. En effet, et pour des raisons parallèles à celles rencontrées dans le logiciel[621], une *blockchain* voit sa sécurité et sa fiabilité reposer sur la multiplicité des acteurs y participant. La pratique contractuelle dans le cadre d'une *blockchain*

[620] Pour rappel, les droits patrimoniaux découlant du droit d'auteur ont une durée de 70 ans à partir de la mort de l'auteur et les droits moraux sont perpétuels ; ces deux types de droit existant dès la création d'une œuvre.

[621] Cf. *Supra*, p.127 et suiv.

née de l'initiative de personnes privées et construite dans une logique classique de valorisation d'actif immatériel sera d'autant plus importante pour éviter tout conflit dans l'utilisation d'une telle base. Et s'agissant d'une *blockchain* soumise au régime du logiciel libre, la licence sélectionnée devra elle aussi, comprendre l'ensemble des droits et exceptions tirées du droit *sui generis*.

308. Sur la notion d'extraction substantielle et l'*open data*, appliqués à la *blockchain*. Il ressort que la *blockchain* a le potentiel de gérer et d'organiser des volumes importants de données, pour lesquels il peut se trouver des intérêts pour un *data mining*[622] opportun. En effet, on peut, compte tenu du développement des initiatives des acteurs bancaires dans le monde de la *blockchain*[623] imaginer une analyse des différents flux financiers se basant sur les différentes données issues d'une *blockchain*. En ce sens, les États membres ont l'obligation d'instaurer des exceptions ou des limitations pour les extractions d'œuvres et d'autres objets protégés accessibles de manière licite « aux fins de la fouille de textes et de données[624] ». Également, doit être rappelé ici les développements sur l'accessibilité d'une base de données qui serait être une « ressource essentielle[625] ».

309. S'agissant de l'utilisation de données publiques, contenues dans une base de données protégée par le droit *sui generis*, le Conseil d'état a pu estimer que la réutilisation de données publiques ne peut être empêchée par cette protection[626]. En conséquence, si l'utilisation de la *blockchain* peut être encouragée pour l'organisation et la gestion de données publiques, cette dernière ne saura être un moyen détourné de limiter l'utilisation - y compris dans la mise en œuvre de licences d'utilisation - de données publiques. En reste que compte tenu des investissements actuels nécessaires à la mise en place d'une *blockchain*, la gestion des droits de propriété intellectuelle ne saurait être un moyen lucratif pour compenser les dépenses

[622] BRUGUIERE J-M., FAUCHOUX V., QUIQUEREZ A., *Actualité du droit des technologies nouvelles*, Revue Lamy Droit civil, n°184, 1er sep. 2020

[623] WARDZALA C., Deskoin signe un accord avec la Caisse d'Epargne Grand Est, Cryptoast, 14 sept. 2021, disponible à : https://cryptoast.fr/deskoin-partenariat-caisse-epargne-achat-cryptomonnaies-france/, consulté le 18/09/2021

[624] BINCTIN N., *TDM : un enjeu de l'intelligence artificielle*, RIDA 2019, nº 262, p. 5., sur la directive (UE) 2019/790 du Parlement européen et du conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE

[625] CJCE 29 avr. 2004, IMS Health, aff. C-418/01, D. 2004. 2366, note SARDIN

[626] CE 10ème - 9ème ch. réunies, 8 fév. 2017, nº 389806 arrêt « Notrefamille. com / Département de la Vienne »

réalisées ; d'autres moyens devront être envisagés, notamment la mise en place d'une redevance[627].

[627] Sur ce point : https://guides.etalab.gouv.fr/juridique/reutilisation/#les-restrictions-a-la-reutilisation-des-donnees

Conclusion du Chapitre 2

310. Au-delà des débats actuels sur la nécessité ou non du remodelage du droit des bases de données[628], ce dernier peut s'appliquer à une *blockchain*. Outre les spécificités liées à la titularité et l'exploitation des différents droits accordés à l'auteur et/ou au producteur de données, une *blockchain* reste alors un objet juridique identifié. Si la production tirée du droit d'auteur paraît plus fragile en raison de la nature d'une *blockchain* en tant que protocole informatique, les prérogatives du producteur sont plus intéressantes, quoique liées à de difficiles justifications comptables au sujet des investissements substantiels. Néanmoins, il ne faut pas perdre de vue qu'une *blockchain* ne reste, une nouvelle fois, qu'un outil, au service de projets, qui eux pourront faire l'objet de contractualisation et/ou de régulation. En conséquence de quoi, la nature de la *blockchain* déjà comme outil et non pas comme objet seul de droit ne doit pas être omise.

311. Le droit *sui generis* relatif à la protection des bases de données peut présenter des lacunes face à la pratique technologique relative à la *blockchain*. De manière native, si ce droit permet au producteur d'être « récompensé » pour ses investissements, l'utilisation d'une *blockchain* entraîne *de facto* un affaiblissement de ses droits. Une *blockchain* prévoyant techniquement la réutilisation et la réplication entière de ses données, le droit d'interdire la réutilisation d'une base de données paraît clairement affaibli. En conséquence, le producteur devra être attentif à plusieurs pans : la délimitation des rôles, afin d'identifier clairement la qualité de participant au réseau *blockchain* (qui elle conférera la possibilité, notamment, de réutilisation et de réplication des données contenues dans la *blockchain*), et la délimitation des autorisations conférées aux utilisateurs d'une telle *blockchain* (qui pourront faire l'objet de contractualisation spécifiques).

312. Il reste l'hypothèse de l'utilisation de licences libres pour l'exploitation de *blockchain*, notamment dans le cadre d'une diffusion en ligne d'un tel réseau et des données y afférents. De manière similaire aux problématiques rencontrées dans l'application du droit des logiciels, si on comprend la tendance à l'abandon et la contractualisation des droits de propriété

[628] Voir par exemple : http://laminutedroit.com/protection-juridique-bases-donnees/ ou encore BENSAMOUN A., GABLA E., LEFORESTIER G., *Note d'étape, Mission Bases de données*, CSPLA, avril 2021, disponible à https://www.culture.gouv.fr/Sites-thematiques/Propriete-litteraire-et-artistique/Conseil-superieur-de-la-propriete-litteraire-et-artistique/Travaux/Missions/Mission-du-CSPLA-sur-la-protection-juridique-des-bases-de-donnees (consulté le 18/05/2021)

intellectuelle rattachés à une *blockchain*, il reste que l'ensemble des hypothèses rattachées à ces droits devraient faire l'objet d'une mention claire au moment du partage des données *blockchain*.

313. Enfin, la protection d'une base de données procède d'une dualité de protection[629], même si ces protections restent bien indépendantes d'autres, telles que la protection au titre du droit des logiciels. En effet, doivent être simplement rappelées les oppositions ou rapprochements potentiels entre base de données et logiciel[630]. Au-delà, si le texte du CPI découle de la directive de 1996[631], en reste des difficultés pratiques, notamment liées aux natures mouvantes des bases de données et de leurs utilisations. En résumé, doit une nouvelle fois être rappelée l'importance de la distinction entre contenu et contenant d'une base de données ; le premier étant protégé (pris dans son ensemble) contre les extractions ou encore les réutilisations, et donc par le droit *sui generis*, le second étant protégé par le droit d'auteur. Au-delà, tout protection tirée du droit des obligations, dans le cadre d'une gestion contractuelle efficace ne saurait être un obstacle pour toute protection d'une base de données non concernée par un régime de protection tiré du droit de la propriété intellectuelle[632].

[629] Cass. 1re Civ., 13 mai 2014, nº 12-27.691, précité

[630] « Pour résumer, deux choses sont sûres : 1) les dispositions relatives aux bases ne s'appliquent pas aux logiciels ; 2) les dispositions relatives aux logiciels ne s'appliquent pas aux bases, sauf pour les composantes programmes utilisées par une base pour son fonctionnement ou la consultation. Mais il n'y a alors aucune spécificité ». SIRINELLI P. *Le Lamy Droit des médias et de la communication*, précité.

[631] Directive 96/9/CE du 11 mars 1996, précitée

[632] CJUE, 15 janv. 2015, n°C-30/14, arrêt Ryanair, voir com. Revue Lamy Droit de l'immatériel, n°112, 1er fév. 2015

Conclusion du Titre 1

314. Une nouvelle fois, l'étude sémantique juridique d'un nouvel élément particulier, faisant suite à une compréhension globale et non isolée, apparaît comme étant une solution viable. En effet, la seule définition d'une *blockchain*, au-delà de la prise en compte des intérêts socio-économiques, informatiques, ou même politiques, ne doit pas être un obstacle à l'étude d'un tel objet. Le droit positif de la propriété intellectuelle, appliqué à la *blockchain* pris en tant qu'objet seul et non pas support d'une fonction autre paraît majoritairement suffisant. L'appréhension du contexte, la recherche et l'application ordonnée du droit applicable devant alors se résoudre de manière naturelle et ordonnée, sans chercher à faire appliquer ou créer un pan juridique à la seule motivation de l'application de l'objet visé. La *blockchain* demeure un outil, et si l'étude de l'outil est réalisée, alors le résultat doit être indifférent d'une telle étude.

315. Néanmoins, et en particulier pour la *blockchain*, une application sémantique du droit positif n'est pas exclusive d'une approche et d'une considération extensives de la *blockchain*. Dans une approche pouvant paraître comme paradoxale par rapport aux propos précédents, la *blockchain* demeure un accélérateur à la considération d'un droit de la donnée. En effet, protocole informatique particulier, mêlant architectures techniques et juridiques, la *blockchain* se retrouve au carrefour de considérations souvent étudiées indépendamment. Au-delà, la *blockchain*, dans une approche également pragmatique, soulève certains questionnements au sujet de la gestion de la donnée. Questionnements qui sont indispensables dans l'état actuel du droit positif relatif à la protection des données, personnelles ou non.

Titre 2 : Vers une appréciation fonctionnelle du droit de la donnée

« Le code est parmi nous pour toujours, et le droit n'est pas près de nous quitter. ».

Les Golems du Numérique, 2016, Mélanie Dulong De Rosnay

316. L'objet de la présente étude conduit à donc réaliser une application ordonnée du droit dans le cadre de l'utilisation d'un protocole *blockchain*. Les éléments primaires d'une *blockchain* étant un logiciel et une base de données décentralisée ont, comme analysé précédemment, un régime dédié et existant. Néanmoins, focaliser cette étude sur ces seuls éléments mettrait de côté le caractère intrinsèque d'une *blockchain*, à savoir la mise en place d'une architecture informatique aux caractéristiques particulières, au service de la gestion de données. Une distinction forte et nécessaire doit être faite entre données personnelles - « toute information se rapportant à une personne physique identifiée ou identifiable[633]» - et données non personnelles - « les données autres que les données à caractère personnel[634] ». Sachant que la « *data*, non rivale, circulante, co-construite appelle ainsi l'élaboration d'un droit de la donnée élargi au niveau européen[635] », il convient d'apprécier le droit de la donnée comme une matière de plus en plus autonome, ou, *a minima*, dans une approche plus extensive et fonctionnelle qu'elle ne l'est actuellement, c'est-à-dire une approche tenant compte de la technique de manière concomitante à la prise en compte des impératifs juridiques.

317. Avancer qu'il peut exister une appréciation fonctionnelle du droit de la donnée, compte tenu du caractère néo-juridique[636] d'un tel droit revient en réalité à participer à la construction d'une telle matière. Les prochains développements, au surplus d'étudier l'applicabilité de normes existantes (sur la gestion des données personnelles ou non dans le cadre d'une

[633] Règlement n°2016/679, précité, article 4

[634] Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 nov.2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, dit RGNP

[635] ZOLYNSKI C., *La place du règlement (UE) 2018/1807 dans la construction du droit des données de l'Union européenne*, Dalloz IP/IT 2020 p.429

[636] Néo-juridique dans le sens où, à notre connaissance aujourd'hui, le droit de la donnée ou droit des données n'existe pas de manière autonome compte tenu du caractère disparate des matières que ce droit peut irriguer.

blockchain), mettent en exergue la connexion permanente entre un droit que l'on pourrait considérer nommé (en reprenant l'opposition contrat « nommé/innommé[637] ») - comme le droit des logiciels ou des bases de données - avec ce que l'on pourrait appeler un droit innommé ou dérivé. Un droit conçu et réfléchi au service du premier, compte tenu du contexte et des objectifs. À cet effet, le droit des données (personnelles ou non) pourrait effectivement être considéré comme un droit innomé, car absent - aujourd'hui - des matières traditionnellement étudiées. Dans le même sens, une telle caractérisation d'un droit dit innomé trouve de nombreux échos dans d'autres matières pratiques. De manière parallèle, l'ensemble du « droit du multimédia » pourrait être considéré comme un droit innomé au regard d'autres droits nommés (de la même manière que le régime du contrat électronique peut l'être au regard du droit des contrats, etc.). C'est dans cette optique, légitimé par la nature même de la technologie *blockchain*, qu'il convient d'étudier, au sein de ce titre, les différents régimes applicables pour participer à la construction de ce droit innommé que pourrait être le « droit de la donnée »[638]. Dont une ramification pourrait même porter directement sur la technologie *blockchain*, comme certains auteurs tendent à le souligner[639].

318. Une approche du droit de la donnée peut être étudiée à travers deux grands pans : la protection et l'exploitation de la donnée. Si le second volet peut tenir à une simple étude de la pratique, que ce soit à travers l'utilisation de la donnée (contrat de transfert de données, exploitation des bases de données, etc.) ou à travers l'exploitation (*data mining*, exploitations algorithmiques), le premier volet parait aujourd'hui bien plus développé au regard du droit positif, et, par extension, à travers l'étude de la *blockchain*. À cet effet, cette technologie nous amène à la réflexion au bénéfice d'un dualisme de l'approche protectionniste de la donnée (Chapitre 1), compte tenu des interactions entre *blockchain* et données personnelles ou non personnelles. De surcroît, rappelant le caractère disruptif de la *blockchain*, le dépassement des frontières entre matières peut être envisagé, à un point où cette technologie permet de découvrir une complémentarité entre droit et technique (Chapitre 2).

---

[637] Pour rappel, le contrat nommé est un contrat qualifié et réglementé par la loi, et le contrat innommé est un contrat qui n'est pas réglementé par la loi.

[638] Qui, peut déjà être considéré comme tel si l'on considère l'existence d'ouvrages (par exemple : BOURGEOIS M., *Droit de la donnée*, LexisNexis, 2017) ou de fascicules dédiés (par exemple : « Numéro 21-22 JCP E Droit de la donnée »)

[639] O'RORKE W., *L'émergence d'un droit de la blockchain*, Dalloz IP/IT 2019. p.422

Chapitre 1 : Dualisme d'une approche protectionniste de la donnée

319. La notion de protection, si elle est entendue premièrement comme l'action de protéger ou défendre quelqu'un contre un danger, un mal peut être aussi comprise dans le sens de favoriser une activité, aider à son développement. En ce sens, la protection des données peut être également entendue comme les moyens de favoriser l'usage de ces données. La protection se définissant comme aussi bien les mesures consistant à se prémunir d'un risque, mais vise également « le système de protection établi[640] ». Une telle compréhension, une nouvelle fois purement sémantique, nous invite alors à s'interroger sur la dualité d'un tel terme, et il ressort qu'une fois appliquée à la protection des données, cette dualité se retrouve facilement. Si la protection des données personnelles a notamment pour but de protéger les droits et libertés fondamentaux des personnes physiques, donc de défendre les personnes physiques contre des atteintes à ces droits et libertés, elle a aussi pour intérêt de favoriser et faciliter la circulation des données[641]. Et s'agissant des données non personnelles, on peut comprendre les moyens pour protéger ou même favoriser ces données, mais aussi appréhender l'ensemble d'un système centré sur ces dernières.

320. En tant que protocole informatique, dont l'objet restera, de manière schématique, une gestion décentralisée et organisée de données, un protocole *blockchain* aura pour vocation de se voir appliquer l'ensemble des règlementations applicables à ces données. Une qualification, nécessaire et en amont, de la notion de données peut amener à une classification entre donnée personnelle, soit « toute information ou ensemble d'information permettant d'identifier directement ou indirectement une personne physique[642] », et donnée non personnelle, à savoir les données autres que les données à caractère personnel au sens du RGPD[643]. Et si la *blockchain* peut apparaître comme opposée aux impératifs de protection des données, il en ressort pourtant une compatibilité de cette technologie avec les objectifs de la protection des données (Section 1), puis ceux entre données non personnelles et *blockchain* (Section 2).

[640] CORNU G., précité

[641] Considérants 12, 13, 21, RGPD, précité ; on notera également que cette notion de libre circulation est directement mentionnée dans le titre même du règlement 2016/679.

[642] RGPD, art.4 point 1

[643] RGPD, art. 3

Section 1 : Compatibilité de la protection des données personnelles avec la *blockchain*

321. Entendue comme impératif et même comme corollaire des libertés fondamentales, la protection des données personnelles demeure un exercice fondamental pour tout opérateur effectuant des traitements de telles données. Et pour faire un rappel lapidaire, la protection des données personnelles impose à tout responsable de traitement le respect et l'application de plusieurs principes directeurs, parmi lesquels le principe de limitation de la conservation - requérant une limitation et une proportionnalité des données personnelles - mais aussi le respect de différents droits de la personnalité, au sein desquels le renommé droit à l'oubli se trouve. La consécration de la protection des données personnelles s'entendant aujourd'hui à la lumière de la protection de la vie privée, consécration acquise depuis 2010 à un niveau européen[644], corroborant d'ailleurs de ce fait une certaine volonté d'entendre la protection des données - et donc un droit des données - à une échelle européenne.

322. L'opposition apparaît ainsi de manière flagrante : le droit positif a, dans un premier temps, voulu renforcer les prérogatives des personnes physiques sur la gestion de leurs données personnelles, en conférant ou en renforçant des droits de la personnalité dédiés issus de la protection de la vie privée[645], et, dans un second temps, permettre l'exploitation de telles données par des opérateurs[646] - personnes morales pour la grande majorité, en parallèle des acteurs étatiques). Cette opposition, appliquée à la technologie des chaînes de blocs, peut se cristalliser autour de la question du respect ou non des principes issus de la protection des données par le biais d'une *blockchain*, point qui a d'ores et déjà fait l'objet de premières études[647], pointant d'ailleurs souvent une incompatibilité entre *blockchain* et protection des données personnelles[648]. Au contraire, que ce soit pour le droit à l'oubli[649] ou pour le droit à

[644] CEDH, 2 sept. 2010, Uzun c. Allemagne, Req. n° 35623/05

[645] Pour une référence à l'impératif de la protection de la vie privée : Considérant 4, RGPD

[646] Considérant 2, RGPD

[647] DOUVILLE T., *Blockchain et protection des données à caractère personnel*, AJ Contrats d'affaires-concurrence-distribution, 01/07/2019, 7, pp.316-320

[648] CULLAFFROZ-JOVER S., BACQ E., *Blockchain et données à caractère personnel, l'improbable conciliation ?*, Droit et patrimoine, 01/04/2019, 290, pp.28-30

[649] CE, 13 déc. 2019, n°391000, disponible à https://www.conseil-etat.fr/actualites/actualites/droit-a-l-oubli-le-conseil-d-etat-donne-le-mode-d-emploi (consulté le 10/12/2019)

la portabilité, nous pourrons mettre en avant les avantages d'une *blockchain* pour la gestion de telles données.

323. Si un géocentrisme[650] actuel autour de la donnée personnelle, notamment avec la mise en application du Règlement Général sur la protection des données personnelles (dit « RGPD ») et la modernisation de la loi Informatique et Libertés de 1978, n'est pas ici à démontrer, l'ensemble de ces dispositions doivent trouver application pour tout protocole *blockchain* dont l'utilisation reviendrait à la mise en œuvre d'une ou de plusieurs « opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou des ensembles de données à caractère personnel, tels que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction[651] ».

Une approche protectionniste, c'est-à-dire une approche dans laquelle les données personnelles doivent être protégées, contre les altérations, mais aussi de manière à respecter les droits accordés aux personnes concernées par le droit positif, peut présenter une incompatibilité apparente avec un protocole *blockchain*. On rappellera également que la protection des données personnelles peut se réaliser au prisme de la protection de la vie privée[652]. Dès lors, comment l'utilisation d'une technologie mettant en avant ses capacités de sauvegarde et d'horodatage des données peut être utilisée en accord avec les dispositifs légaux en vigueur ? Cette approche protectionniste, prônant donc la thèse selon laquelle la technologie *blockchain* ne serait pas compatible avec le droit positif relatif à la protection des données doit toutefois être nuancée. Si la volonté du législateur (national mais aussi européen) a bien été de garantir un socle de protection pour les personnes physiques afin d'en garantir une meilleure gestion, c'est également en effectuant un équilibre avec les nécessaires flux de données.

D'ailleurs, la mise en application du RGPD, en parallèle d'une économie de la donnée toujours plus forte[653], fait renaître des problématiques quant à la mise en place d'un droit de

---

[650] Métaphoriquement, la notion de géocentrisme démontre l'importance actuelle de la protection des données personnelles.

[651] RGPD, art. 4 point 2

[652] CEDH, 2 sept. 2010, précité

[653] ISAAC H., *La donnée, une marchandise comme les autres ?*, Annales des Mines - Enjeux Numériques, Conseil général de l'Économie, ministère de l'Économie et des Finances, 2018.

propriété sur les données[654]. Le débat sur la construction d'un droit de propriété sur les données personnelles peut trouver des raisons pour[655] ou contre[656], toujours est-il que la *blockchain* peut avoir le mérite d'être un argument pour une création d'un droit de propriété. Permettant une traçabilité et un contrôle sur les données partagées, le caractère non rival d'une donnée peut être contrebalancé par l'utilisation d'une *blockchain*.

324. Sans pour autant créer, aujourd'hui, un régime de propriété des données personnelles, régime pour lequel la CNIL est encore opposé[657]), sa volonté apparaît comme duale, notamment au profit des différents opérateurs cherchant à utiliser toujours plus de données personnelles dans le cadre de leurs activités. Pour autant, l'étude, aussi bien pragmatique que théorique de cette technologie ne ferait-elle pas apparaître une possibilité de mettre en balance ces deux intérêts en apparence contradictoire ? C'est en réalisant, une nouvelle fois, une application ordonnée de la lettre de la loi qu'une réponse tend à se dessiner, notamment pour déterminer les conséquences du droit positif sur l'utilisation d'une *blockchain* dans le cas où un tel protocole supporterait l'utilisation de données personnelles[658]. Si la *blockchain* ne permet pas de trancher ce débat, il convient de mentionner qu'elle peut devenir un argument au profit d'une telle patrimonialisation des données.

325. Toutefois, compte tenu des caractéristiques techniques de la *blockchain*, en particulier l'utilisation de réseaux pair-à-pair, invite à une minutie dans la détermination des acteurs d'une *blockchain* au service de l'applicabilité du régime de protection des données (§1), pourtant, cette minutie n'apparaît pas comme obstacle à la compatibilité de la *blockchain* avec le respect des règles de protection des données personnelles (§2).

---

[654] PADOVA Y., *Entre patrimonialité et injonction au partage : la donnée écartelée ?*, Revue Lamy Droit de l'Immatériel, n°155, 1er janv. 2019

[655] LESSIG L., *The Architecture of Privacy*, Conference Taiwan Net, 1998

[656] Contre l'idée de patrimonialité, comme pouvant créer de nouveaux systèmes discriminants et inégalitaires (ELVY T.-A., *Paying for Privacy and personal data economy*, Columbia Law Review, Vol. 117, nº 6, Oct. 2017, p.1405 et s.

[657] CNIL, rapport d'activité, La documentation française, 2017, p.52

[658] Excluant ainsi toute donnée non personnelle, y compris des données personnelles anonymisée (et donc, par définition, des données non personnelles).

§1 : La nécessaire minutie dans la qualification des acteurs d'une *blockchain*

326. Aux origines de la protection des données se trouve la protection de la vie privée établie par le Code civil, en son article 9 : « Chacun a le droit à la protection de sa vie privée ». La protection des données est également marquée par l'iconique loi dite « Informatique et Libertés[659]» de 1978, dont la construction n'est pas anodine dans le cadre de nos propos. En effet, sans pour autant retracer l'historique de l'intrusion de l'informatique dans notre société, depuis les années 1970 à aujourd'hui, la construction de cette loi a débuté par un rejet de l'immixtion de l'agrégation massive de données sur l'ensemble des citoyens français, avec le projet dit « SAFARI[660]». Cela étant, l'une des motivations des différentes commissions en charge de la LIL était justement la crainte de l'agrégation trop massive de données personnelles, à travers l'interconnexion de différents fichiers étatiques, permettant d'identifier l'ensemble des citoyens français, et qu'une telle agrégation serait un pas trop fort pour la stigmatisation et le « fichage » d'individus.

Plus récemment, la protection des données a été fortement marquée par l'établissement puis l'entrée en vigueur du « Règlement pour la Protection des données[661] ». Abrogeant la directive 95/46/CE[662], ce règlement (dont la nature le rend applicable à l'ensemble des citoyens européens), a su devenir depuis son entrée en application une pierre angulaire du droit positif relatif à la protection des données personnelles. Même si, de manière parallèle, la LIL a pu être remaniée[663] suite à ce règlement, en particulier pour reprendre les différentes définitions applicables les règles de détermination des régimes de responsabilités inhérents.

327. La notion de responsable de traitement fait écho à la capacité juridique et organisationnelle ainsi qu'à l'autonomie dans la définition des moyens du traitement. Le responsable de traitement peut parfois être désigné par la loi, et ne peut en tout cas, être soit la

[659] Loi n°78-17 du 6 janv. 1978, précitée

[660] https://sites.ina.fr/cnil-40-ans/focus/chapitre/2

[661] Règlement (UE) 2016/679, précité

[662] Directive 95/46/CE du Parlement européen et du Conseil, du 24 oct. 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

[663] Notamment par l'Ordonnance n° 2018-1125 du 12 déc. 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janv. 1978, précitée.

personne concernée, soit le destinataire ou encore le sous-traitant de ce dit traitement[664]. Dans une architecture centralisée standard mettant en œuvre des traitements de données personnelles, le responsable de traitement est le plus souvent le représentant légal de la société qui met en place ce traitement[665]. Or, la première difficulté qui apparaît est qu'un système d'information supportant un protocole *blockchain* (et, une nouvelle fois, si tant est qu'il traite des données personnelles) repose sur une architecture décentralisée. Il convient donc de pouvoir déterminer qui est le responsable de traitement, et à cet effet, plusieurs hypothèses trouvent illustration ; ces hypothèses découlant directement du choix de gouvernance retenu pour la mise en place, la maintenance et l'évolution d'un tel protocole.

Dans les différentes applications de la technologie *blockchain*, cette architecture peut être mise en place au sein d'une seule et même société (ou une autre structure), dans le cadre d'une gouvernance uniquement centralisée. Dès lors, la détermination du responsable du traitement ne posera guère de souci. La structure (ou son représentant) ayant mis en place un réseau *blockchain* sera considérée comme le responsable de traitement selon des critères de droit commun (à savoir la définition, la mise en place ou encore la détermination des choix arbitraires sur les moyens et les finalités d'un tel traitement de données personnelles). Toutefois, et en fonction des aspects de gouvernance retenus, le cas d'un groupement de personnes morales dépourvu de personnalité juridique procède d'une approche pragmatique intéressante en présence de deux hypothèses possibles : la présence d'un groupement dépourvu ou non de personnalité juridique.

En particulier, cette mise en place d'une gouvernance contractuelle lors de la mise en place d'un protocole *blockchain* mettant en œuvre des traitements de données personnelles devra mettre en place une définition précise des rôles et responsabilités (exercice des droits, désignation d'un délégué à la protection des données, mise en place de mesures

[664] Article 3 - Loi Informatique et Libertés (précitée)

[665] Article 2 - Loi Informatique et Libertés (précitée) : Un traitement est « toute opération ou tout ensemble d'opérations portant sur (des données à caractère personnel), quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. ». On peut ainsi voir une définition extrêmement large donnée par le législateur. Ainsi, tout ème d'information touchant de près ou de loin à une donnée personnelle est concerné par cette loi.

organisationnelles ou techniques de sécurité) pour éviter de souffrir d'une requalification de « *pool*[666] » par le juge en cas de litige.

328. S'agissant de la présence éventuelle d'un sous-traitant, on peut se borner à rappeler que, pour reprendre la lettre de la loi et en particulier celle du RGPD, le sous-traitant est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement[667] ». En pratique, il peut s'agir de l'hébergeur de données, un fournisseur de services applicatifs, ou encore une société partenaire. La présence d'un tel sous-traitant n'impacte que peu le régime applicable à l'utilisation d'une *blockchain*[668], compte tenu du fait qu'il n'aurait aucun impact sur les moyens et finalités d'un traitement de données personnelles.

La désignation d'un tel correspondant (ou délégué) devra correctement se faire en amont de la mise en place de tout traitement de données personnelles au sein d'un réseau *blockchain* pour assurer une correcte sécurité juridique. D'ailleurs, la lecture du règlement sur les données personnelles[669] permet à un groupe d'entreprises de désigner un seul délégué à la protection des données, « à condition qu'un délégué à la protection des données soit facilement joignable à partir de chaque lieu d'établissement ». Ainsi, une détermination commune de la personne en charge de ce rôle déterminé devra se faire de façon concertée, entre tous les acteurs d'un réseau *blockchain*. Cette désignation *ex ante* fait d'ailleurs écho à une nécessaire prévoyance dans l'élaboration de tout traitement de données personnelles, principalement pour la gestion des données personnelles qui seront recueillies par la suite.

---

[666] La notion de « *pool* » est principalement utilisée en droit financier ; une telle qualification pouvant emporter caractérisation d'une société en participation, même si la doctrine comporte un courant qui n'admet pas cette qualification ; LEGEAIS D. *Pool Bancaire*, RTD com. 2007. p.429

[667] Art. 4, règlement n°2016/679 du 27 avril 2016, précité

[668] Outre les différentes obligations pesant sur le sous-traitant, notamment dans le cadre de sa collaboration avec le responsable de traitement de données personnelles (https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf, (consulté le 05/10/2019)

[669] Section 4 : Délégué à la protection des données, Règlement européen sur les données personnelles d'avril 2016, précité

329. La désignation du responsable de traitement répondra aux critères désignation classique (soit légale[670], judiciaire[671], ou encore de manière contractuelle), et il convient de faire référence à ces critères dans une telle situation. Au-delà, une désignation contractuelle pourra se faire dans le cadre d'une « approche risque », en particulier pour identifier et réduire le risque juridique inhérent à l'exploitation de traitements de données personnelles[672].

Pour faire une illustration, nous pouvons reprendre le cas du consortium R3. Or, dans un tel cas, l'architecture décentralisée mise en place par la technologie *blockchain* fait que tous les acteurs à cette architecture participent de façon égale, sans centralisation possible des traitements, et encore moins de centralisation décisionnelle. Dès lors, les critères de détermination du responsable de traitement vont être difficiles d'application. La détermination, les moyens et les finalités d'un traitement de données personnelles se faisant de manière commune à tous les acteurs d'une *blockchain*. Dans un tel cas, la situation contractuelle des différentes parties sera le premier point à prendre en compte, en particulier compte tenu de la pratique (pratique découlant irrémédiablement de la loi et notamment du RGPD[673]). Toutefois, cette gouvernance purement contractuelle, notamment en cas de litige ou en cas d'exercice des droits des personnes concernées par un traitement de données personnelles reposant sur un protocole *blockchain*, sera confortée à une gouvernance factuelle. À cet effet, la lecture de la doctrine du - feu - « Groupe de travail de l'article 29 » nous invite à une réflexion structurée.

---

[670] Par exemple, le Ministre chargé des relations sociales a la responsabilité d'un traitement, responsabilité conférée directement par la loi (Article R161-59, Code de la sécurité sociale : « Il est créé un traitement automatisé permanent d'informations nominatives à des fins statistiques en matière de retraite, mis en œuvre par un service statistique placé sous l'autorité du ministre chargé des affaires sociales et composé de : (…) »).

[671] De par l'expression de désignation judiciaire, il est fait ici, notamment référence aux critères déterminés par la CNIL ou encore du G Groupe de l'article 29, Avis n°01/2010, Groupe de travail « article 29 », WP 169 - Le groupe de travail «article 29» sur la protection des données a été institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 oct. 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), ou ceux retenus par la CJUE (exemple CJUE, gr. ch., 5 juin 2018, aff. C-210/16).

[672] Par exemple, au sein du Groupe Altice (acteur du secteur des télécommunication), lequel regroupe à la fois les dimensions techniques, commerciales, et d'exploitation de réseaux de communication, notamment avec la société « SFR », cette dernière a été désignée comme responsable de traitement même pour les activités non directement rattachées à la exploitation de lignes téléphoniques (cf. https://www.sfr.fr/offre-mobile/tarifs-conditions).

[673] Art. 26, RGPD, précité

La lecture de cette doctrine[674] nous invite à suivre les états d'analyse identifiés suivants[675] pour déterminer le responsable de traitement :

- « appréhender l'aspect personnel de l'entité désignée comme responsable de traitement de manière globale, de telle sorte qu'elle s'applique plutôt à des sociétés ou des organismes qu'à des personnes physiques ;

- vérifier si le pouvoir de déterminer les finalités et les moyens du traitement résulte d'une disposition légale ou une situation de fait ;

- ne pas hésiter, notamment en cas de détermination conjointe des finalités et des moyens d'un même traitement, à établir une coresponsabilité entre les différents acteurs participant à la mise en œuvre de ce traitement ».

330. Néanmoins, si ces critères paraissent adéquats, certaines difficultés pratiques s'opposent à l'identification d'un responsable de traitement s'agissant d'une *blockchain* publique. Premièrement, comme cela a pu déjà être souligné, les participants à une *blockchain* demeurent identifiés en premier lieu sous un pseudonomyne[676], avec les difficultés que cela engendre (techniques de ré-identification, recoupage de données, etc.). Dans le cadre d'une *blockchain* privée ou hybride, ou même dans le cadre d'une *blockchain* de type BaaS, les réflexions permettant de déterminer le responsable de traitement pourront reprendre les critères préalablement déterminés.

Dès lors, dans une approche déterministe de la responsabilité d'un traitement de données personnelles, une considération d'une pluralité de responsables de traitement est tout à fait concevable, d'autant plus que le récent règlement sur les données personnelles prévoit une possible détermination des finalités et un exercice d'un traitement de données personnelles conjoints[677]. Cela entraine *de facto* la responsabilité de tous les participants à une *blockchain*

---

[674] VIVANT M., *Lamy Droit du numérique (guide)*, p4255

[675] G29, Avis n°1/2010, précité

[676] BARBET-MASSIN A., FLEURET F., LOURIMI A., O'RORKE W, PION C., *Droit des cryptoactifs et de la blockchain*, Lexisnexis, 2020

[677] RGPD, précité : «responsable du traitement», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

mettant en œuvre un traitement de données personnelles comme possibilité. D'ailleurs, c'est la position de l'autorité de protection hongroise[678]. Néanmoins, compte tenu de la charge des différentes obligations relatives à la protection des données, cette possibilité reste particulièrement difficile à mettre en pratique[679].

331. Toutefois, il ressort d'une analyse de la CNIL[680] qu'une distinction préalable des participants et des utilisateurs doit être effectuée. S'agissant des mineurs et autres participants au réseau, ces derniers pourraient être considérés comme simples hébergeurs de données, effectuant leur prestation au nom et pour le compte du responsable de traitement (et auraient donc la qualité de sous-traitant). Néanmoins, si une tendance est à considérer le mineur d'une *blockchain* comme sous-traitant au sens du RGPD, rappelons que ce dernier possède plusieurs obligations, notamment une obligation de conseil envers le responsable de traitement[681], et que l'utilisation d'une *blockchain* ne viendrait que renforcer cette obligation de conseil compte tenu des spécificités d'une telle technologie[682]. Enfin, le cas de la coresponsabilité est également envisageable, notamment parce qu'elle est prévue par le RGPD[683]. Toutefois, elle interviendra le plus souvent dans le cadre de *blockchain* privées, au sein desquelles la détermination des rôles et responsabilités n'aurait pas été prévue. Il est également intéressant à relever que dans une position difficilement soutenable, à notre sens, en cas de contentieux, que la responsabilité conjointe pourrait découler du seul fait d'avoir choisi une infrastructure distribuée[684]. Au-delà, faire appliquer *de facto* un régime contraignant de responsabilité à un

[678] NAIH, *The opinion of the Hungarian National Authority for Data Protection and Freedom of Information on Blockchain Technology in Contexte of Data Protection*, Juil. 2017, p. 4.

[679] BARBET-MASSIN A, FLEURET F., LOURIMI A., O'RORKE W, PION C., *Droit des cryptoactifs et de la blockchain*, Lexisnexis, 2020, précité

[680] CNIL, Premiers éléments d'analyse de la CNIL, Sept. 2018, disponible à https://www.cnil.fr/sites/default/files/atoms/files/la_*blockchain*.pdf (consulté le 18/102018)

[681] Art. 28, 3°, f), RGPD : le sous-traitant « aide le responsable du traitement à garantir le respect des obligations (…) ».

[682] Sur le devoir de conseil, devenu depuis la réforme du droit des contrats le devoir d'information précontractuel, voir : Art. 1112-1, al. 1er, C. Civ. Sur le devoir de conseil appliqué à aux contrats du numérique : LE TOURNEAU P., *Du particularisme de l'obligation de conseil*, Dalloz référence Contrats du numérique, Chap. 014, 2021.

[683] RGPD, Considérant 79, art. 4, 7), et art. 26

[684] European Parliamentary Research Service, *Blockchain* and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law ? Study - Juil. 2019, disponible à https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf (consulté le 19/08/2019)

opérateur économique pour la simple raison d'un choix technique paraît contraire à la prise en compte de la seule qualité et typologie de ces activités[685].

332. Dans le cadre d'une entreprise utilisant une *blockchain* dans le cadre d'une activité professionnelle ou commerciale[686], il en ressort que le responsable de traitement serait la même personne effectuant cette activité professionnelle. Il peut être vu ici une application de la théorie de l'accessoire, théorie qui serait validée ici compte tenu que l'utilisation d'une *blockchain* ne serait ici qu'un support à une activité professionnelle ou commerciale. Au-delà, toute *blockchain* n'était qu'un outil, si ce dernier est utilisé au nom et pour le compte d'un responsable de traitement déterminée, alors toute personne œuvrant sur une *blockchain* (mineur, ou même prestataire de service) pourrait être considéré *a fortiori* comme un simple sous-traitant[687] au sens de la règlementation sur la protection des données personnelles.

Néanmoins, même si un engagement de responsabilité est possible pour un opérateur soit qualifié de responsable de traitement soit de sous-traitant, elle n'entrera en compte qu'en cas de litige. Il est logique que les différents acteurs se réunissant via une *blockchain* cherchent à tout faire afin que leur responsabilité ne soit pas engagée, ou *a minima* encadrée. En conséquence, les attraits d'une gouvernance purement contractuelle entre entités d'un groupement ne possédant pas de personnalité juridique retrouvera son intérêt pour l'exploitation d'une *blockchain*. Par exemple, pour l'exercice des différents droits accordés aux personnes physiques. Dans un tel cas, la possibilité la plus simple et efficace, est que chaque participant à ce groupement désigne en amont les différents rôles et responsabilités inhérents, le tout dans une démarche de conformité aux règles de protection des données[688].

Il est également entendu que, sur la notion de responsabilité conjointe, la CNIL a pu retenir l'importance du « rôle fondamental dans l'ensemble du processus décisionnel portant sur le traitement en cause (peu importe) la lecture formelle du contrat de sous-traitance[689] ». Il

---

[685] Pour rappel, les critères d'application matériels du RGPD ne vise pas les technologies utilisées mais bien la présence ou non de traitements de données personnelles (RGPD, art. 2).

[686] CNIL, Premiers éléments d'analyse de la CNIL, précité, p.2

[687] Cf. *Supra*, p.168 et suiv.

[688] DOUVILLE T., *Le contrat en matière de responsabilité conjointe de traitement des données*, Dalloz IT/IP 2021, p.188

[689] CNIL, délib. n°SAN-2020-012, 7 déc. 2020

faut entendre ici que c'est la réalité de la création et de la gestion du traitement de données personnelles qui prévaudra sur toute stipulation contractuelle. Toutefois, et à défaut, une reprise des critères dégagés par la jurisprudence[690] permettra d'anticiper une résolution des problèmes. Enfin, s'agissant de potentiels conflits de loi à un niveau international, l'utilisation de la *blockchain*, en particulier avec un anonymat fort, peut néanmoins être un obstacle particulier[691] à la détermination des responsables et des lois applicables[692]. Enfin, si la détermination des rôles et responsabilités comporte effectivement certaines difficultés, d'autres peuvent être identifiées pour le respect des principes de protection des données

§2 : La comptabilité technique de la *blockchain* avec le respect des règles de protection des données personnelles

333. Issus du « RGPD[693] », repris par la « LIL[694]», ces différents principes doivent être éclaircis pour en permettre une meilleure application dans le cadre de cette étude. Notamment pour comprendre si une différenciation d'application se créera en raison de l'utilisation d'une *blockchain*. Également, pour encadrer cette énumération de principes, nécessaires pour réaliser une application ordonnée de la loi à un protocole *blockchain*, il conviendra de rappeler que les récentes évolutions du droit de la protection des données tendent à mettre en place un principe de conformité au sein des entreprises, dans le sens où les responsables de traitement et leurs sous-traitants doivent créer, maintenir et actualiser une série de documentation inhérente à la protection des données personnelles, notamment pour pouvoir rapporter la preuve de la bonne application de ces principes. Il est également possible, à ce titre, de considérer la mise en place des différents principes issus de la protection des données comme

[690] Voir notamment : CJUE 5 juin 2018, aff. C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c/ Wirtschaftsakademie Schleswig-Holstein GmbH, pt 29, D. 2018

[691] À ce sujet, et compte de la spécificité de la résolution d'un conflit de loi d'un point de vue international, il est possible de reprendre certains raisonnements déjà retenus, tels que : F. MACLEAN, *Governing The Blockchain : How to determine applicable law*, (2017), 6 JIBFL 359, spéc. p. 361. », DE VAUPLANE H., *Blockchain and Conflict of Laws*, RTDF 2017, 50-52. ; il n'y aura pas lieu, dans le cadre de cette étude, de plus approfondir cette problématique tant elle sort du cadre de l'étude de la *blockchain* au regard de la protection des données.

[692] AUDIT M., *Le droit international privé confronté à la blockchain*, Revue Critique de droit international privé, 2020, p.669, Dalloz

[693] Art. 5, règlement n°2016/679 du 27 avril 2016, précité

[694] Loi n°78-17 du 6 janv. 1978, précitée

la mise en place de politiques à l'internes à l'entreprise[695], et faisant ainsi écho aux différents développements sur la gouvernance[696].

Ces principes sont à concevoir au regard de la personne physique concernée par un traitement de données personnelles[697]. En effet, le responsable de traitement doit mettre en œuvre de manière « loyale » ses traitements de données personnelles. Si le RGPD n'indique pas de définition du caractère loyal, un arrêt de juin 2018[698], qui a pu faire l'objet de commentaires[699], donne une vision souple de ce principe. Serait considéré comme loyal un traitement de données personnelles qui respecte l'ensemble de ces autres principes, et pour lequel le responsable de traitement garanti l'exercice des droits accordés aux personnes concernées (droit de rectification, etc.).

334. D'une manière empruntée au droit de la concurrence, un comportement loyal serait l'inverse d'un comportement déloyal[700], caractérisé par des actes contraires aux règles et aux usages. Par exemple, pourrait être considéré comme déloyal un traitement de données personnelles réalisé à l'insu de la personne concernée. Sur le principe de transparence, le RGPD apporte des premiers éléments de compréhension[701] et la CNIL a pu apporter quelques précisions notamment sur les modalités de mise en œuvre de ce principe[702].

En réalité, ce principe de transparence peut trouver un écho avec d'autres règles et bonnes pratiques de gouvernance, par exemple en matière sociale en ce que l'on retrouve ce principe porté en exigence dans la transmission d'informations auprès du Conseil économique et social en entreprise[703]. Enfin, la licéité fait l'objet d'un article complet du RGPD[704], et porte sur la base légale, obligatoire, sur laquelle doit reposer un traitement de données personnelles.

---

[695] DEROULEZ J., *L'actualisation des enjeux liés aux données personnelles*, Revue Lamy Droit de l'Immatériel, n°156, 1er Fév. 2019

[696] *Supra*, Partie I, p.100 et suiv.

[697] Art. 5, RGPD, précité

[698] Cass. Soc. 13 juin 2018, FS-P+B, n° 16-25.301

[699] CIRAY H., *Du contrôle de loyauté d'un système de traitement automatisé de données personnelles, Dalloz actualité*, 02 juil. 2018

[700] Fiches d'orientation, *Concurrence déloyale*, Juil. 2019, Dalloz

[701] RGPD, précité, considérant 39 : « Le principe de transparence exige que toute information et communication relatives au traitement de ces données à caractère personnel soient aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples. »

[702] CNIL, « Conformité RGPD : comment informer les personnes et assurer la transparence ? », https://www.cnil.fr/fr/conformite-rgpd-information-des-personnes-et-transparence (consulté le 26/07/2019)

[703] DUPAYS A., *Transmission au CSE d'une information précise et écrite*, Le Lamy social, §4496, voir notamment : CA Versailles, 14e ch., 19 mars 2014, n°13/05954

[704] Art. 6, RGPD

Ces premiers principes, du fait de leur portée générale, permettent de poser un premier cadre, que l'on pourra retrouver dans son application à la *blockchain*. Mais surtout, ils permettent d'assurer, sur ces trois pans, un axe protectionniste avéré de l'utilisation des données personnelles. En ce sens, l'utilisation d'une *blockchain* face au RGPD dans ce contexte n'emporte aucune difficulté, du fait qu'il ne s'agisse, une nouvelle fois, qu'un aspect purement technique d'un traitement de données personnelles. En conséquence, l'usage ou non d'une *blockchain* ne peut modifier le respect ou non de ces principes par un responsable de traitement.

En l'occurrence, il appartiendra à ce dernier de veiller à la bonne application de ces premiers principes. Cette bonne application pourra se trouver notamment dans le matériel préparatoire ou dans les actes internes de gouvernance de la donnée. S'agissant de la licéité, l'existence et la documentation d'une base légale (exécution de mesures contractuelles par exemple) satisfont les exigences du RGPD. S'agissant de la transparence et de la loyauté, la communication d'une information claire et notamment précise[705] sur le traitement de données personnelles suffira au respect de ces principes. Il convient d'ailleurs de préciser que si l'information doit être « concise, transparente, compréhensible et aisément compréhensible, en des termes clairs et simples[706]», il n'est nullement indiqué une obligation de communiquer sur les moyens techniques d'un traitement de données personnelles. Si la transparence doit conduire à la compréhension de la personne physique concernée des modalités de traitement de ses données, il y a fort à parier que l'énumération de procédés techniques complexes (comme le serait l'explication du fonctionnement d'un hébergement via une *blockchain*) nuise au contraire à la bonne compréhension de l'information, au point qu'elle nuirait à la transparence ici requise.

La notion de finalité de traitement[707] renvoie au fait qu'un traitement de données personnelles doit avoir un « but » précis, et permet d'éviter, tout en donnant une impulsion forte aux systèmes de gouvernance adaptés, que des données ne soient traitées que « au cas où », sans but ni objectif précis. La réflexion précédente sur l'utilisation d'une *blockchain*, prise en tant que simple outil, peut trouver de nouveau application.

[705] Art. 12, RGPD
[706] Considérant 39 et Art 12, al. 1, RGPD
[707] Art. 5 et art. 6, RGPD

335. Ces deux principes[708] font échos aux caractéristiques techniques d'un traitement de données personnelles ; ils imposent la prise en compte d'impératifs de sécurité dès la conception, et pendant l'usage d'un traitement de données personnelles, dans le cadre d'une approche par les « risques[709] ». Là encore, si la *blockchain* présente de manière pertinente des avantages pour la sécurité de l'information, ce point ne soulève pas de difficultés particulières. De surcroît, les caractères techniques d'une *blockchain* présentent même des atouts pour le respect de ces principes, en particulier compte tenu des caractères immuables des données dans une *blockchain*.

Au-delà, ces principes imposent, de manière proportionnée aux typologies de données traitées et aux objectifs à atteindre des différents traitements[710] l'utilisation de *blockchain* permissionnées (ou hybrides) comme un moyen d'atteindre ces objectifs de sécurité et de *privacy by design/default*[711]. Une nouvelle fois, la prise en compte des attributs techniques d'un outil au bénéfice d'un traitement de données personnelles ne remet pas en cause l'application ou non des principes jusqu'ici énoncés.

336. Une nouvelle fois, pour l'application de ces deux principes[712], il conviendra de renvoyer aux réflexions précédentes, ces principes s'appliquant directement au responsable de traitement et non pas aux techniques mises en place par lui. Il appartient à ce dernier de réaliser des traitements de données personnelles avec des jeux de données exacts (tout en garantissant pour les personnes concernées leur droit de rectification[713]) et que ces jeux de données soit limités aux seuls besoins de son traitement de données personnelles. L'exactitude, compte tenu

---

[708] Considérant 78, art. 25, RGPD

[709] L'article 25 du RGPD indique que les mesures de protection des données dès la conception et par défaut doivent être prises « Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée ». Cette approche traduisant alors une approche par les risques, faisant référence à l'état de l'art en termes de techniques de sécurité, mais aussi dans une façon où le responsable de traitement doit mettre en place des mesures proportionnées au traitement de données personnelles concerné.

[710] Ici sont visés notamment la présence ou non de données qualifiées de « sensibles », et l'impact sur les droits et libertés des personnes concernées.

[711] Demeurant ainsi un moyen de satisfaire un critère notamment rappelé par la jurisprudence européenne (CEDH, 18 sept. 2014, Brunet c. France, Req. n° 21010/10)

[712] Considérant 156, art. 5 et art. 25, RGPD

[713] RGPD, précité, article 16

du caractère intangible d'une *blockchain,* devrait être respectée dès la collecte des données, au risque de la multiplication des opérations techniques par la suite nécessaire afin de prendre en compte une éventuelle modification des données. Toutefois, si les données d'une *blockchain* peuvent être considérées comme intangibles, rien ne s'oppose à l'enregistrement de données postérieures ayant pour seul but de préciser que des données antérieures soient modifiées.

337. L'anonymisation est une technique permettant l'impossibilité d'identification d'une personne à partir d'un jeu de données[714]. L'un des intérêts de l'anonymisation est de sortir du cadre du RGPD[715], mais il répond à des critères stricts, notamment l'utilisation de techniques de chiffrement particulière[716]. Au-delà, une facette importante de l'utilisation d'une *blockchain* face aux règles de protection des données doit être prise en compte. Il est opportun de rappeler que l'anonymisation des données, si l'expression n'est mentionnée qu'au sein des considérants du RGPD[717], implique la mise en place de procédés techniques rendant impossible l'identification d'une personne physique à partir d'un jeu de données.

De surcroît, la CNIL a pu préciser[718] que l'anonymisation, pour être efficace doit répondre à trois critères : celui de l'individualisation (il ne doit pas être possible d'isoler une personne physique au sein d'une même base de données), de la corrélation (l'identification grâce à deux ou plusieurs jeux de données individualisantes ne doit pas être possible) et de l'inférence (il ne doit pas être possible de déduire des informations sur une personne à partir d'un premier jeu de données). L'ensemble de cette étude étant étroitement liée aux aspects techniques de la *blockchain*, il convient alors de les rappeler. Les caractéristiques d'une *blockchain* en ce qu'elle reste fondamentalement un arbre de Merkle[719] nous renvoie à la possibilité d'utiliser des données personnelles de manière corrélée, en doublant les bases de données. En effet, les données stockées puis partagées dans une *blockchain* peuvent être

[714] https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles, consulté le 30 mai 2020

[715] Considérant 26, RGPD ; par simple application du fait que le RGPD s'applique à des données personnelles, et qu'une donnée anonyme est, par définition, non personnelle ; voir notamment : VIVANT M., « Les données anonymisées », VIVANT M., *Le Lamy Droit du numérique*, §458

[716] Avis n°05/2014, Groupe de travail « article 29 », sur les techniques d'anonymisation, adopté le 10 avril 2014, WP216 sur les techniques d'anonymisation du groupe de travail « Article 29 » adopté le 10 avril 2014, WP216

[717] RGPD, précité, considérant 26

[718] https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles (consulté le 02/12/2019)

[719] Cf. *Supra*, p.13

seulement des « *hash* [720] » de documents, des empreintes numériques et donc pas nécessairement des données permettant une identification directe ou indirecte de personnes physiques (soit des données personnelles). Dès lors, des données personnelles peuvent être utilisées, indirectement par une *blockchain*, mais la seule utilisation d'une *blockchain* n'emporte pas forcément application de la réglementation sur les données personnelles. Néanmoins, il convient de mentionner que si la CNIL a déjà pu considérer les fonctions de hachage comme permettant d'assurer un haut niveau de confidentialité[721], permettant la satisfaction des principes issus de la protection des données personnelles, il parait plus opportun d'appréhender une architecture d'hébergement de données à deux niveaux, permettant ainsi d'éviter de stocker des données personnelles sur une *blockchain*. Au surplus, ces techniques de chiffrement ont déjà pu être reconnues à nouveau comme satisfaisant les règles de protection des données personnelles, insistant d'autant plus sur la nécessité d'une bonne gouvernance de tout projet *blockchain*, dans le cadre d'une gestion des risques maîtrisés[722].

338. Corollaire du principe de loyauté, l'exercice des droits accordés[723] aux personnes physiques[724] doit être garanti dans le cadre d'un traitement de données personnelles. Dès lors, afin de pouvoir répondre positivement à toute demande de gestion de données personnelles, formulée par une personne faisant l'objet d'un traitement, cette possibilité devra être implantée dans le protocole *blockchain* afin que toute modification ou même suppression de données n'entraine pas d'instabilité dans le système. Cette nécessaire régulation *ex ante* est justement à mettre en exergue avec le possible engagement de responsabilité du créateur de logiciel qui devra porter toute son attention lors de l'écriture du code informatique servant de base au

[720] Rappelons qu'une fonction de hachage permet d'obtenir un condensé normé de n'importe quelle information, et qu'en l'état actuel de la technique, un *hash* ne permet pas, à lui seul, de retrouver un document originel, ou ici la personne concernée ; cependant, il permet d'effectuer une comparaison entre deux fichiers, en assurant une simple comparaison de ces dits « *hash* ». Pour plus d'information, voir notamment : DE VAUPLANE H., *Introduction Blockchain, cryptomonnaies, finance et droit : état des lieux*, Revue Lamy droit des affaires, n°140, 1er sep. 2018

[721] CNIL, Premiers éléments d'analyse de la CNIL, précité

[722] Agence espagnole pour la protection des données, *Introduction to the hash function as a personal data pseudonymisation technique*, oct. 2019, disponible à ;https://edps.europa.eu/data-protection/our-work/publications/papers/introduction-*hash*-function-personal-data_en (consulté le 11/11/2019)

[723] On pourra se borner à mentionner ces différents droits : droit d'accès, droit à la rectification, droit à l'effacement, droit d'opposition, droit à la limitation, droit à la portabilité, droit d'information et d'opposition concernant la prise de décision automatisée et le profilage, mais également le droit de disposer de ses données après la mort, droit créée par la loi n° 2016-1321 du 7 oct. 2016 pour une République numérique.

[724] Considérant 39, art. 12, RGPD

logiciel *blockchain*, notamment dans le cadre de son devoir de conseil[725]. Devoir qui pèse également sur un prestataire mettant à disposition une *blockchain*. En cas d'oubli (volontaire ou non) de prise en compte de ces droits dans le protocole *blockchain*, ces différents doivent peuvent être mis à mal, en particulier le droit à la modification ou le droit d'opposition[726,727]. Compte tenu des spécificités de la *blockchain*, aucune modification ou opposition sur les données personnelles ne serait facilement et techniquement possible, pouvant placer le responsable de traitement dans une impossibilité technique de répondre favorablement à une telle demande. Or, l'impossibilité technique comme motivation au non-respect de ces droits n'est pas prévue par les textes[728].

339. Une nouvelle fois, l'étude et la compréhension de la technologie devra être antérieure à toute mise en œuvre. Par exemple, l'exercice du droit à la portabilité[729] peut parfaitement se conjuguer avec soit l'extraction de données d'une *blockchain* (en remplaçant ces données par la seule indication de leur fourniture, fait techniquement possible grâce aux fonctionnalités d'une *blockchain*), soit en utilisant un format ouvert de données. Les caractéristiques techniques d'une *blockchain* n'apparaissant pas comme incompatibles avec la protection des données personnelles[730]. Le droit à la modification ou encore à l'opposition peut faire l'objet de spécificités techniques préalables.

340. Si le droit à l'oubli a notamment été marqué par la jurisprudence européenne[731], le principe de conservation limitée[732] induit l'obligation, pour le responsable de traitement de ne pas conserver les données plus longtemps que nécessaire. Cette durée de conservation devant être définie par lui, que ce soit en fonction des durées de traitements ou encore d'impératifs légaux (par exemple, le Code de commerce impose une conservation de 10 ans pour les documents comptables et les pièces justificatives associées[733]). C'est ici un parallèle de ce que

---

[725] Cf. *Supra*, p.176

[726] Art. 21, RGPD ; pour rappel, le droit à l'opposition permet à la personne concernée d'interdire au responsable de traitement la réutilisation de ses données pour un objectif précis.

[727] Sur le droit à l'oubli : cf. *Supra,* p.168

[728] Art. 21, RGPD : « Le responsable du traitement ne traite plus les données à caractère personnel, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice. »

[729] Art. 20, RGPD, précité

[730] CNIL, « Premiers éléments d'analyses », précité

[731] CJUE, 13 mai 2014, aff. C ‑ 131 ‑ 12, arrêt Google Spain

[732] RGPD, précité, considérant 65 et article 5

[733] Art. L123-22 C. Com

le principe de conservation limitée impose une suppression des données à l'arrivée de termes préalablement décidés par le responsable de traitement. Le droit à l'oubli paraît peu compatible avec la technologie *blockchain* dont l'immuabilité est mise en avant.

Par ailleurs, la technique apporte une réponse concrète et satisfaisante à cet apparente problématique. En effet, il ne faut pas omettre la possibilité d'utiliser des données en amont verrouillées ou avec un accès limité en sus de l'utilisation d'une *blockchain*. Un protocole de permission pour accéder à des données qui seraient, initialement, non accessibles, est tout à fait envisageable[734]. Ce type de solution entraîne, techniquement, une impossibilité d'accéder aux données. Compte tenu du fait que ces données ne sont lisibles qu'avec une autorisation informatique permissionnée, grâce à laquelle seules les données personnelles relatives à l'accès sont sauvegardées en tant que telles, cette solution été reconnue comme étant une solution viable par la CNIL[735] et le service de recherche du Parlement Européen[736]. Au-delà, les difficultés sont principalement présentes pour une *blockchain* de type publique, compte tenu du caractère public des informations et l'impossibilité d'effacer sans consensus les données présentes sur une *blockchain*. Ainsi, la possibilité technique d'effacement de données est possible, mais reste, en pratique, difficile[737]. Toutefois, et compte tenu des difficultés pratiques sur l'identification des responsables de traitement et de l'engagement de leur responsabilité[738], l'exercice d'un droit à l'oubli paraît compromis. En conséquence, ce n'est pas la technologie *blockchain* en tant que telle qui représente un obstacle à l'application de la réglementation inhérente à la protection des données personnelles, mais seule sa gouvernance[739] initiale. De surcroît, la maîtrise de l'outil emporte solution face aux difficultés d'application de la norme.

341. Néanmoins, la problématique du droit à l'oubli peut prendre une autre dimension compte tenu des différents traitements de données personnelles envisagés, en particulier pour les traitements ayant un intérêt public. Cette problématique est intimement liée à l'arrêt «

---

[734] Pour un exemple de protocole *blockchain* compatible avec une protection de la vie privée : https://blog.oceanprotocol.com/ocean-and-secret-collaborating-on-access-control-and-private-compute-for-datatokens-1427acd1fcbe (consulté le 27 mai 2021)

[735] CNIL, Premiers éléments d'analyse de la CNIL, précité

[736] European Parliamentary Research Service, précité

[737] DE FILIPPI P., REYMOND M., *La blockchain : comment réguler sans autorité ?*, In : NITOT T. (dir.) & CERCY N., Numérique : reprendre le contrôle, Framabook 2016

[738] Cf. *Supra*, p.176 et suiv.

[739] Étant entendu ici que la gouvernance est utilisée comme terme pour englober l'ensemble de l'éventuel projet utilisant une *blockchain* pour l'exploitation de données personnelles.

Manni[740] », rendu par la Cour de Justice de l'Union Européenne, qui interroge sur la portée du droit à l'oubli[741] sur la tenue des registres publics tels qu'un RCS. Cette problématique est d'autant plus renforcée par l'utilisation d'une *blockchain*, réputée pour être intangible, et donc non modifiable *a posteriori*. En dépit de l'apport de l'arrêt précité qui nous indique une portée extrêmement réduite de ce droit à l'oubli dans le cadre d'une telle utilisation des données, la mise en œuvre de ce droit ne semble pas, dans l'immédiat, être un obstacle à l'utilisation d'une *blockchain* pour la gestion du RCS. De surcroît, et dans un tel cas, la publicité des données va primer sur l'intérêt des personnes concernées[742]. Une nouvelle fois, le principe de conformité, invitant les acteurs concernés à démontrer leur capacité à s'autoréguler, ou, à défaut, à exprimer les raisons de leur non-conformité peut tenir de justification fiable, tant ces acteurs sont invités à pouvoir prendre acte de l'état de l'art de la technique. Si aujourd'hui la technique ne permet pas forcément à une *blockchain* de supprimer des données sans se corrompre, elle permet de rendre inaccessible et, dans une mesure acceptable, obtenir un résultat similaire à une suppression. Un parallèle entre l'impératif de la prise en compte de la protection des données personnelles au prisme de la vie privée[743] et la prise en compte de cette protection au regard de l'information.

342. Il reste néanmoins un enjeu particulier, celui des données composites[744], qui vont pouvoir avoir une nature hybride. Outre la caractérisation de telles données comme enjeu de complexification des règles relatives à la protection des données, un axe de réflexion sur les données non personnelles doit s'engager. À ce titre, l'exemple du RCS est opportun car composé de données à caractère personnel et non personnel, sachant que les données concernées sont utilisées dans une *blockchain*. Cette problématique revenant à réaliser une articulation de deux régimes de protection, celui des données personnelles et celui des données non personnelles. Pour autant, la protection des données non personnelles va pouvoir s'effacer contre la première, et ce pour une raison simple : le fait que cette situation soit prévue dans le RGNP[745]. Cela étant, la protection des données non personnelles ne doit pas pour autant être sous-estimée.

---

[740] CJUE, 9 mars 2017, n°C-398/15, dit arrêt « Manni »
[741] RGPD, précité, art. 17
[742] Arrêt Manni, précité.
[743] Arrêt Uzun c. Allemagne, précité.
[744] ZORN C., *Le jeu de données composites : données personnelles et (en même temps) non personnelles ?*, Dalloz IP/IT 2020 p.420
[745] Art. 2, RGNP

Section 2 : Valorisation des données non personnelles grâce à la *blockchain*

343. Si la notion de protection peut alors renvoyer soit à l'étude de mesures réduisant un risque, soit à l'étude d'un système particulier, l'étude de la protection des données non personnelles pourrait alors revenir à réaliser une étude similaire à la section précédente. À savoir l'étude d'une part de la caractérisation du régime applicable à la *blockchain* au regard de la protection des données personnelles (notamment la détermination des rôles et responsables en découlant) et d'autre part la détermination de l'applicabilité des principes issus de cette protection à la *blockchain*. Néanmoins, la protection des données personnelles, prise dans son illustration la plus récente, à savoir le RGNP, n'entend pas placer la protection des données non personnelles comme garante de droits et libertés face à un risque particulier : l'exploitation massive de données personnelles. Dès lors, quel est le risque identifié faisant l'objet de mesures le réduisant dans la protection des données non personnelles ? Il faut considérer que la protection des données non personnelles se réalise notamment par suite d'un constat, portant sur l'importance grandissante de l'économie de la donnée[746], et qu'il existe des obstacles qui aujourd'hui contraignent les intentions économiques libérales européennes. Obstacles auxquels le RGNP entend répondre, afin de renforcer les libres circulations de biens et de services, auxquelles sont rattachées de manière inexorable les données non personnelles. Ainsi, le risque identifié auquel le RGNP, pris en tant que socle de la protection des données non personnelles est l'entrave au libre-échange économique, dus aux différentes mesures de localisations des données non personnelles[747]. Le RGNP le rappelle textuellement, il a vocation à simplement « sauvegarder cette liberté » (de localisation des données), et alors, il permet le respect d'un cadre fondamental sur la circulation des données personnelles.

344. Cela étant, assurer une liberté de circulation sur les données personnelles n'emporte pas pour autant des contraintes pour les entreprises privées, qui restent libres de déterminer contractuellement les différentes localisations de leurs données[748]. Toutefois, le but est bien

[746] Considérant 1, RGPN : « La transformation numérique de l'économie s'accélère ». Le caractère lapidaire de cette phrase pourrait être vu soit comme une affirmation nette, au bénéfice d'une nécessaire intervention, mais aussi comme une frayeur, sur le fait que cette transformation numérique s'accélère de façon inexorable, et qu'il convient aujourd'hui, enfin, d'y répondre ou d'y participer concrètement.

[747] Considérant 4, RGNP

[748] *Ibid*.

de permettre aux entreprises d'avoir un renouveau sur leurs pratiques informatiques, et de leur permettre de se ressaisir de leurs données non personnelles[749]. Le système de protection s'élargit alors : au-delà de permettre aux entreprises de retrouver une gestion une partie leurs actifs immatériels (leurs données), c'est l'encouragement d'une gouvernance stratégique de leurs données qui est formulée. La *blockchain* se présente alors comme une technologie habile au service de la protection d'une partie des actifs immatériels d'une entreprise (§1), le tout dans une apparente conformité à des cadres fondamentaux (§2).

§1 : L'habilité de la *blockchain* pour la protection des données non personnelles

345. Le règlement européen du 14 novembre 2018 relatif aux données non personnelles[750] a donc vocation, notamment, à assurer la libre circulation des données à caractère non personnel. Outre la taille réduite de ce règlement (seulement neuf articles, là où le RGPD en comporte quatre-vingt-dix-neuf) et la reprise d'éléments du RGPD, trois aspects importants du RGNP peuvent être retenus dans le cadre de l'étude de la *blockchain* : l'encouragement du libre flux des données, la notion de disponibilité des données et la notion de portabilité. Au-delà, la protection des données non personnelles peut être également perçue, avec la récente adoption du RGPD en complément, comme témoin d'une construction d'un socle européen plus ambitieux encore, celui de la gouvernance européenne des données. Or, si l'encouragement du libre flux des données va bien être vecteur stratégique de la gouvernance des données, les deux autres notions sont plus rattachées à la protection de cadres fondamentaux.

346. Si les définitions des données personnelles ou non personnelles sont liées l'une à l'autre, et si les données personnelles sont rattachées par nature à la personne physique à laquelle elles sont rattachées, la notion de données non personnelles emporte un *distinguo* important à réaliser. En amont, la donnée non personnelle va pouvoir émaner et concerner uniquement les personnes morales. En ce sens, elles doivent être considérées comme restant « confidentielles à raison soit d'une conception très extensive du secret des affaires et de

[749] Considérant 5, RGNP
[750] Règlement (UE) n°2018/1807, précité

l'avantage concurrentiel que la structure veut préserver[751] », soit une lacune dans la gouvernance de leurs données conduisant à une dépendance économique[752] (et donc à un manquement dans l'exploitation de données). Si les données non personnelles sont définies comme « les données autres que les données à caractère personnel[753] » par le RGNP, ce dernier avance également que : « les technologies de l'information et des communications ne constituent plus un secteur d'activité parmi d'autres, mais la base de tous les systèmes économiques innovants et des sociétés modernes[754] », renforçant encore l'idée que la protection des données non personnelles est un support indispensable à l'innovation.

Ce même règlement met alors au même niveau les obstacles juridiques et techniques[755] ayant trait à la circulation des données non personnelles. Si ce droit marqué par l'existence de techniques juridiques[756], le droit de la donnée demeure bien rattaché à la technique car empreint fondamentalement de technicité matérielle et immatérielle. Au surplus, ce texte appuie également la mise en place, par les entreprises, de mécanismes d'autorégulation[757]. Corollaire indispensable à la création d'ensembles massifs de données, la libre circulation des données facilite alors l'émergence de nouveaux marchés, constitués notamment pour contrer une hégémonie américaine[758] ou asiatique[759].

347. En amont, s'agissant du champ d'application matériel du RGNP, tous les traitements[760] de données sont concernés, peu importe qu'il soit effectué par une personne physique ou

---

[751] FAVRO K., *Les données non personnelles : un nouvel objet juridique*, Dalloz IP/IT 2020, p.234

[752] DUBOC S., NOËL D.-J., *Économie et gouvernance de la données*, Avis du Conseil économique, social et environnemental, JO, 10 fév. 2021

[753] Art. 2, Règlement (UE) 2018/1807, précité

[754] Considérant 1, Règlement (UE) 2018/1807, précité

[755] Considérant 5, Règlement (UE) 2018/1807, précité ; « En même temps, la mobilité des données dans l'Union est également freinée par des restrictions relevant du secteur privé, à savoir les questions juridiques, contractuelles et techniques qui dissuadent ou empêchent les utilisateurs des services de traitement des données de transférer leurs données d'un fournisseur de services à un autre ou de les rapatrier vers leur propre système informatique, en particulier au terme de leur contrat avec un fournisseur. »

[756] ENCINAS DE MUNAGORRI R., *Qu'est-ce que la technique juridique ? : Observations sur l'apport des juristes au lien social*, Recueil Dalloz, Dalloz, 2004, pp.711-715

[757] POUILLET Y., *"La troisième voie", une voie difficile*, Revue Lamy Droit de l'Immatériel, n°182, 1er juin 2021

[758] Est fait référence ici aux GAFAMI.

[759] Les BATX (cf. Notamment https://fr.wikipedia.org/wiki/BATX, consulté le 17/04/2018).

[760] Art. 3, RGNP ; sein du RGNP, la notion de traitement est la même que celle définie dans le RGPD, à savoir « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou à des ensembles de données sous forme électronique, telles que la collecte, l'enregistrement, l'organisation, la structuration, le stockage, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ».

morale (tant qu'elle réside dans l'Union ou qu'elle dispose d'un établissement dans l'Union), si tant est qu'il soit fourni en tant que service aux utilisateurs résidants ou disposant d'un établissement dans l'Union[761]. Tout en étant rappelé que le RGNP n'est pas exclusif de l'application du RGPD lors de traitements portant sur des données personnelles et non personnelles[762]. La notion de traitement ici décrite est à considérer alors comme liste non exhaustive d'actions sur les données, et en conséquence, l'application d'une *blockchain* répond à cette opération, peu important ses particularités tenant au partage des données au sein d'un réseau P2P. Ainsi, la *blockchain* peut être concernée par l'application du RGNP en ce qu'elle constitue un moyen de traitement de données. Au-delà, la *blockchain* peut produire une architecture de données permettant une incrémentation horodatée des données, dès lors, ses bénéfices pour la structuration de grands volumes de données sont indéniables.

Néanmoins, la non-localisation des données, au-delà de mesures de sécurité mise en place par l'hébergeur de données peut être source de faiblesse dans la maîtrise de ces données. C'est dans ce cadre que la *blockchain* peut présenter un intérêt, ne serait-ce que pour assurer une traçabilité des accès aux données visées.

Ces différentes notions (traçabilité, accès, considérations réglementaires techniques et juridiques) ne sont pas sans rappeler la problématique relative à la gouvernance des données, dans le sens où elles appellent les opérateurs à s'auto réguler sur des aspects propres à la gestion de leurs données. D'ailleurs, elle fait l'objet d'un texte encore à l'état de projet[763], la gouvernance des données appelant notamment le partage de données entre entreprises[764], en ayant notamment pour but d'assurer une confiance dans le partage de ces données, y compris dans le respect des droits de propriété intellectuelle et du secret des affaires[765]. En ce sens, la *blockchain* présente des intérêts certains, notamment pour ses fonctions de traçabilité d'accès aux données, permettant de savoir quand, comment sont réalisés des accès aux donnée, mais alors aussi la présence d'une légitimité ou non, de ces accès. Cette notion de légitimité d'accès aux données qui n'est pas sans rappeler le cadre du secret des affaires.

---

[761] Art. 2, RGNP

[762] Art. 2, 2., RGNP

[763] Proposition de Règlement du Parlement européen et du Conseil sur la gouvernance européenne des données (acte sur la gouvernance des données), Bruxelles, le 25.11.2020, final 2020/0340(COD), précité

[764] Exposé des motifs, Proposition de Règlement final 2020/0340, précitée

[765] PETEL A., *Publication de l'Acte sur la gouvernance des données : les propositions de la Commission européenne*, Revue Lamy Droit de l'Immatériel, n°176, 1er déc. 2020

348. Quant à la loi n°2018-670 du 30 juillet 2018, relative à la protection du secret des affaires, procédant à une transposition de la directive 2016/943/UE du 8 juin 2016[766], à un premier but simple : encourager et protéger les investissements conférant un avantage concurrentiel. Axé notamment sur la recherche de l'innovation, le secret des affaires a vocation à protéger une information secrète, ayant une valeur commerciale, faisant l'objet de mesures de protection raisonnables[767]. Et la notion de secret est d'autant plus importante dans le cadre d'un univers numérique, au sein duquel l'information est d'autant plus facile à répliquer.

« Le secret se distingue des droits de propriété intellectuelle en ce qu'il ne fait pas l'objet d'un droit exclusif spécifique mais résulte du comportement des opérateurs économiques[768] ». Le secret des affaires permettant l'engagement de la responsabilité civile de l'auteur de l'accès illégitime à l'information protégée[769]. En résumé, l'application du secret des affaires nécessite une valorisation potentielle de données non accessibles pour les personnes familières du domaine informationnel concerné[770], et la mise en place de mesures de protection proportionnées. Une nouvelle fois, le parallèle avec la mise en place d'action de gouvernance autour de la donnée est aisé.

Dans un premier temps, la valorisation potentielle de données peut faire écho à l'inventaire des *assets* dans le cadre de la mise en place d'un système de management de la sécurité de l'information[771]. L'inventaire et la détermination des valeurs accordées assets ou actifs sont indispensables à la réalisation des mesures de prévention liées aux gestions du risque dans le cadre de mesures de protection de ces derniers. Permettant dès lors la mise en place de mesures de sécurité adaptées et proportionnées dans le but de leur protection.

Dans un second temps, et dans une logique propre à la protection des données[772], ce même caractère de proportion dans la mise en place de mesure de protection retrouve sens dans l'incorporation du secret des affaires dans la protection des données non personnelles.

---

[766] Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites (Texte présentant de l'intérêt pour l'EEE)

[767] Art. L151-1, C. Com.

[768] RICHARD J., *La divulgation de l'information protégée et les libertés économiques*. Thèse, Droit. Université Paris-Saclay, 2018

[769] RAYNARD J., *Le contenu et la particularité de la protection*, Propriété industrielle, 2018, dossier n°3

[770] Art. L151-1, C. Com

[771] ISO 27001 – Annex A.8: Asset Management

[772] Considérant 49, RGPD

En effet, le responsable de traitement doit mettre en place des mesures de sécurité proportionnées aux données personnelles qu'il peut traiter, et ce, soit en fonction des typologies de données concernées[773], mais aussi en fonction des risques informatiques identifiés[774]. En conclusion, une invitation est caractérisée, même si difficilement refusable, portant sur la mise en place d'un cadre interne au service d'une régulation des données. En définitive, le secret des affaires peut alors être un attribut au service de la protection des données non personnelles d'une entreprise[775].

Appliqué à la *blockchain*, le secret des affaires y trouve également intérêt, dans le sens où la *blockchain* possède des caractéristiques techniques utiles à ce secret. Une nouvelle fois, les fonctions de traçabilité de la *blockchain* peuvent être utiles[776], mais également les fonctions d'enregistrement horodaté ou les fonctions de hachage, utiles pour comparer des données publiées et permettre l'identification d'une fuite de ces données. D'ailleurs, précisons que la notion d'horodatage fait l'objet de dispositions légales, en particulier au sein du règlement eIDAS[777]. Ce dernier distingue l'horodatage électronique de l'horodatage électronique qualifié, en précisant que pour être qualifié, l'horodatage doit lier « la date et l'heure aux données de manière à raisonnablement exclure la possibilité de modification indétectable des données »[778]. À ce titre, la *blockchain* semble satisfaire ce critère. Il reste alors que la *blockchain* peut être un outil au service d'un « moyen de fait[779]», et donc un outil non pas juridique mais technique au service de la protection du secret. En outre, si la *blockchain* apparaît comme outil pratique de la protection du secret des affaires, elle se considère alors comme argument en faveur du processus créatif, et plus largement, dans l'encouragement de l'innovation. La rattachant une nouvelle fois, sans être ultime, à l'encouragement de l'innovation.

---

[773] Sera entendu ici que des données sensibles devront faire l'objet de mesures de protection plus rigoureuses que des données personnelles « simples ».

[774] https://www.cnil.fr/fr/credential-stuffing-la-cnil-sanctionne-un-responsable-de-traitement-et-son-sous-traitant (consulté le 28 janv. 2021)

[775] LAFAYE L., *Pour l'ouverture des données privées*, Expertises, Avril 2020

[776] Notamment pour la détermination des accès aux données gérées et à la recherche d'éléments permettant la caractérisation d'accès illégitime aux données, tels que prévus par l'article L151-5 du Code de commerce.

[777] Règlement (UE) n°910/2014, précité

[778] Art. 42, Règlement (UE) n°910/2014, précité ; précisons que pour être qualifié d'horodatage qualifié, ce dernier doit également satisfaire une exigence technique (être rattaché au temps universel) et être signé au moyen d'une signature électronique avancée ou par une méthode équivalente.

[779] HAGEL F., *Secrets et droits de propriété intellectuelle : un tour d'horizon*, Revue Lamy Droit de l'immatériel, n°53, 1er oct. 2009

349. Le RGNP postule donc que le libre flux des données jouera un rôle nécessaire dans l'innovation[780] au sein de l'Union Européenne. La recherche et développement (R&D) peut justement se définir notamment comme la recherche de connaissances nouvelles, emportant une valeur ajoutée pour l'économie de la connaissance[781]. L'une des difficultés de la R&D est de pouvoir consigner de manière régulière et sincère les différentes actions ou avancées de travaux de recherche, notamment pour satisfaire les règles du Crédit Impôt Recherche correspondant. La fonction de registre de la *blockchain* répond à ces exigences, le tout complété par une fonction d'horodatage forte[782]. En ce sens, la *blockchain* est d'ailleurs mise en avant pour ses avantages relatifs à la mise en place de système de « gouvernance et de suivi du processus créatif[783]».

350. Rappelons que la propriété intellectuelle est notamment au service de l'innovation, et que si le processus créatif peut être améliorer grâce à la *blockchain*, la possibilité d'utiliser une *blockchain* dans le cadre d'une création de preuve d'antériorité[784] est également un moyen au service de la valorisation de la propriété intellectuelle, et donc, une nouvelle fois, à celui de l'innovation. Rattachant cette dernière, à travers la *blockchain*, à la protection des données, mais aussi aux problématiques de gouvernance des données, tant l'inscription d'un cadre d'utilisation et de valorisation doivent être pris en compte pour de telles problématiques.

Toujours dans cet axe relatif à la valorisation de la propriété intellectuelle, il reste que la *blockchain* demeure également un atout pour la gestion collective de droits[785]. En particulier pour la gestion du droit de suite et du suivi du droit de reproduction et de représentation[786], la

---

[780] Considérant 13, RGNP

[781] « La R-D englobe les activités créatives et systématiques entreprises en vue d'accroître la somme des connaissances - y compris la connaissance de l'humanité, de la culture et de la société - et de concevoir de nouvelles applications à partir de connaissances disponibles. (...) Ainsi, pour être considérée comme relevant de la R-D, une activité doit comporter un élément : de nouveauté, de créativité, d'incertitude, ET être systématique, transférable et/ou reproductible » ; OCDE. (2016), Manuel de Frascati 2015, : *Lignes directrices pour le recueil et la communication des données sur la recherche et le développement expérimental*, Mesurer les activités scientifiques, technologiques et d'innovation, OECD Publishing, Paris.

[782] On pourra rappeler que la fonction de registre de la *blockchain* a été l'un des arguments en faveur de l'adoption de l'ordonnance n° 2017-1674 du 8 déc. 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers, qui légitime l'utilisation de la fonction de registre.

[783] BOUNOT V., précité

[784] Cf. *Supra*, p.70

[785] FAVREAU A., *Les outils technologiques de légitimation de la propriété intellectuelle*, Légipresse 2019, p.21

[786] ZLOTYKAMIEN C., *Blockchain et Propriété Littéraire et Artistique*, Mémoire de recherche, CEIPI, sept. 2017

blockchain peut être un outil efficace et pragmatique, au service de ces droits[787]. En ce sens, une meilleure traçabilité et un meilleur suivi (y compris comptable) de l'exercice de ces différents permettant, la valorisation des droits de propriété intellectuelle en matière de droit d'auteur[788], là où l'idée de valorisation s'entend traditionnellement en propriété industrielle[789]. Cette idée de valorisation permettant d'ailleurs de se rattacher les attraits de la propriété intellectuelle pour la recherche publique[790], et notamment du sort des données émanant de ces acteurs.

351. Initié dans les années 70, le mouvement d'ouverture des données publiques, d'*open data*, répondait à un mouvement en trois étapes, dont l'un était la prise en compte de la valeur des données produites par l'administration. On retrouve alors l'idée derrière laquelle la protection des données entend correspondre aux mesures de gouvernance des données, prises en tant que composante de la protection des données personnelles. Le concept d'*open data* fait aujourd'hui l'objet de nombreuses effervescences, au point nous parlons aujourd'hui d'une multitude d'*open data*[791] ; des données de la CNIL à l'*open data* des décisions de justice par exemple. À titre de rappel, de la création d'Etalab à la loi pour une République numérique, ainsi que les volontés des politiques successives pour que « le maximum de données produites par l'Administration[792,793] » soient rendues publiques, de nombreuses initiatives sont nées et continuent de naître dans une volonté de permettre un accès toujours plus large aux données publiques.

352. Au-delà, la mise en place d'*open data*, outre les problématiques purement techniques, notamment rappelées par la Professeure Favro[794], qu'elles soient liées à des questions

---

[787] BARBET-MASSIN A. DAHAN V., *Les apports de la blockchain en droit d'auteur*, BRDA n°8-2018, Francis Lefebvre, pp.21-25

[788] CLARK B., *Blockchain et droit de la propriété intellectuelle : une combinaison idéale au pays de la cryptographie ?*, OMPI Magazine, fév. 2018

[789] https://www.inpi.fr/fr/comprendre-la-propriete-intellectuelle/les-enjeux-de-la-propriete-intellectuelle/quest-ce-que-la-propriete-industrielle (consulté le 17/08/2019)

[790] BRONZO N., *Propriété intellectuelle et valorisation des résultats de la recherche publique*, Thèse Droit, Université Aix-Marseille, 2011

[791] Sur les difficultés à appréhender une unicité dans l'*open data* : DENIS J.D., GOËTA S., *Les facettes de l'Open Data : émergence, fondements et travail en coulisses*, MENGER P-M., PAYE S., *Big data et traçabilité numérique. Les sciences sociales face à la quantification massive des individus*, Conférences du Collège de France, Collège de France, 2017

[792] Revue Lamy Droit de l'Immatériel, n°104, 1er mai 2014

[793] https://elysee.fr, 25 avril 2014

[794] FAVRO K., *Les données non personnelles : un nouvel objet juridique*, précité : « Derrière la distinction données personnelles/non personnelles, se cache une approche de la donnée par l'éthique, car le principe de libre circulation ne vise pas le partage de toutes les données, mais celles que l'on qualifie de « propres » complètes, intègres, disponibles, et utiles à l'ensemble de la société ».

d'interopérabilité ou encore de transparence pure dans la sélection du jeu des données, interrogent certaines matières, la protection des données personnelles, mais aussi des questions inhérentes aux gestions de droit de propriété intellectuelle, en particulier le droit des logiciels et des bases de données.

353. Pour faire un lien avec les problématiques précédentes, nous pouvons citer une consultation publique, formalisée entre la CNIL et la CADA[795], sur les conditions de publication et de réutilisation de données publiques ; les premières recommandations issues de ce guide pratique, nous indique que la diffusion de données publiques doit répondre à plusieurs caractéristiques :

- Que par base de données, on entend un recueil d'œuvre, de données, ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen ;

- Que les bases de données doivent être mises à jour de façon régulière ;

- Que les données concernées doivent présenter un intérêt économique, social, sanitaire ou environnemental.

À notre sens, c'est à raison que la *blockchain* doit être encouragée pour l'ouverture de données publiques telles que celles présentes, par exemple au sein du RCS : une telle technologie permet de satisfaire les différents critères énoncés par la CNIL et la CADA. En effet, une *blockchain* permet la constitution et l'organisation de données, individuellement accessibles, et à ce titre, elle répond, à notre sens, à une base de données telle que définie par le Code de la propriété intellectuelle[796]. De plus, une *blockchain* permettant l'alimentation, de façon régulière et sécurisée de cette base de données, le second critère nous semble être respecté (principes d'une *blockchain* permissionnée). Enfin, il n'a pas en effet lieu de contester l'intérêt économique (et même, dans une certaine mesure, social) des données, ici, du RCS. L'utilisation d'une *blockchain* permet ainsi d'assurer une pérennité des données visées, tout en garantissant leur accès et la traçabilité des actions réalisées sur elles.

[795] https://www.cnil.fr/sites/default/files/atoms/files/guide_open_data.pdf (consulté le 24/11/2020)
[796] Cf. *Supra*, p.142 et suiv.

Par ailleurs, s'agissant du format de diffusion des données, caractère indispensable à un *open data*, la *blockchain* ici utilisée est basée sur la *blockchain* Hyperlegder[797] à savoir un format *open source*, et réutilisable en l'état (même si une interrogation demeure sur la gestion des différents droits de propriété intellectuelle, interrogation découlant particulièrement de la gestion contractuelle réalisée dans le cadre des travaux réalisés entre les différents greffes concernés et IBM - concepteur d'un POC). En rapide conclusion sur ce POC, et pour revenir au sens même de l'*open data*, à savoir la diffusion libre, et accessible, dans un format permettant la réutilisation et la participation, la technologie *blockchain* demeure même un atout pour ces caractéristiques intrinsèques, à condition qu'elle soit utilisée non pas dans une approche au bénéfice d'une personne unique, mais plutôt dans le cadre d'une « conjonction de bénéfices tangibles pour les différents acteurs impliqués dans l'écosystème[798] ».

Également, dans un cadre propre à la protection des données non personnelles, la *blockchain*, en raison de ses caractéristiques techniques s'agissant de la fiabilité et de l'accès aux données contenues présente d'ailleurs un intérêt fort pour tout producteur et hébergeur de données. L'hégémonie actuelle des services d'informatique en nuage (*cloud*[799]), en particulier pour l'hébergement des données a pu provoquer des questionnements sur la comptabilité avec les exigences de localisation des données. L'utilisation de *cloud*, en particulier pour les données issues de l'administration ont pu d'ores et déjà trouver des incertitudes, par exemple, pour les données relevant des trésors nationaux[800]. En effet, il faut considérer que toute archive publique est un trésor national, conformément à la loi[801], et avant l'entrée en vigueur du RGNP, tout trésor national ne pouvait être conservé que sur le territoire douanier français, excluant ainsi tout stockage dans un *cloud*.

Or, avec l'entrée en vigueur du RGNP, qui prévoit l'interdiction des exigences de localisation des données hormis pour des motifs de sécurité publique, le stockage des données

---

[797] https://fr.wikipedia.org/wiki/Hyperledger ; "Hyperlegder est une plateforme open source de développement de *blockchain*. Ce projet a été initié en déc. 2015 par la fondation Linux. Le développement s'y fait essentiellement en langage Go" (consulté le 12/09/2017)

[798] DE COËTLOGON P., DURAND M., JEANTET M., GÉNON C., RAMON R. Et al. P, *Les technologies blockchain au service du secteur public*, Rapport de recherche, Université de Lille juin 2021

[799] Ou *Cloud computing* ; Le *cloud* computing (en français, « informatique dans les nuages ») fait référence à l'utilisation de la mémoire et des capacités de calcul des ordinateurs et des serveurs répartis dans le monde entier et liés par un réseau. Les applications et les données ne se trouvent plus sur un ordinateur déterminé mais dans un nuage (*cloud*) composé de nombreux serveurs distants interconnectés, https://www.cnil.fr/fr/definition/*cloud*-computing, consulté le 01/10/2021.

[800] Assemblée nationale, Question n°7619, 24 avril 2018 ; JOAN 9 juil. 2019, p.6465

[801] Art. L111-1, Code du patrimoine

dans un *cloud* peut être utilisé, même en cas de non-localisation précise des données[802]. Cette notion d'archive publique, dans le sens où il s'agit notamment de données produites par des opérateurs publics, n'est pas sans rappeler les problématiques liées à l'*open data*, et doit d'ailleurs pouvoir faire partie des éléments à prendre en compte dans toute analyse sur ce sujet. Invitant tout responsable de projet *open data* à ne pas seulement considérer les régimes propres à l'*open data*, mais bien à prendre en compte, de façon extensive, l'ensemble du droit de la protection des données (personnelles ou non).

Enfin, il doit être rappelé que l'*open data* est notamment né de la nécessaire protection de l'usager contre les « menaces de l'administration informatique, contre l'opacité de ses décisions et les risques d'arbitraire[803]», rappelant ainsi l'idée même du concept de protection des données, il en reste que ce dernier entend bien également assurer le respect de cadres fondamentaux[804].

354. En tout état de cause, la mise en application du RGPD, en parallèle d'une économie de la donnée toujours plus forte[805], font renaître des problématiques quant à la mise en place d'un droit de propriété sur les données[806]. L'adoption du RGNP, en ce qu'il peut être considéré comme instituant une 5ème liberté de circulation au sein de l'UE[807], a également permis la tenue de développements s'agissant de la difficulté de créer un tel droit de propriété, tant les risques et lacunes sur sa création sont importants[808]. En effet, de manière parallèle aux débats sur le partage des données[809], le débat sur la construction d'un droit de propriété sur les données peut trouver des raisons pour[810] ou contre[811], toujours est-il que la *blockchain* peut avoir le mérite d'être un argument pour une création d'un droit de propriété. En effet, permettant une traçabilité et un contrôle sur les données partagées, le caractère non rival d'une

---

[802] On relèvera que l'article L111-7 du Code du patrimoine, précisant que les trésors nationaux peuvent être exportés, sous autorisation du territoire douanier, n'a pas été mis à jour suite à l'adoption du RGNP (au 20/09/2021).

[803] PADOVA Y., *Entre patrimonialité et injonction au partage : la donnée écartelée ?*, Revue Lamy Droit de l'Immatériel, n°155, 1er janv. 2019, précité

[804] Cf. *Supra* p.198 et suiv.

[805] ISAAC H. précité

[806] PADOVA Y., précité

[807] BOEV I., *Le nouveau règlement : un 5e principe de libre circulation ?*, Dalloz IP/IT 2020, p.223

[808] CARRE S., *Libre circulation des données, propriété et droit à l'information : à propos du règlement (UE) 2018/1807 du 14 nov.2018*, Dalloz IP/IT 2020, p.228

[809] PADOVA Y., précité

[810] Cf. note n°640

[811] Contre l'idée de patrimonialité, comme pouvant créer de nouveaux systèmes discriminants et inégalitaires (cf. ELVY T.-A., *Paying for Privacy and personal data econom*, Columbia Law Review, Vol. 117, nº 6, Oct. 2017, p. 1405 et s.

donnée peut être contrebalancé par l'utilisation d'une *blockchain*, en raison des possibilités de contrôle et de suivi de l'exploitation de la donnée, facilitant dès lors une monétisation des données[812].

Cette problématique trouve sens dans l'étude de la protection des données non personnelles, dans le sens où la règlementation applicable trouvera application sans préjudice du RGPD en cas de connexité forte entre données personnelles et non personnelles[813]. Toutefois, même si la *blockchain* faciliterait une telle monétisation[814]. Il reste qu'une telle monétisation apparaît comme risquée[815], la facilitation de la maîtrise des données personnelles créant donc bien une dichotomie entre la maîtrise et la propriété doit être plutôt renforcée, notamment avec la mise en place de cadre fondamentaux.

§2 : La libéralisation contrôlée des données grâce à la *blockchain*

355. Les initiatives législatives sur la gestion des données personnelles ou non personnelles, si elles peuvent mettent l'accent sur la protection des libertés individuelles, ont également pour but de favoriser un libre échange des données. Pourtant, ce libre échange ne peut se faire en occultant certains cadres fondamentaux. Cette notion fait écho, de manière large, à l'existence de principes qui, sans être des libertés ou droits fondamentaux[816], doivent faire l'objet de protections. Si la présente étude n'a pas vocation à établir et débattre de manière fondamentale des différentes classifications permettant d'analyser les régimes applicables à ces principes, il reste que le RGNP, mais aussi une série de considérations autour de la donnée non personnelle trouvent écho grâce à la *blockchain*. La notion de protection, prise dans sa conception de mesure contre un risque identifié, et appliqué à l'étude de la *blockchain*, permet de mettre en avant, au sein de la protection des données non personnelles, plusieurs axes de protection, qui ne pourraient être exhaustifs dans le cadre de cette étude. Certains sont directement issus du

[812] Sur les difficultés de tarification de l'usage et de tarification des données, voir : GUICHARDAZ R, PÉNIN J., *L'économie de la réutilisation des données (non personnelles*), Dalloz IP/IT 2020, p.218

[813] Cf. *Infra*, p.207

[814] JOST C., *Monétisation des données : un nouveau modèle économique en préparation,* Archimag, 02/10/2019, disponible à : https://www.archimag.com/univers-data/2019/10/02/monetiser-donnees-nouveau-modele-economique-prepare (consulté le 04/10/2019)

[815] DESCHANEL C., *L'instauration d'un droit de propriété des données personnelles : vrai danger ou fausse utilité ?*, Revue Lamy Droit de l'Immatériel, n°156, 1er fév. 2019

[816] C'est-à-dire des droits inhérents à la personne humaine, établie notamment par la Déclaration des Droits de l'Homme et du Citoyen de 1789 (voir notamment : https://www.vie-publique.fr/fiches/23865-libertes-et-droits-fondamentaux-de-quoi-sagit-il, consulté le 26/06/2020).

RGNP, cœur de la présente section, mais une étude fonctionnelle du droit de la donnée implique de prendre en compte des aspects issus du droit de la concurrence (tant la protection des données personnelles a notamment pour but de favoriser un marché de libre échange sur les données). Puis, dans une logique adéquate à l'étude de la *blockchain*, à la revue des limites nées de la technique.

S'agissant des cadres fondamentaux à prendre en compte dans le cadre de la protection des données non personnelles, le RGNP met l'accent sur deux notions : la notion de disponibilité et la notion de portage des données.

356. La notion de disponibilité est à la base empruntée du vocabulaire informatique[817] et est donc un terme à vocation technique, portant en particulier sur la sécurité des systèmes d'information. Dans un jargon plus technique, la disponibilité de la donnée fait référence à un état opérationnel de cette donnée par rapport aux attentes, c'est donc un état de performance[818]. Cette exigence de disponibilité, dans le cadre du RGNP, porte aussi sur une obligation de disponibilité des données pour les autorités compétentes[819]. Ainsi, il est possible de considérer une dichotomie sur le terme employé. S'il est empreint de sécurité informatique en premier lieu, l'un des objectifs du RGNP est également d'assurer un potentiel contrôle sur le libre flux des données qu'il souhaite mettre en place. Il aurait été peut-être plus clair de parler de « mise à disposition » plutôt que de disponibilité, tant cette notion avait déjà pu faire l'objet de dispositions dans le RGPD, qui plus est dans le sens précédemment illustré[820]. Toutefois, s'agissant de cette « disponibilité », le règlement précise ainsi que les autorités compétentes pourront demander la relocalisation des données dans le cadre de mesures provisoires, permettant à ces dernières d'accéder à des données dans le cadre de l'exécution de pouvoirs officiels.

Une logique est palpable, celle de permettre à des autorités de contrôle de saisir ou même geler des données sur son territoire, le temps d'investigations plus poussées[821].

---

[817] GHERNAOUTI S., *Sécurité informatique et réseaux*, Paris, Dunod, 2013

[818] https://fr.wikipedia.org/wiki/Disponibilit%C3%A9 (consulté le 06/08/2020)

[819] Art. 5, RGNP

[820] Art. 32, RGPD, relatif à la sécurité du traitement de données personnelles, imposant au responsable de traitement de prendre les mesures adéquates pour assurer la disponibilité des données personnelles faisant l'objet d'un traitement.

[821] Cette logique ayant sens, notamment au regard des pouvoirs des autorités de contrôle dans le cadre de l'application du RGPD. En effet, les autorités de contrôle ont notamment le pouvoir de saisir mais aussi suspendre tout traitement de données personnelles (art. 58, RGPD).

Néanmoins, avec la *blockchain*, une potentielle lacune dans la mise à disposition peut être perceptible dans le cadre d'une application de cet article. La relocalisation des données ne fait que référence à une appréciation purement géographique (et qui vient donc en exception avec l'interdiction des mesures de localisation des données), et passe outre les exigences techniques de cette relocalisation ; doit-elle être exclusive ? Doit-elle seulement permette un accès aux autorités de contrôle, peu importe l'existence ou non de données répliquées dans d'autres lieux ? Cette question de location est importante dans le cadre de l'utilisation d'une *blockchain*. En effet, l'architecture des données retenues dans une *blockchain* permet une multi-localisation des données à un instant T, chaque donnée devant faire l'objet d'un enregistrement de la part des mineurs, une fois validée par la méthode de consensus, chaque donnée se trouve répliquée auprès de l'ensemble des mineurs participants.

357. La notion de portage des données[822], outre l'encouragement pour l'élaboration de codes de conduites, demeure un point important du RGNP, en ce qu'il encourage et facilite le libre flux des données. Au sein des dispositions concernant le portage des données, plusieurs analyses applicables à la *blockchain* peuvent être faites. Premièrement, concernant l'utilisation de formats « structurés, usuels et lisibles par machine[823] », encouragés par le RGNP. Il est possible de percevoir un nouveau parallèle avec le RGPD, en ce qu'il porte sur le droit à la portabilité des données[824]. Si la *blockchain* a été entendue, par la CNIL, comme ne créant pas d'obstacle technique à la portabilité[825], alors aucun obstacle ne devrait être caractérisé pour des données non personnelles. Également, les dispositions du RGNP sur la portabilité contiennent également des dispositions sur des obligations de conseil et de transparence des mesures techniques employées, notamment en cas de transfert ou de réversibilité des données[826]. Cette exigence de conseil, et l'incitation, à travers la création d'un code de conduite encadrant ses aspects, peuvent trouver un nouveau souffle d'application avec la *blockchain*.

On pourra rappeler que la *blockchain* permet une réplication des données auprès de l'ensemble des participants au réseau, et si la réversibilité comprend, en d'autres mots, les

[822] Art. 6, RGNP
[823] Art. 6, 1. a), RGNP
[824] Art. 20, RGPD
[825] CNIL, « Premiers éléments d'analyse », précité
[826] NB : si la réversibilité n'est pas expressément mentionnée dans le RGNP, elle est pourtant directement visée grâce à l'expression « rapatrier (ses données) vers ses propres systèmes informatiques ».

moyens permettant de « reprendre le contrôle exclusif de ses données[827] », la *blockchain* permet au contraire de réduire les cas où il y a une perte de contrôle sur ces données. En effet, de par cette réplication, un opérateur souhaitant garder le contrôle de ses données pourra être participant à la *blockchain* qu'il utilise, et ce, même si ce n'est pas lui qui est à l'initiative de la mise en place d'une telle architecture. Dès lors, même en cas de défaillance d'une autre partie, il conservera une copie des différentes données, et gardera ainsi la possibilité technique de réexportation de ces données. En d'autres termes, la *blockchain*, dans le cadre des codes de conduite encouragés par le RGNP, demeure un outil fort et particulièrement opportun.

358. L'inscription, comme principe fondamental sauvegardé par l'Union, de la libre circulation des données a pour but de renforcer une « concurrence effective sur les marchés pour les services de traitement des données[828] ». L'intention libérale l'Union, en ce qu'elle concerne le marché des données non personnelles, affirmée avec l'adoption du RGNP, se voit renforcée par le principe de libre flux des données. Or, une lacune potentielle de ce règlement est de ne faire aucun *distinguo* quant aux usages de ces données, cette lacune ayant pour conséquence de permettre une « plénitude d'exploitation sans véritables limites [829] ». Néanmoins, si la libre circulation permet effectivement un tel libre flux de données, ce n'est qu'au regard de la protection des données non personnelles. Dans une telle situation, une telle affirmation n'est pas sans poser de problèmes quant à une application extensive, prise dans une volonté exhaustive, car elle semble ignorer d'autres pans juridiques applicables. Face à ces « plénitudes d'exploitation[830] », le RGNP semble adopter la technique de la régulation, à l'opposé d'une réglementation. Comme le souligne le professeur Supiot, « règlementer c'est dicter les règles de l'extérieur, tandis que réguler, c'est faire observer les règles nécessaires au fonctionnement homéostatique d'une organisation[831] ».

359. C'est l'objet des différents codes de conduite et bonnes pratiques, encouragés par le RGNP, notamment en réaction au fait que l'information « est de plus en plus souvent traitée comme un bien immatériel appropriable[832] », avec les revers que cette appropriation peut

[827] VIVANT M., précité
[828] Considérant 29, RGNP
[829] BOUGEARD A. *Les dispositions relatives à l'accès et au portage des données : code de conduite et bonnes pratiques*, Dalloz IP/IT 2020, p.408
[830] *Ibid.*
[831] SUPIOT A. *Homo juridicus, essai sur la fonction anthropologique du Droit*, Essais, Editions du Seuil, 2005
[832] *Ibid.*

revêtir, notamment le renforcement d'entreprises monopolistiques, susceptibles d'abus. Néanmoins, les règles de la concurrence, si elles ne sont pas directement mentionnées par les articles du RGNP, planent sur l'ensemble de ses dispositions[833].

Au-delà, et de manière logique, trouveront d'ailleurs applications les différentes règles relatives au droit européen de la concurrence. Plusieurs séries d'obstacles au libre flux de données peuvent être mentionnés : les obstacles techniques et les obstacles comportementaux et contractuels[834]. Si la régulation par des techniques de conformité peut être utilisée, ainsi que les études classiques d'abus de position dominante en présence d'abus d'exclusion ou d'exploitation d'un marché, il reste que la *blockchain* peut être un outil en défaveur d'un marché concurrentiel libre, notamment face à des ententes illicites[835].

360. Rappelons que le fonctionnement d'une *blockchain* reste particulier compte tenu de sa capacité, d'une part, à pouvoir être transnational, et d'autre part, en liant toute une série d'acteurs identifiés de manière pseudonymes. Également, la *blockchain* peut être support de *smart contracts*, à savoir des opérateurs informatiques logiques, permettant l'exécution automatique de conditions contractuelles préétablies par un ou plusieurs parties. Ce caractère automatique peut présenter des inconvénients à plusieurs égards par rapport au droit de la concurrence. D'une part, c'est un caractère complètement novateur. En effet, le plus souvent, les ententes sont caractérisées par des accords ou des pratiques concertées entre personnes. Or, l'accord peut être complètement déporté de manière purement technique grâce à la *blockchain*. En ce sens, le caractère décentralisé, l'existence de la pseudonymisation D'autre part, le caractère automatique emporte *de facto* exécution des conditions préalablement réalisées, si bien qu'une fois un *smart contract* en cours d'exécution, une modification technique sera forcément nécessaire pour arrêter son fonctionnement (à défaut, il continuera d'être exécuté dans les conditions préalablement définies) ou, dans le cas où un tel protocole est utilisé à des fins d'entente, une simple modification de ce dernier permettra d'avoir un caractère « dynamique[836] ». Ce caractère écrivant la potentielle adaptation d'une entente de manière

[833] Notamment Considérant 3, 7, 29 du RGNP

[834] ÉRÉSÉO N., *Libre circulation des données et droit de la concurrence (à propos du règlement du 14 nov.2018 relatif à la libre circulation des données non personnelles)*, Dalloz IP/IT 2020, p.414

[835] On pourra se borner, dans le cadre de la présente étude, à rappeler que les ententes anticoncurrentielles sont listées, de manière non exhaustive, par l'article L420-1 du Code de commerce.

[836] SCHREPEL T., précité.

continue, permettant alors un « nombre presque infini de possibilités évolutives d'infractions au droit de la concurrence[837] ».

Néanmoins, force est de constater que le droit de la concurrence, en ce qu'il concerne la prohibition des ententes anticoncurrentielles ne peut consacrer une exhaustivité de telles pratiques. En conséquence, même si l'usage de la *blockchain* peut permettre la mise en place d'une pratique prohibée, en reste qu'elle est déjà prise en compte par les règles en vigueur.

Une fracture méthodologique peut être relevée. En effet, si l'Autorité de la concurrence utilise un faisceau d'indices[838] afin de caractériser la pratique anti concurrentielle, les caractères techniques de la *blockchain*, pris comme élément novateur ou même disruptif, risquent de créer certaines difficultés pour leur appréciation, et alors, devenir un risque pour la libre concurrence, compte tenu du fait qu'une « violation du droit de la concurrence n'est, en pratique, jamais tirée de la violation d'une disposition légale ou réglementaire extérieure au droit de la concurrence[839] ». En définitive, si la *blockchain* présente des intérêts certains pour la protection des données personnelles, la non-perméabilité et l'absence de raisonnement global sur l'exploitation de données en raison de la non-compréhension de caractéristiques techniques particulières peuvent conduire à certaines incertitudes d'articulation de régimes juridiques ayant vocation à créer des cadres fondamentaux (étant considéré, ici, le cadre fondamental de la libre concurrence).

361. Les implications techniques de la *blockchain*, dans le cadre du respect de cadres fondamentaux comme attribut de la protection des données non personnelles présente néanmoins des limites fortes. La *blockchain* n'a pas vocation à s'appliquer de manière homogène et spécialisée pour des données personnelles ou non personnelles. En l'occurrence, la matière première d'une *blockchain* est la donnée, et plus précisément, le *hash* d'une donnée[840]. Or, l'utilisation d'une fonction de hachage donnera toujours un résultat similaire, qu'il s'agisse d'une donnée personnelle ou non. Ainsi, le résultat d'un hachage d'une donnée

[837] *Ibid.*

[838] ATSARIAS-DUMAS S., *Le contrôle du contrat par l'Autorité de la concurrence*, AJ Contrat 2020, p.474

[839] ÉRÉSÉO N., précité.

[840] Pour rappel, le *hash* d'une donnée est un condensa informatique résultant de l'utilisation d'une fonction de hachage, et possède notamment la caractéristique technique d'être une donnée calibrée, dont le format sera toujours le même au sein d'une *blockchain*.

personnelle et d'une donnée non personnelle sera sensiblement le même[841]. De surcroît, la caractéristique d'une telle fonction est qu'il est techniquement impossible de revenir à l'état d'origine d'un *hash*, au point qu'il est impossible de savoir la nature de la donnée ayant fait l'objet d'un *hash*[842]. Dès lors, il doit être déterminé avec certitude l'application ou non des régimes de protection des données personnelles ou non personnelles. En réalité, le RGNP présente une réponse au sein de son article 2[843]. Ce dernier dispose qu'en cas de présence de données personnelles « inextricablement liées, le présent règlement s'application sans préjudice de l'application du règlement (UE) 2016/679. Ces données inextricablement liées pouvant alors être considérées comme « données composites[844] ».

Cette réponse paraît peu satisfaisante face aux difficultés d'identification de telles données. Au-delà de cette catégorie de données, illustrée avec l'adoption du RGNP, le débat sur la nature même des données et la volonté de caractériser des ensembles est nécessaire. En effet, s'il est possible de créer un premier clivage entre données personnelles et non personnelles, cette catégorisation paraît comme peu satisfaisante, comme le démontre une caractérisation nécessaire de « données composites[845] », à la fois personnelles et non personnelles. Également, de manière plus affinée, les données personnelles peuvent être identifiées comme sensibles[846] (sachant que le RGPD ne les désigne pas ainsi, mais seulement comme « catégories particulières de données »), conférant alors une valeur particulière à des sous-catégories de données personnelles. Il est également possible de considérer d'autres typologies de données, qui pourront être caractérisées soit comme des données personnelles

[841] Par exemple, avec l'utilisation d'une fonction de hachage, il est possible d'arriver aux résultats suivants (ici un SHA256) :
- le *hash* de la donnée « Thibaut Labbé » est :
39518F7E16F307567F3202BB83C979CCD6D4A4AA837CCCE9745770C8722665E6
- le *hash* de la donnée « *Blockchain* » est :
EF7797E13D3A75526946A3BCF00DAEC9FC9C9C4D51DDC7CC5DF888F74DD434D1

Ces deux *hash* comportant chacun 64 caractères, il est particulièrement difficile d'y percevoir la nature de donnée personnelle ou non ; en tout état de cause, une telle donnée pourra être qualifiée de pseudonyme en cas de possibilité de réidentification, et à défaut, de donnée non personnelle.

[842] Il convient de préciser que cette affirmation n'est vraie qu'en présence de fonctions de hachage reconnues d'un point de vue cryptographique. L'inversion d'une fonction de hachage reste techniquement possible en cas de fonction de hachage faiblement chiffrée.

[843] Art. 2, 2., RGNP

[844] ZORN C., précité.

[845] *Ibid.*

[846] Art. 9, RGPD

ou non, comme peut en témoigner l'exemple des données de connexion[847]. Il reste alors l'apparent problème insoluble d'identification utile des données faisant l'objet d'un traitement.

En réalité, il convient d'instituer une nécessaire identification des données personnelles ou non personnelles faisant l'objet d'un traitement de manière préparatoire afin de pouvoir faire application des règles applicables de manière distributive. Ainsi, la problématique technique liée à la *blockchain* peut se résoudre de manière anticipée. La connaissance, en amont, des données utilisées, permet ainsi d'exploiter plus efficacement ces dernières, et favorisent ainsi un libre échange numérique, tout en cadrant ce marché économique grandissant.

[847] Considérant 30, RGPD ; les données de connexion, quand elles sont combinées à des identifiants uniques peuvent permettre d'identifier des personnes physiques, et sont donc, à ce titre, considérées comme données personnelles.

Conclusion du Chapitre 1

362. En synthèse, et s'il convient de constater d'apparentes contradictions dans la construction des régimes de protection des données personnelles[848], la construction d'une approche protectionniste de la donnée doit prendre en compte notamment des impératifs de sécurité informatique, notamment pour assurer la disponibilité des données personnelles ou non personnelles. Impératifs considérés d'ailleurs comme axe stratégique de la politique européenne[849]. Cette prise en compte de la sécurité doit être un complément naturel d'une approche fonctionnelle du droit de la donnée. Si la protection des données personnelles est « un droit bousculé par la technique[850] », il pourrait être plus juste de dire que la protection des données est rattachée à la technique. Une mauvaise compréhension entre techniciens et juriste peut conduire à des situations insolubles, vers une « interdiction en droit d'une opération techniquement indispensable, ou l'obligation en droit d'une opération techniquement impossible[851] », et le droit des données, et par rattachement, l'étude de la *blockchain*, nécessite une collaboration entre ces deux milieux.

[848] FAVRO K., précitée

[849] Conseil de l'UE, *Cybersécurité : le Conseil adopte des conclusions sur la stratégie de cybersécurité de l'UE,* Communiqué de presse, 22 mars 2021

[850] LE CLAINCHE J., *Données personnelles, vie privée, et non-discrimination : des protections complémentaires, une convergence nécessaire*, Revue Lamy Droit de l'Immatériel, n°90, 1er fév. 2013

[851] GOSSA J., *Les données non personnelles : un tech checking*, *Dalloz IP/IT*, Dalloz, 2020, pp.213-217

Chapitre 2 : Complémentarité naturelle entre droit et technique

363. Une approche fonctionnelle du droit de la donnée, outre la caractérisation potentielle d'une matière à part entière, au même titre que le droit des logiciels ou des bases de données, revêt une particularité liée à la nature même de son objet. En effet, si la protection et l'exploitation de données peuvent être vues d'un œil purement juridique, ce seraient en occultant une part technique indispensable. Abordée notamment avec la question des *smart contracts*, et avec la nécessité d'avoir des juristes capables d'appréhender une version / traduction informatique du droit. Au-delà du débat « *Code is Law* » *versus* « *Law is Code* », une approche pourrait « *Law by Code* », dans le sens où l'expression de loi, qui doit rester (dans une conception classique) claire, intelligible et surtout accessible, peut en réalité trouver son expression dans le Code. La loi, aussi bien souveraine (dans le sens où elle trouve son origine dans le pouvoir étatique) que contractuelle (« la loi des parties ») trouve en fait application, de manière ordonnée, dans le code. Elle se trouve ainsi aussi bien dans le *smart contract* (la mise en place de conditions contractuelles automatisées de manière informatique), ou dans la sécurisation des échanges électronique (dans laquelle se retrouvent des obligations de sécurité, renforcées par des impératifs de gouvernance et de gestion des données). En réalité, une approche hybride entre technique et droit trouve déjà de premiers échos dans la sécurisation des échanges électroniques (Section 1), qui a pu faire l'objet de développements bien avant la démocratisation de la *blockchain*, au point qu'il existe plus généralement une tendance vers une atténuation des oppositions entre droit et technique (Section 2).

Section 1 : L'originelle sécurisation des échanges électroniques

364. Un échange d'informations peut se faire d'une façon particulièrement simple : un transport de documents. Or, les risques liés à un tel transport peuvent être la perte, la destruction, ou même la corruption de ces documents par un opérateur malveillant. Le système de preuve, et notamment le régime de l'acte authentique a notamment pour but de sécuriser

des échanges, en conférant une valeur probante forte aux échanges qu'il peut retranscrire[852]. L'intérêt d'un tel acte, outre sa valeur probatoire, peut être donc compris comme une retranscription fidèle, quasi incorruptible, d'informations. Avec la reconnaissance de l'équivalence de l'écrit classique avec l'écrit électronique[853], certaines garanties ont dû être apportées afin de pouvoir l'admettre à titre de preuve, soit quand celle-ci est libre, soit quand la loi impose un certain formalisme. En tout état de cause, des mesures de sécurisation, adaptées au numérique, sont nécessaires afin d'admettre cette équivalence. La sécurisation, nom commun tiré du verbe sécuriser renvoie à une notion d'impression de sécurité, mais renvoie également au fait de donner un caractère sécurisé à quelque chose, qu'il s'agisse de moyens techniques, mais aussi juridiques.

365. Dès l'Antiquité, l'une des premières techniques de chiffrement a été utilisée par Jules César, qui utilisait une technique de substitution alphabétique[854], dans le but de sécuriser et de garantir la fiabilité de ses échanges. Depuis, les techniques de chiffrement ont pu évoluer[855], et les intérêts pour ces techniques sont nombreux, de la préservation du secret des messages au tournant décisif d'un conflit armé[856]. Les échanges électroniques renvoyant simplement à l'utilisation de moyens de télécommunications électroniques à des fins de communication. Ainsi, de manière littérale, la sécurisation des échanges électroniques renvoie alors aux méthodes permettant de sécuriser les communications utilisant les technologies de l'information entre personnes. Il est possible d'y voir une idée tautologique, dans le sens où une communication électronique doit toujours être sécurisée afin d'être fiable. À défaut, une communication électronique pouvant être potentiellement erronée, falsifiée, ou altérée ne saurait être acceptée comme équivalente à une communication classique.

[852] Art. 1369, C. Civ.
[853] Art. 1366, C. Civ.
[854] https://fr.wikipedia.org/wiki/Chiffrement_par_d%C3%A9calage (consulté le 15/09/2018)
[855] MERCIER D-J., *Du chiffrement de César à la mathématique de la carte bancaire*, *Repères IREM*, 2002, pp.59-90
[856] Est fait référence ici à la machine de chiffrement Enigma, utilisée par l'Axe pendant la seconde guerre mondiale, dont le déchiffrement, par Allan Turing notamment, a marqué un tournant dans ce conflit.

366. Quand on aborde les questions de sécurité, on pense immédiatement à des termes comme « cybersécurité[857] », « cryptologie[858] » ou encore « chiffrement[859] ». Pourtant, les deux premiers sont bien distincts[860], et le troisième n'est qu'une partie du deuxième. Ainsi, faire l'étude de la cryptologie revient, en partie, à étudier le chiffrement. Dans le cadre de la présente étude, et dans une approche permettant d'appréhender une complémentarité entre droit et technique issue de la démocratisation de la *blockchain*, il revient à percevoir un encouragement des techniques de chiffrement mais surtout une tendance pour la création d'un régime de conformité pour la sécurité des systèmes d'information. La protection des réseaux et des systèmes d'information, devenus « le nerf de la croissance économique[861] », ne sont pas exempts d'aspects particuliers quant à la mise en œuvre de la responsabilité contractuelle ou délictuelle. À ce titre, il est possible de constater une tendance vers la conformité de la sécurité des systèmes d'information (§1), mais il reste important d'étudier les régimes de responsabilité informatique face à la *blockchain (§2).*

§1 : Une tendance induite vers la conformité de la sécurité des systèmes d'information

367. De manière schématique, la cryptologie utilise les mathématiques, notamment les probabilités et les caractéristiques des nombres premiers afin de crypter un message, partant d'un texte dit « en clair » vers un texte « crypté[862] ».

[857] D'un point de vue européen, la cybersécurité est notamment visée par une stratégique de l'Union européenne (Communication conjointe au Parlement Européen, au Conseil, au Comité Économique et social européen et au Comité des régions - Stratégie de cybersécurité de l'Union européenne : un cyber espace ouvert, sûr, et sécurisé, Fév. 2013, JOIN(2013) 1 final), mais est également marqué par un récent règlement de 2019 (Règlement (UE) 2019/881 du Parlement Européen et du Conseil du 17 avril 2019, relatif à l'ENISA - l'agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n°526/2013 (règlement sur la cybersécurité), dit règlement ENISA.

[858] La cryptologie est, étymologiquement la science du secret.

[859] Le chiffrement est un procédé mathématique permettant la confidentialité d'une information.

[860] La cybersécurité peut être également définie comme les atteintes à la sécurité des systèmes et réseaux d'information du point de vue de la sécurité de l'état de ses installations ; FRAYSSINET E., *La cybercriminalité en mouvement*, Hermès, 2012

[861] Règlement ENISA, précité

[862] H. CORMEN T., *Algorithmes - Notions de bases*, DUNOND, 2013

Sans réaliser ici un historique de la cryptologie[863] et des différentes normes en vigueur sur les aspects abordant la cryptologie en droit français, dont l'étendue et les possibilités offertes seront abordées dans une partie ultérieure de la présente étude, il reste à noter une disposition importante, qui est l'article 30 de la LCEN[864]. Le « I » de cet article est limpide. Il a concrétisé la libéralisation des outils cryptographiques. Sachant que l'article 29 de la LCEN définit le moyen de cryptologie comme « tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète ».

Il reste que malgré cette libéralisation des moyens cryptographiques, leur importation ou exportation restent soumises à des obligations déclaratives auprès de l'ANSSI. La détermination de ces obligations déclaratives découle de la catégorie de produits cryptographiques visés[865], étant entendu que la plupart de ces outils sont considérés, sauf exception, comme étant à des biens à double usage (c'est-à-dire des biens pouvant présenter à la fois des applications civiles et militaires de haut niveau). On retrouve, dans la catégorie des biens grand public[866], des outils dont l'usage est exclusivement centré sur des fonctions d'authentification et de contrôle et d'intégrité, ou encore des produits conçus pour une utilisation purement personnelle. À ce titre, il conviendra alors de mentionner que la *blockchain*, en tant que technologie de stockage garantissant notamment une intégrité et une traçabilité des données ne devrait pas être concernée par les obligations déclaratives précitées.

368. S'agissant des garanties de sécurité d'une *blockchain*, un décret d'application du 24 décembre 2018 a fixé des garanties minimales de sécurité et de fiabilité des registres[867], dans une mesure propre à l'utilisation de la *blockchain* pour l'enregistrement de mouvement sur

[863] Loi n°2004-575, loi pour la confiance dans l'économique numérique du 21 juin 2004, dite loi LCEN, article 29, « On entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité.

On entend par prestation de cryptologie toute opération visant à la mise en œuvre, pour le compte d'autrui, de moyens de cryptologie. »

[864] Loi n°2004-575, précitée, article 30 I

[865] https://www.ssi.gouv.fr/administration/reglementation/controle-reglementaire-sur-la-cryptographie/demarches-a-accomplir/ (consulté le 29/05/2021)

[866] Décret n°2007-663 du 2 mai 2007 pris pour l'application des articles 30, 31 et 36 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et aux prestations de cryptologie

[867] Décret d'application n°2018-1226 du 24 déc. 2018, Journal Officiel du 26 Déc. 2018, texte n° 33

des titres financiers. Néanmoins, outre la mention « d'un plan de continuité d'activité actualisé comprenant notamment un dispositif externe de conservation périodique des données[868] », aucune autre indication de sécurité n'est listée par la loi. Si, d'une part, l'exhaustivité aurait pu être recherchée dans ce texte, c'est, d'autre part, la contradiction de ces mesures de sécurité avec les caractéristiques d'une *blockchain* qui peut être relevée. En effet, si un plan de continuité d'activité permet notamment de réagir en cas de crise et notamment d'indisponibilité des données, cela reste une mesure peu propice à une *blockchain* tant ses données sont normalement répliquées au sein de serveurs gérés par d'autres participants (à condition qu'il s'agisse d'une *blockchain* publique ou même hybride).

De plus, le dispositif externe de conservation périodique des données est tautologique dans le cadre d'une *blockchain*, étant donné qu'il s'agit de caractéristiques basiques d'un tel protocole (les données devant être partagées auprès d'une communauté de participants, et faisant l'objet d'un horodatage constant). Il reste qu'une obligation générale de conformité sur l'utilisation d'une telle technologie devrait être entendue, tant les particularités de la *blockchain* sont importantes. À ce titre, cela viendrait en complément d'une généralisation de cette obligation de conformité pour la sécurité informatique. En effet, l'un des objectifs de la certification de cybersécurité, prévue dans le règlement ENISA, est de garantir une « trace des données fonctions ou services qui ont été consultés, utilisés ou traités de toute autre façon, du moment où ils l'ont été et par qui[869] », mais aussi « faire en sorte qu'il soit possible de vérifier quels données, services ou fonctions ont été consultés, utilisés ou traités de toute autre façon, à quel moment et par qui[870] ».

369. Le règlement ENISA, invite le fabricant ou le fournisseur de produits TIC à entrer dans un processus d'autoévaluation de la conformité[871] en prenant pour état cible les schémas de certification de cybersécurité. Il convient de mentionner que seuls les produits, services ou processus TIC de faible risque peuvent être concernés par cette autoévaluation de conformité. La raison de cette exception est logique. L'évaluation et la certification de cybersécurité sont prévues pour des produits, systèmes ou processus TIC à haute valeur ajoutée, ou, autrement

[868] Art. R211-9-7, 2ème al. du CMF

[869] Art. 51, e), Règlement (UE) 2019/881 du Parlement Européen et du Conseil du 17 avril 2019, relatif à l'ENISA - l'agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n°526/2013 (règlement sur la cybersécurité), dit règlement ENISA

[870] Art. 51, f), Règlement ENIS, précité

[871] Art. 53, Règlement ENISA, précité

dit, ceux présentant des répercussions fortes en cas d'incidents[872]. Toutefois, cette auto-évaluation présente de nombreux bénéfices pour les entreprises pouvant et souhaitant la réaliser.

En amont, cette limite dans l'auto-évaluation est expliquée par l'importance de produits, services ou processus TIC dans le cadre d'une politique européenne de cybersécurité. Sont ici concernés, par exemple, les hébergeurs de données de santé ou encore les fournisseurs de connexion internet. Ce type d'opérateurs représentent des éléments essentiels du marché économique européen, dans le sens où les TIC sont aujourd'hui devenues « le nerf de la croissance et une ressource critique dont dépendant tous les secteurs économiques[873] ». Et à l'inverse, les opérateurs de faible importance ne devraient pas être concernés par ce type de certification, ne serait-ce que pour des raisons d'opportunité et de proportionnalité des mesures de sécurité à mettre en œuvre par elles.

370. Ce critère de proportionnalité des mesures de sécurité[874] a déjà été rappelé avec l'adoption du RGPD, et il ne convient pas d'imposer de deux façons différentes la mise en place de mesures de sécurité, alors qu'en pratique, un produit, service ou processus TIC permettra la réalisation de traitement de données personnelles. Pour autant, et compte tenu du nombre important d'entreprises reposant sur une disponibilité constante d'Internet, l'ouverture à la certification de cybersécurité[875] ou à défaut, l'incitation à l'autoévaluation en partant du référentiel de certification aurait eu comme effet de créer une distorsion concurrentielle dans les propositions de service.

371. Réserver la certification de cybersécurité à certaines entreprises pouvant s'analyser comme l'inscription d'une capacité de résilience à deux vitesses face aux impacts d'attaques informatiques. Plaçant d'un côté les entreprises capables d'accéder à la certification (et donc celles possédant un gage de qualité et de résilience sur les produits, services ou processus TIC) et d'un autre, celles ne pouvant démontrer leurs capacités à résister à des attaques informatiques, malgré la mise en œuvre de mesures de sécurité adéquates et pertinentes.

---

[872] Art. 52, Règlement ENISA, précité

[873] Communication conjointe au Parlement Européen, au Conseil, au Comité Économique et social européen et au Comité des régions - Stratégie de cybersécurité de l'Union européenne : un cyber espace ouvert, sûr, et sécurisé, Fév. 2013, JOIN (2013) 1 final, p. 2

[874] Art. 32, RGPD

[875] Dans une dimension applicable à la protection des données mais démontrant l'intérêt d'une certification, voir : TAMBOU O., précité.

Ainsi, les dispositions relatives à l'auto-évaluation semblent entrer en harmonie avec les dispositions du RGPD et du RGNP, invitant les entreprises à entrer dans une démarche de conformité sur des aspects complémentaires : la protection des données et la mise en œuvre de mesures de sécurité informatique. En pratique, et comme pour toute démarche de conformité, les acteurs souhaitant s'y conformer devront créer, entretenir et laisser à disposition des autorités de contrôle l'ensemble des documentations y afférents ainsi que toutes les « informations pertinentes relative à la conformité des produits TIC ou services TIC[876] ».

D'ailleurs, l'invitation, généralisée, effectuée par le règlement ENISA, à entrer dans une démarche de conformité aux règles de cybersécurité tient parfaitement sens dans la construction actuelle du droit de la conformité[877]. En conséquence, l'ensemble des développements relatifs à la démonstration de la conformité appliqués à la *blockchain* trouvent écho s'agissant de la sécurité informatique. En pratique, les intérêts de la *blockchain* sur la traçabilité, la vérification ou encore l'utilisation de données remplissent une partie des critères présents dans le schéma européen de certification[878].

372. L'intérêt de la cybersécurité, et donc de l'encouragement de l'utilisation de techniques issues de la cryptologie n'est pas sans incidence sur un débat de plus en plus actuel, portant sur la souveraineté numérique[879]. Si la notion de souveraineté fait écho à une puissance absolue[880], une fois appliquée à l'ère numérique, elle renvoie à une expression employée pour « désigner une forme de relégation provoquée par l'émergence de plateformes venant concurrencer les États et les difficultés rencontrées par ceux-ci pour asseoir leur autorité sur les réseaux, le tout sur fond d'un rapport de force constant avec les géants technologiques[881] ». Cette recherche d'autorité, à la fois interne et en réaction aux pouvoirs conséquents de ces géants doit passer par la mise en place de mesures propres à la sécurité informatique, notamment pour assurer une imperméabilité aux intrusions extérieurs et garantir une gouvernance autonome sur les données.

---

[876] Art. 53, Règlement ENISA

[877] Cf. *Supra*, p.206 et suiv.

[878] Art. 51, Règlement ENISA

[879] WATIN-AUGOUARD M., *La cybersécurité, enjeu de la souveraineté à l'ère numérique*, Dalloz IT/IP, 2021, p.130

[880] BODIN J., *Les six livres de la République*, 1576, Livre Premier, Chapitre VIII

[881] G'SELL F., *Remarques sur les aspects juridiques de la « souveraineté numérique »*, Revues des Juristes de Sciences Po n°19, Oct. 2020, 13

Ce n'était pas la première avancée au bénéfice du renforcement de la sécurité informatique des systèmes. Dès 1992, l'OCDE insistait pour la création de cadres généraux, applicables à toute entreprise, pour la sécurité des systèmes d'informations[882]. Également, pour faire un parallèle avec les développements portant sur les certifications, la norme ISO 27k mentionne que la « direction doit établir une politique de sécurité de l'information[883] », insistant ainsi pour un véritable management de la sécurité informatique au sein des entreprises. En ce sens également, il conviendra de noter que l'État français, en 2014, a réalisé une politique de sécurité des systèmes d'information, qui est, au demeurant, opposable[884]. En outre, de nombreux secteurs sont concernés aujourd'hui par des objectifs de sécurité informatique comme la finance[885]. Et de manière générale, la lutte contre la cybercriminalité vise à protéger contre toute infraction contre la confidentialité, l'intégrité ou encore la disponibilité des systèmes d'information font partie des moyens garantissant les droits fondamentaux compte tenu de leur inscription dans un « cyberespace » de plus en plus étendu[886].

373. Dès lors qu'un moyen de cryptologie est utilisé dans une base de données classique ou au sein d'un logiciel expert visant à installer une *blockchain*, son utilisation restera licite, ouvrant ainsi la possibilité d'utiliser de tels moyens à des fins de preuve ; la complexité liée à l'utilisation d'algorithmes informatiques de chiffrement poussés (tels que des protocoles SHA-2 [887] ou autres) n'étant pas encadrée spécifiquement pour leur utilisation au-delà d'une nécessaire gestion d'un état de conformité. D'ailleurs, si le droit de la preuve semble accueillir facilement la *blockchain*[888], l'objectif de tout procès est de convaincre le juge[889]. Ainsi, plus une technique de chiffrement sera réputée comme étant fiable, plus cette technique aura tendance à emporter la conviction du juge. En l'état actuel des techniques de chiffrement et de

[882] Recommandation du Conseil et annexe (lignes directrices régissant la sécurité des systèmes d'information), 26 nov.1992

[883] Norme ISO 27001 :2013, chapitre 5.2

[884] Article 193, Loi n° 2016-41 du 26 janv. 2016 de modernisation de notre système de santé (1), et Arrêté du 22 mars 2017 relatif au référentiel de sécurité applicable au Système national des données de santé

[885] AKSABI M., *Le droit financier au défi de l'IA et de la cybersécurité*, Revue Droit et patrimoine, 1 janv. 2020, n°298, pp.51-55

[886] CE, *Le numérique et les droits fondamentaux*, Étude annuelle 2014

[887] Le protocole SHA-2 regroupe en réalité plusieurs fonctions de hachage cryptographiques ; Federal Information Processing Standards (FIPS) Publication 180-1, Secure Hash, disponible à : https://csrc.nist.gov/publications/detail/fips/180/2/archive/2002-08-01 (consulté le 08/10/2021)

[888] Cf. *Supra*, p.60 et suiv.

[889] AMMAR D., *Preuve et vraisemblance. Contribution à l'étude de la preuve technologique*, RTD civ. 1993. 499

gestion de la preuve électronique, il reste que la *blockchain* reste une technologie à encourager. Pour autant, l'utilisation de la *blockchain* n'est pas exempte de régimes de responsabilité particuliers.

§2 : Les régimes de responsabilité informatique face à la *blockchain*

374. Le règlement ENISA, au-delà du fait qu'il précise en premier lieu les missions et le fonctionnement de cette agence européenne, a une dimension politique forte concernant la cybersécurité. Différents considérants du règlement appuient la volonté de faire de l'ENISA une autorité compétente et reconnues pour stimuler la cybersécurité et la mise en place d'un cadre informatique sécurisé européen. En effet, l'une des missions de l'ENISA est de mettre à disposition toute information utile[890] au public. Cette notion de public étant entendue largement par ces considérants ; sont visés les personnes physiques, mais aussi les TPE, PME, ou encore start-ups[891]. En réalité, un constat amer est réalisé, celui que la cybersécurité est avant tout une question humaine plus qu'une question purement technique[892]. C'est notamment pour ces raisons, à un échelon national, que l'ANSSI est aussi un acteur de la culture de la cybersécurité, auprès des entreprises mais aussi des citoyens[893].

Outre cet aspect pédagogique pour la cybersécurité, de manière connexe, la sensibilisation aux risques et aux obligations inhérentes à la protection des données (et donc aux principes, notamment, de *privacy by design* et de sécurité informatique) fait partie du RGPD. À cet effet, le droit positif a su mettre en place différents régimes de responsabilité, et grâce à la *blockchain* et à ses caractéristiques techniques, la sécurité informatique peut trouver de nouveaux échos juridiques face aux seules considérations techniques qu'elle peut avoir aujourd'hui.

La récente pandémie de coronavirus a également des impacts sur l'appréciation de la sécurité informatique en entreprise[894], et malheureusement la *blockchain* n'est pas inconnue des attaques informatiques qui ont pu sévir pendant cette période. En l'espèce, de nombreuses

---

[890] Considérant 4, Règlement ENISA
[891] *Ibid.*
[892] Considérant 8, Règlement ENISA
[893] https://www.ssi.gouv.fr/agence/missions/lanssi-en-un-coup-doeil (consulté le 04/01/2020)
[894] QUÉMÉNER M., *Virus et pandémie numériques : actualités en matière de cyberattaques*, RPPI n°2, Oct. 2020, dossier 14

attaques informatiques (même avec la pandémie) reposent sur un nouveau type de virus informatique : le rançongiciel[895], dont la rançon est le plus souvent demandée en *Bitcoin*. Faut-il y voir un argument en défaveur de la *blockchain* ? Assurément pas. En effet, la *blockchain* ne reste qu'un outil, et l'utilisation d'un outil à des fins illicites ne saurait justifier une répression ou une régulation uniquement fondée sur l'outil en lui-même.

375. La LCEN a édicté un régime particulier de responsabilité pour les fournisseurs de prestation de cryptologie[896]. Ce régime de responsabilité ayant sens compte tenu des impératifs de protection des données transformées grâce à des procédés de cryptologie. Également, la LCEN précise l'interdiction des clauses exonératrices de responsabilité, dans une logique parallèle à l'arrêt « *Faurecia*[897] », quand celles-ci portent sur les obligations essentielles souscrites par un débiteur[898]. La détermination de ces obligations essentielles va de pair avec l'appréciation de la portée de l'engagement souscrit, portée qui s'apprécie *in concreto*, notamment en réalisant une appréciation concrète de la cohérence contractuelle et donc dans une approche globale, notamment sur la répartition des risques du contrat[899]. Étant précisé que la responsabilité pourra être écartée si l'utilisation d'une telle fonction dépasse les limites fixées à son utilisation[900].

Il reste qu'il convient alors de déterminer les obligations essentielles d'un contrat portant sur la mise en place d'une *blockchain*, en faisant application d'une appréciation globale et centrée sur la gestion des risques supportés par les différentes parties. Si la *blockchain* peut faire l'objet soit d'une implantation en interne, à savoir l'exécution d'un projet de manière classique au sein d'entreprise, mais surtout, la fourniture d'une architecture *blockchain* comme

---

[895] Ou *ransomware :* « un logiciel informatique malveillant, bloquant les données qui chiffre les fichiers contenus sur les ordinateurs et demande une rançon en échange d'une clé permettant de les déchiffrer »., cf. *Ibid.*

[896] Art. 32, LCEN : « Sauf à démontrer qu'elles n'ont commis aucune faute intentionnelle ou négligence, les personnes fournissant des prestations de cryptologie à des fins de confidentialité sont responsables au titre de ces prestations, nonobstant toute stipulation contractuelle contraire, du préjudice causé aux personnes leur confiant la gestion de leurs conventions secrètes en cas d'atteinte à l'intégrité, à la confidentialité ou à la disponibilité des données transformées à l'aide de ces conventions ».

[897] Cass. Com. 29 juin 2010, n° 09-11.841, voir notamment : RTD civ. 2010. 555, obs. FAGES B.

[898] On rappellera que cette jurisprudence a été codifiée par la réforme du droit des obligations de 2016, et est présente au sein de l'article 1170 du Code civil : « Tout clause qui prive de sa substance l'obligation essentielles du débiteur est réputée non écrite ».

[899] JOURDAIN P., *Clauses restrictives de responsabilité et obligation essentielles : une précision et des incertitudes*, RTD Civ. 2008, p.310

[900] Art. 33, 4°, LCEN, précitée

service (type BaaS) s'entend parfaitement et est même objet de services actuels[901]. Dès lors, comme apprécier les obligations essentielles dans un tel contrat de prestation de services ?

Rappelons que la *blockchain* permet l'enregistrement ou encore la traçabilité de données, mais peut également être considérée comme permettant la fourniture d'une prestation de cryptologie tant la *blockchain* repose sur de telles fonctionnalités pour fonctionner[902].

Conformément à une logique d'appréciation *in concreto*, réalisée de manière globale sur l'environnement contractuel, plusieurs questions doivent se poser. La première peut porter sur la valeur ajoutée qu'apporte une *blockchain* à une problématique posée pour laquelle le contrat et la prestation fournie apporte une réponse. Ensuite, une deuxième question peut porter sur la recherche de caractéristiques techniques : est-ce que le créancier de l'obligation recherche avant tout une disponibilité des données ou plutôt un horodatage électronique potentielle qualifié[903] ? Enfin, quelles sont les caractéristiques retenues par le prestataire sur la *blockchain* proposée ? En réalité, c'est une véritable approche en méthodologie projet plus que purement juridique, qu'il convient d'avoir pour une appréciation d'un projet *blockchain*.

376. Si certaines questions portent effectivement sur la portée ou la validité des données traitées par une *blockchain*, et donc sur des aspects juridiques, d'autres ne concernent que des aspects purement techniques (architecture de la base de données, disponibilité, etc.). En fonction des différents éléments de réponse, soit la *blockchain* ne saura qu'un moyen pour arriver à un but, soit la *blockchain* sera la caractéristique essentielle du projet.

Or, comme rappelé précédemment, la *blockchain* se dote techniquement et irrémédiablement d'une ou plusieurs fonctions cryptographiques. En conséquence, si une clause limitative de responsabilité apparaît comme possible dans le droit commun, elle ne saurait être valable en présence d'une *blockchain* en vertu des dispositions de la LCEN, en raison de la nature même de la *blockchain*.

---

[901] Par exemple : https://www.ibm.com/*blockchain*/getting-started, consulté le 28/09/2021

[902] La résilience d'une *blockchain* dépendant notamment des fonctions cryptographiques sur lesquelles elle repose ; par exemple, la difficulté d'une attaque des 51% repose notamment, pour la *blockchain* Bitcoin, sur l'utilisation du SHA-256 comme fonction de hachage ; dès lors, une *blockchain* utilisant des fonctions cryptographiques plus faibles se retrouvent plus sensibles à une attaque informatique.

[903] Potentiellement car, conformément à ce qu'il a été exposé précédemment un horodatage qualifié doit notamment reposer sur une signature elle-aussi qualifiée pour bénéficier de la présomption de fiabilité.

Ces connaissances, à la fois techniques mais également juridiques plaident une nouvelle fois pour une appréciation globale de la *blockchain*, et invitent à caractériser une nécessaire collaboration entre juridique et technique, au point que ces deux domaines voient leurs frontières de plus en plus effacées. Pour autant, l'utilisation de moyens de chiffrement telles qu'une *blockchain* emporte d'autres aspects de responsabilité ?

377. Sur le droit d'un suspect de ne pas participer à sa propre incrimination[904], une évaluation de la teneur du délit et des peines encourues doivent être prises en compte, notamment pour suivre deux arrêts de la CEDH, les arrêts *Jalloh*[905] et *O'Halloran*[906], néanmoins, les moyens utilisés pour chiffrer des données, vont être, à notre sens, également incriminantes. Le code de déverrouillage d'un téléphone peut être considéré comme une convention secrète de déchiffrement, et peut, par application de l'article 434-15-2 du Code pénal[907] être requise dans le cadre d'une enquête[908]. D'ailleurs, appliqué à la *blockchain*, la clé privée, ou alors les mots-clés de récupération[909] d'une telle clé devrait, à notre sens, suivre cette même logique.

Aussi, une simple utilisation d'un service grand public telle que *Telegram*[910] ou l'utilisation d'une combinaison de différents services et/ou supportés, par exemple, par une *blockchain* spécifique ou d'autres systèmes de chiffrements plus complexes, risquent au contraire, du fait de leur technicité et leurs spécificités, d'induire une éventuelle position du juge judiciaire vers une circonstance aggravante[911]. En effet, le Code pénal prévoit une

---

[904] BOUGLON T., *Obligation de déchiffrement d'un moyen de cryptologie et respect du droit de ne pas contribuer à sa propre incrimination : quelle issue à prévoir en cas de contentieux français devant la CEDH ?,* Revue Lamy droit de l'immatériel, n°181, 1er mai 2021

[905] CEDH, Grande Chambre, arrêt *Jalloh c. Allemagne*, nº 54810/00, 11 juil. 2006

[906] CEDH, Grande Chambre, *O'Halloran c. Royaume-Uni*, nº 15809/02, 29 juin 2007

[907] Art. 434-15-2, C. Pénal : « Est puni de trois ans d'emprisonnement et de 270 000 € d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités délivrées en application des titres II et III du livre Ier du code de procédure pénale.

Si le refus est opposé alors que la remise ou la mise en œuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée à cinq ans d'emprisonnement et à 450 000 € d'amende.

[908] Cass. Crim., 13 oct. 2020, n°20-80.150, n°JurisData 2020-015967

[909] En pratique, la création d'un compte sur un exchange *blockchain* ou encore la création d'un portefeuille de crypto-actifs (Ledger par exemple) s'accompagne de la création d'une liste de mots clé, permettant de retrouver une clé privée en cas d'oubli des codes d'accès au portefeuille en question.

[910] https://telegram.org/

[911] On retiendra simplement ici qu'une telle circonstance permet l'aggravation d'une peine pénale encourue. « Circonstances aggravantes », Fiche d'orientation, sept. 2020, Dalloz

aggravation des peines dans le cas où l'utilisation de moyens de cryptologies a vocation à préparer ou commettre un crime ou délit[912]. Il reste que, compte tenu des développements précédents, une incertitude demeure. Si l'utilisation d'un code de verrouillage d'un téléphone mobile constitue une convention secrète de déchiffrement, et est donc, logiquement, un moyen de cryptologie[913]. Alors il devrait être possible de caractériser une telle circonstance aggravante lorsqu'un téléphone mobile est utilisé pour la préparation ou la commission d'un crime ou délit. Cette solution paraît peu satisfaisante compte tenu d'une démocratisation complète des téléphones mobiles et tant l'encouragement des méthodes de chiffrement est fort notamment dans un but protection des données personnelles et « l'exercice des libertés individuelles dans cet univers[914] » numérique.

Au demeurant, si la libéralisation des techniques de chiffrement est une politique louable et nécessaire pour atteinte d'une sécurité globale des systèmes d'informations, elle ne doit pas être l'occasion de renforcer plus que nécessaire l'incrimination d'infractions et ne reste pas exempte de paradoxes.

378. Rappelons que le RGPD, notamment en ce qu'il impose le respect, pour le responsable de traitement le respect de différents principes (minimisation, proportionnalité, etc.), conditionne le respect de cette protection au respect d'un principe de conformité[915]. L'une des nouveautés majeures du RGPD a été également l'abandon des formalités déclaratives au profit de ce principe de conformité. Néanmoins, des survivances de ces formalités déclaratives existent encore. L'une d'entre elles[916] porte sur l'analyse d'impact relative à la protection des données[917]. Une telle analyse est rendue obligatoire lors que le traitement de données envisagé est susceptible de créer un risque fort pour les droits et libertés des personnes concernées, notamment en raison des caractéristiques du traitement envisagé. La déclaration auprès des autorités de contrôle compétentes étant requise en cas de risque résiduel, c'est-à-dire quand les mesures de protection des droits et libertés des personnes physiques laissent des risques

[912] Art. 132-79, C. pén.

[913] Sur ce point, il est d'ailleurs possible de noter que la mise en place de mesures de sécurité fortes sur l'IPhone est devenue un atout commercial, et que tout développeur d'application sur iPhone est invité à mettre en place des mesures de sécurité (https://developer.apple.com/documentation/uikit/protecting_the_user_s_privacy/encrypting_your_app_s_files, consulté le 28/08/2021).

[914] CNIL, *Les enjeux de 2016 : quelle position de la CNIL en matière de chiffrement ?*, 8 avril 2016

[915] Considérant 74 et 89, RGPD

[916] En reste des déclarations de conformité et des demandes d'avis auprès de la CNIL pour ces obligations déclaratives (https://www.cnil.fr/fr/declarer-un-fichier, consulté le 28/04/2021).

[917] Art. 35 et 36, RGPD

dont l'occurrence et la gravité ne sont pas négligeables. Une liste des opérations de traitements pour lesquels une étude d'impact est requise a été adoptée[918] , ainsi qu'une liste des critères selon lesquelles elle l'est également[919]. La volonté derrière cette analyse d'impact est louable : responsabiliser les responsables de traitement avant toute mise en place de traitements de données personnelles afin de garantir les droits et libertés des personnes concernées. Pour autant, la seule utilisation d'une *blockchain* au sein d'un traitement de données personnelles ne semble pas être une raison suffisante pour formaliser une étude d'impact. En effet, il est requis d'effectuer une analyse d'impact quand deux des neuf critères sont remplis[920].

Néanmoins, le cas des *blockchain*s réparties sur un espace européen et international peut poser quelques problématiques. En effet, une *blockchain* peut voir son architecture répandue sur n'importe quel territoire, y compris des territoires hors de l'UE, ou dans des États de faisant pas l'objet de décisions d'adéquation[921]. Il est vrai que l'extraterritorialité n'est pas l'un des neuf critères retenus, néanmoins, celui du traitement de données à grande échelle l'est. Et à défaut de définition de cette « grande échelle », il convient de l'apprécier de multiples façons : grande échelle géographique, volumétrique, ou qualitative (nombre de données sur une seule et même personne). Dès lors, l'utilisation d'une *blockchain* peut très bien avoir comme conséquence le traitement de données personnelles sur le territoire d'états tiers. En conséquence, une étude préalable d'un traitement de données personnelles utilisant une *blockchain* sera, à notre sens, toujours nécessaire, tant les caractéristiques de cette technologie peuvent avoir des répercussions sur la territorialité des données. Pour autant, la *blockchain* reste compatible avec les règles de droit international[922].

379. La mise en place d'une *blockchain* requière ainsi une pluralité de compétences. Techniques d'une part, afin d'appréhender les caractéristiques de l'architecture de données en

---

[918] Délibération n° 2018-327 du 11 oct. 2018 portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise

[919] Délibération n° 2018-326 du 11 oct. 2018 portant adoption de lignes directrices sur les analyses d'impact relatives à la protection des données (AIPD) prévues par le règlement général sur la protection des données (RGPD)

[920] *Ibid.*

[921] Considérants 104 et 108 et article 45, RGPD ; Les décisions d'adéquation sont des décisions émanant de la Commission et permettant de reconnaître la législation d'un état tiers comme garantissant suffisamment les droits et libertés des personnes physiques au regard de règles internes de protection des données personnelles.

[922] À cet effet, voir notamment : JAULT-SESEKE F., *La blockchain au prisme du droit international privé, quelque remarques*, Dalloz IP/IT 2018, p.554 ; FERAL-SCHUHL C., Praxis Cyberdoit, Dalloz, 2020-2021, Chap. 532.46 ; AUDIT M, précité

place, et juridiques d'autre part, afin notamment de pouvoir considérer correctement les différentes problématiques inhérentes à l'application d'une telle technologie. Les aspects particuliers de la *blockchain* invitent alors à une atténuation des oppositions entre droit et technique.

Section 2 : Atténuation des oppositions entre droit et technique

380. D'un point de vue sécurité informatique, la *blockchain* demeure donc un objet à double usage, insistant d'une certaine façon sur le caractère ambivalent de cette technologie. Au-delà, si la *blockchain* n'est pas la seule technologie de cet acabit, la complémentarité entre droit et technique ne se limite pas à la prise en compte d'intérêts purement techniques, ici relatifs à la sécurité des systèmes d'information. La *blockchain*, notamment avec l'avènement des *smart contracts* a invité à une réflexion présentée comme novatrice, à savoir le dépassement des frontières entre droit et technique. Or, la *blockchain*, prise comme expression de fonctions mathématiques dans l'univers numérique, n'est pas la première opportunité pour la construction de telles réflexions. C'est elle n'est qu'un exemple de la construction continue d'un langage commun entre l'informatique et le droit (§1), permettant l'avènement d'une véritable transdisciplinarité[923] juridique (§2).

§1 : Construction continue d'un langage commun

381. Dans un rapport datant de 1977, la réflexion suivante a pu être exprimée, réflexion gardant tout son sens actuellement : « Il est rare dépendant de voir le législateur se procurer aussi des conséquences de l'introduction d'une nouvelle technique (….) nous connaissons trop la difficulté d'appréhender sur le plan juridique des situations aussi nouvelles que celles qui sont et seront créées par l'introduction massive non seulement des ordinateurs, mais de toutes

[923] Le concept de transdisciplinarité (Piaget, années 1970 ; Nicolescu, années 1990), au surplus de l'interdisciplinarité, consiste à voir au-delà de plusieurs matières pouvant être prises indépendamment ; des finalités transdisciplinaires ne restant pas dans le cadre d'une recherche mono-disciplinaire. L'objectif d'une telle approche, allant au-delà du concept de pluridisciplinarité, permet de confronter des conceptions différentes afin d'en sortir de nouvelles données, permettant l'articulation de ces conceptions.

leurs applications et de tous leurs prolongements (…)[924] ». Il convient de rappeler que le contexte de cette citation fut l'adoption de la loi « Informatique et Libertés », mais au demeurant, les réflexions inhérentes restent parfaitement applicables à l'appréciation de la *blockchain* aujourd'hui, en particulier en ce qu'elle touche à la mixité entre droit et technique. Par ailleurs que cette appréciation fut renforcée notamment par le dernier rapport sur les Verrous technologiques des *blockchain*s[925]. La *blockchain* en est un exemple d'objet ambivalent, et est déjà caractérisée comme un outil mêlant juridique et technique. Si certains caractères disruptifs de la *blockchain* sont effectivement aisés à démontrer (consécration de nouveaux actifs financiers, modernisation et transformation des exécutions contractuelles, etc.), la portée de la transformation apportée par la *blockchain*[926] doit être nuancée. Si la *blockchain* permet d'appréhender aussi bien l'importance d'une règle technique ou le caractère obligatoire d'une règle juridique, « règle technique et règle de droit ont des buts similaires : il s'agit de guider les comportements et d'orienter les actions[927] ». Doivent-ils alors être considérés comme complémentaires, ou la suprématie de l'un doit-elle toujours être considérée ? En ce sens, la construction d'un langage commun, aussi bien pour permettre aux techniciens de s'adresser aux juristes, et inversement, qui ne serait être qu'encouragée tant les immixtions du pouvoir technique dans la sphère juridique sont nombreuses aujourd'hui. L'omniprésence de code informatique dans notre entourage (qu'il soit présent dans nos téléphones, nos voitures), et plus loin encore la place de l'algorithme dans notre société (*ranking* social, publicités et marketing ciblé, ou calcul de risque emprunteur) invite à une réflexion quant à la régulation de ce langage technique qui irrigue tant nos vies.

[924] THYRAUD J., *Rapport relatif à l'informatique et aux libertés*, Senat, Rapport n°72, rapport annexé au procès-verbal de la séance du 10 nov. 1977

[925] « Nous suggérons également d'étudier la création d'un Institut International Interdisciplinaire de la *Blockchain*, pour dynamiser la recherche française, encourager l'interdisciplinarité et donner à notre pays une meilleure visibilité internationale. », DALMAS S., DUVAUT P., GONTHIER G., JACOVETTI G., LANUSSE A., MEMMI G., TUCCI-PIERGIOVANNI S., Les Verrous Technologiques des *blockchain*s, BCom de la DGE, Avril 2021, disponible à https://www.entreprises.gouv.fr/files/files/etudes-et-statistiques/synthese-*blockchain*.pdf

[926] TARNOPOLSKAYA D., *Blockchain : révolution annoncée de la pratique juridique ?*, Village de la justice, 8 sept. 2017, disponible à https://www.village-justice.com/articles/*blockchain*-revolution-annoncee-pratique-juridique,25755.html, consulté le 28/04/2020

[927] FAVREAU A., *L'état au défi des blockchains, régulation(s) et usages publics de la technologie blockchain*, RFPI, numéro spécial, fév. 2021

382. La perspective de voir naître un *corpus* appelé « *Lex cryptographia* » apparaît prometteuse[928]. Selon De Filippi et Wright, elle est une émanation/extension de la « *Lex mercatoria* » médiévale, cet ensemble de règles informelles qui régissaient les relations entre les commerçants pour les échanges internationaux ou interrégionaux. Pour la régulation d'Internet, nous avions vu apparaître une « *Lex electronica* » hors des cadres juridiques nationaux et émanant d'une communauté internationale d'utilisateurs. La *Lex electronica* est la première forme de régulation par le Code. La *Lex Cryptographia* instaurerait un nouveau *corpus* de règles administrées et exécutées automatiquement à travers les smart contracts et la DAO[929]. Ainsi, à mesure que les technologies de *blockchain* évolueront et que de nouvelles applications apparaîtront, *Code of Law* et *Code as Law* cohabiteront avec plus ou moins d'antagonisme ou de coopération. Invitant alors à s'interroger sur la pertinence ou la possibilité de « coder le droit », ou, inversement, a « judiciariser[930] le code ». Que signifierait « coder le droit », et comment apprécier la nature du code ? Si l'on se réfère, de manière sémantique, à l'action de coder, et dans le cadre d'un processus informatique, on pourrait retenir que coder est la transcription et la représentation de lois ou de règles, et demeure ainsi une expression d'un langage, compréhensible par la machine, abstrait, donnant une signification a une séquence électrique[931]. Une dimension linguistique importante se retrouve : le code ne serait qu'un langage, une suite de caractères compréhensibles, doté d'une signification intelligible, propre à un support informatique. De par une telle définition, son rapprochement avec l'écrit, tel que défini par le Code civil[932], est aisé. Il est possible de concevoir ainsi que le code informatique ne serait qu'un écrit, appréhendé par la loi. Et de cette appréhension en découlerait une soumission du code informatique à la loi, au même titre que l'écrit, et ses potentielles conséquences juridiques, y sont soumises également.

Sur la possibilité de coder le droit, de nombreuses difficultés peuvent se trouver, notamment par rapport à l'essence même d'une norme juridique, qui reste empreinte d'un

---

[928] Le premier texte sur cette question : WRIGHT A. et DE FILIPPI P., *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, 2015, Available at SSRN : https://ssrn.com/abstract=2580664 or http://dx.doi.org/10.2139/ssrn.2580664

[929] https://fr.wikipedia.org/wiki/Organisation_autonome_decentralise (consulté le 16/05/2019)

[930] Quoique non académique, le terme « juridifier », emprunt du terme anglais « *juridify* » aurait pu être utilisé ici pour retranscrire le parallèle entre transformer le droit en code et transformer le code en droit.

[931] BEN HENDA M., *L'enseignement du code informatique à l'école : Prémices d'un humanisme numérique congénital.* Chaire Unesco-ITEN. Actes de la 5e rencontre annuelle d'ORBICOM, Les éditions de l'immatériel, 2017

[932] Art. 1365, C. Civ : « L'écrit consiste en une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quel que soit leur support. »

contenu de pensée, appartenant à un produit de l'esprit[933]. Or, si la caricature de l'informatique peut être une suite logique de caractères numériques, binaire, il serait vain, aujourd'hui, d'essayer d'exprimer une pensée de la même façon, tant elle reste fonction, à l'instant T, de faits de société. Également, peut être considéré le caractère supplétif des règles techniques. Si la *blockchain* repose sur du code et peut servir de tremplin pour des transformations sociétales profondes, il reste que « les systèmes juridiques classiques devront veiller à ce que les droits, les intérêts et les attentes de la communauté au sens large soient protégés[934] ». Plaçant la norme technique, objective, est incapable de prendre en compte les attentes d'une communauté, qui restent potentiellement subjectives.

La conception potentielle d'une *lex electronica* ou *cryptographia* induit, de la même façon qu'une *lex mercatoria*, que sa création soit établie par des acteurs de ce domaine. Bien qu'étant une conception logique, voire naturelle, la réduction du champ de création à de seuls spécialistes du sujet peut conduire à des lacunes de conceptions. La loi étant « l'expression de la volonté générale[935] », elle ne saurait être réduite à une poignée d'experts centrés sur une seule matière.

383. Pourtant, la volonté de création d'un langage commun existe d'ores et déjà, et n'est pas propre aux débats actuels sur l'opportunité créée par la *blockchain* pour l'élaboration d'un tel langage. Le langage informatique présente des éléments de semblables à ceux que l'on peut trouver dans le langage juridique. L'évolution du langage technologique (et par ici est entendue l'évolution des différentes façons de « coder[936] », et donc d'appréhender sans cesse de nouvelles contraintes ou de nouvelles évolutions, aussi bien informatiques que sociétales) a été de pair avec l'évolution du langage juridique. Notamment en ce que ce dernier a dû se normaliser et se codifier. L'évolution des nomenclatures judiciaires, sans cesse affinées, avec pour but de classer les faits, leurs formes, sans forcément décrire les règles de droit positif[937] n'a pas été réalisée pour de seuls traitements statistiques.

L'intérêt de posséder des nomenclatures rationnelles, basées sur des critères normés et répliquables indépendamment de la volonté ou des considérations de leur auteur a permis

[933] WICKERS T., *Peut-on coder le droit, Cahier de droit de l'entreprise*, n°4, Juil.-Août 2019
[934] FAVREAU A., précité.
[935] Déclaration des Droits de l'Homme et du Citoyen, 1789
[936] https://fr.wikipedia.org/wiki/Histoire_des_langages_de_programmation, consulté le 06/05/2021
[937] SERVERIN E., BEROUJON C. BRUXELLES S., *Classer, coder*, Rapport de recherche, Ministère de la Justice. 1988

l'encouragement et la continuité de recherches, fondamentales ou simplement jurisprudentielles. Sans le nommer, l'analyse normée d'affaires judiciaires participe à une première version du codage de la loi. L'apprentissage algorithmique ou statistique repose sur de telles méthodes. Il a pour but de rationaliser l'information, la classer, et en tirer une métadonnée afin d'affiner un modèle et en tirer une valeur ajoutée dans le traitement de problématiques données[938]. En soi, il est possible de considérer que le codage de la loi a déjà débuté, même s'il en est qu'à ses balbutiements. Et sans faire de projections hasardeuses, ces travaux font actuellement l'objet de nouvelles prestations juridiques : par exemple, la société *Case Law Analytics* utilise, grâce à des procédés algorithmiques complexes, ces différentes nomenclatures judiciaires afin de fournir une analyse de risque dédiée à la prévention des contentieux[939].

Dans d'autres matières, et dans une dimension qui paraît légère dans le cadre de cette étude, l'expression de règles normatives de manière informatique existe, même dans un cadre qui paraît profondément limité. La conception d'un jeu vidéo se fait en nombreuses étapes : de la conception théorique (concept du jeu vidéo, plateforme, contraintes techniques, etc.), jusqu'au *game design* et à l'exploitation. Des mécaniques sont acquises depuis le premier jeu vidéo[940], comme le décompte de point, et d'autres vont émerger ou encore la « barre de vie », ou encore le « *high score* », pour être reprises par d'autres. En ce sens, une capacité normative du code informatique peut être entendue dans le seul où le programmeur du jeu vidéo va édicter ses règles, ses paramètres, dans lequel le joueur va évoluer.

384. Il est possible d'y voir un parallèle intéressant avec la possibilité de « coder la loi ». Là où les fonctionnalités d'un jeu vidéo sont d'abord fixées par les contraintes techniques (puissance et mémoire machine, fonctionnalité, etc.), elles peuvent déjà être contrebalancées par une norme juridique par simple implantation. L'exemple des « *loot box*[941] » est particulièrement parlant. Décrié pour sa mécanique défavorable pour le joueur, le système des

[938] Pour plus d'informations : https://www.ibm.com/fr-fr/analytics/machine-learning (consulté le 06/05/2021)

[939] https://www.caselawanalytics.com/produits/risque-contentieux/, consulté le 08/05/2021

[940] Le premier jeu vidéo est considéré comme étant « Pong », un jeu de tennis publié en 1972. Le principe était très simple : les joueurs sont représentés par une barre latérale et le but était de s'échanger un carré de pixels représentant la balle.

[941] Une « *loot box* », pouvant être traduit par « coffre à butins » est le plus souvent représenté par un coffre virtuel, le plus souvent payant (soit en devises réelle, soit en devises propre au jeu concerné), et permettant d'obtenir des éléments supplémentaires, censés enrichir le gameplay d'un jeu.

« *loot box* » présentent dans le jeu vidéo « *Star Wars Battlefront II*[942] » a défrayé les chroniques spécialisées. Était mis en cause le taux d'obtention des éléments déblocables dans le jeu, et le fait que pour obtenir un jeu « complet », le joueur devait débourser de fortes sommes d'argent. Ce système a rapidement été décrié, au point qu'une question sur leur régulation a pu être posée[943]. Néanmoins, ce système a pu faire l'objet d'une régulation purement technique, en publiant et en modifiant les paramètres d'obtention des objets « *in game* » concernés ; un simple changement de paramètre de probabilité, conforme avec des critères légaux préalablement établis, devient avoir expression technique d'une norme. Cela signifiant que l'expression technique de la loi peut exister, et n'est pas incompatible avec des travaux futurs sur cette thématique, si tant est que les outils existent. De manière plus prosaïque, l'univers numérique est déjà jalonné de cette typologie normative, étant donné les règles de fonctionnement d'un réseau social (conditions d'utilisation, algorithmes de présentation et de sélection de contenu), ou encore de par les conditions d'utilisation d'un téléphone (limitation des téléchargements d'application, suivis et recommandations personnalisés). À ce titre, les juristes doivent être vigilants quant à l'appréciation de ces caractères techniques non dénudés de sens juridique[944].

Également, les codes algorithmiques ne sont, en l'état, pas neutres, et ne sont pas exempts de conceptions sociales ou juridiques : « sous l'apparente neutralité de la description du réel, se dissimulent toujours les grilles de lecture de son concepteur[945] ». S'il n'est, aujourd'hui, pas possible de transmuter des normes juridiques en code ou instructions automatisées de manière littérale et exhaustives, c'est le concepteur qu'il est possible d'influencer. S'interdire de réguler de manière informatique le code revient à s'interdire de réguler le concepteur, or, ce dernier est avant une personne, un sujet de droit, qu'il est possible de contrôler ou de former. Pour une contextualisation propre aux *smart contracts*, les travaux de l'association *Open Law* ont pour but de participer à la création de ce langage commun, en ayant pour but de créer un référentiel de « *smart contracts open source*[946] ». De tels référentiels, dont la construction a pu se baser sur la collaboration de juristes et technophiles

[942] Sorti en 2017, édité par le studio Electronic Arts, développé par les sociétés DICE, Criterion Games et Motive Studios

[943] Rép. min., n° 14570 : JO Assemblée Nationale 27/11/2018 page : 10556

[944] NETTER E. *Droit et numérique*, Numérique et grandes notions du droit privé, CEPRISCA, 12 fév. 2019, §20, disponible à https://enetter.fr/introduction/ii-le-numerique-et-le-droit/, (consulté le 20/08/2021)

[945] CHANTEPIE G., *Le droit en algorithmes ou la fin de la norme délibérée ?*, Dalloz IP/IT 2017. 522

[946] https://openlaw.fr/travaux/cycles/smart-contract-academy (consulté le 01/10/2021)

de la *blockchain*, ont pour intérêt de réaliser un lien entre technique et juridique, en ce qu'il a pour objectif de rationaliser juridiquement l'écriture de *smart contracts* et assurer une exception automatique de conditions contractuelles de manière conforme à la loi.

385. Néanmoins, nos conceptions sociales actuelles, prises dans leur dimension technologique, rêvent un paradoxe fort. Le Droit se complexifie, développe son caractère technique, au point d'en devenir obscur et abscons. Mais la recherche juridique et l'application pratique du Droit trouvent un renouveau dans l'appréciation des nouvelles technologies. Si la représentation visuelle du Droit trouve progressivement ses marques[947], elle est représentative de nouveaux axes de recherche, de nouvelles façons d'appréhender le Droit, au biais de prismes empreints d'autres matières ou même d'autres cultures[948]. Ces nouveaux axes de recherches desservant une représentation du Droit, nécessaire pour mieux l'appréhender et en parler[949]. Au-delà, la question de savoir s'il est possible de codifier le Droit, et inversement, rendre juridique le code, ne reste qu'un prolongement, actuel, de débats qui ne sont pas nouveaux. L'introduction de la machine, à l'époque où était utilisé le terme cybernétique, à savoir une science ayant pour but d'obtenir un dialogue « homme-machine » et « machine-machine[950] ». Un refus pur et simple de l'immixtion du code dans le droit serait un aveu de faiblesse face à l'impossibilité de maîtrise d'un tel langage, et pis, serait faire « le dernier pas vers la soumission à la mécanisation[951] ». Ériger des barrières, qui seraient donc linguistiques, entre droit et technique conduirait à une constante incompréhension de deux systèmes, dont la nécessaire collaboration entre eux serait condamnée *de facto*. Pourtant, l'existence de recherches, depuis les années 70, sont focalisées sur les rapports entre Droit et langue, notamment pour répondre à des problématiques liées à la formalisation et à la traduction du Droit, ce qui témoigne du caractère impératif de compréhension mutuelle[952].

---

[947] MONTANT L., *Legal design : vers une transformation radicale de l'expérience client des cabinets d'avocats*, Dalloz Actualité, 17 déc. 2020

[948] Pour un exemple de lecture novatrice du droit : Propriété intellectuelle et pop culture, Lexisnexis, Actes du colloque des JUSPI, 2020, ou encore « *Du punisher au Lawyer : les super héros au prisme du droit* », soirée d'études, Université de Strasbourg - Association Mediadroit, 25/05/2016

[949] GOEDERT N., MAILLARD N., *Énoncer le droit, représenter le droit., « Le droit en représentation(s), »* Mare et Martin, coll. "Libre-droit", pp.16-26, 2017

[950] WIENER N., *Cybernétique et société. L'usage humain des êtres humains*, 10-18, 1962, édition originale : Cybernetics and Society, 1954

[951] KONDRATUK L., *Disputer, codifier, coder. 2018*

[952] MONJEAN-DUCAUDIN S., *De la jurilinguistique à la juritraductologie. Comparaison des approches canadienne et européenne*, Coder-décoder : linguistique et concepts juridiques, Éditions Yvon Blais, 2019. ⟨ hal-03247570⟩

En réalité, le débat pouvant porter sur le possible codage du Droit, ou sa réciproque tenant à informatiser le Droit n'est pas seulement un débat actuel. Il existe depuis la prise en compte des influences sociétales et juridiques de l'informatique sur le comportement des individus et de la société. De surcroît, il ne doit pas pour autant rester un débat enfermé dans une conception tournée vers le passé. Bien au contraire, ce débat doit être tourné vers l'avenir. La complexification et l'importance de l'univers numérique, représentées en premier lieu par des caractéristiques informatiques, invitent à une réflexion tournée vers la modernisation du langage juridique, non pas pris en tant que matière autonome, mais pris en tant que langage, susceptible d'évoluer.

Savoir s'il est possible de coder le Droit est en réalité dépassé, tant certaines expressions d'un droit informatisé existent déjà. Les réflexions sur la manière dont il est possible de le faire doivent primer, même si elles invitent à raisonner sur des mécaniques ou une évolution du langage[953] qui est future, et ainsi accepter l'existence des « influences et rapports réciproques entre le droit et la technique, au lieu de les opposer dans une course stérile à l'efficacité[954] ». En ce sens, un véritable avènement symbiotique de la transdisciplinarité juridique est annoncé.

§2 : Avènement symbiotique de la transdisciplinarité juridique

386. L'époque de l'étude de « disciplines juridiques aux contenus bien identifiés et ne prêtant guère à confusion[955] » paraît révolue avec un renforcement quotidien des attributs d'un monde numérique de plus en plus présent. Dès 1998, le Conseil d'état prônait le fait de ne pas créer un droit spécifique à Internet[956]. Le professeur Caron[957] s'interrogeait sur la pertinence de la création d'un droit commun de l'internet, capable d'appréhender l'ensemble des matières et autres régimes particuliers applicables à ce réseau universellement utilisé. Si ce dernier

[953] Sans pour autant renoncer à l'impératif constitutionnel (sur ce sujet : V. not. Conseil constitutionnel, 7 déc. 2000, n°2000-435-DC) ; NETTER E. *Le « code du travail numérique ». Intelligence artificielle, gestion algorithmique et droit du travail*. Les travaux de l'AFDT, Dalloz, 2020, disponible à : https://hal.archives-ouvertes.fr/hal-02924955/document, (consulté le 05/10/2020)

[954] DULONG DE ROSNAY M., *Les Golems du numérique*. Droit d'auteur et Lex Electronica, Paris, Presses des Mines, Collection Sciences sociales, 2016, p.58

[955] CARON C., *À la recherche d'un jus unum de l'Internet*, Communication Commerce électronique n° 6, Juin 2017, repère 6

[956] CE, *Internet et les réseaux numériques*, Collection Études du Conseil d'état, La Documentation française, 1998

[957] *Ibid.*

constate une préférence pour une prospérité de « multiples droits spéciaux » de l'Internet, en rappelant les intérêts d'une réflexion sur la création d'un droit commun. Cette construction ne saurait être aisée, il faut le concevoir. Le « droit de l'internet » pouvant aujourd'hui regrouper nombre de matières disparates en raison d'une multiplicité de situations et d'objets juridiquement identifiables. Le droit du commerce électronique (regroupant un pan du droit des obligations et rattaché à Internet) peut se trouver pour les sites de e-commerce ; la protection des données pour l'ensemble des traitements de données personnelles s'y rattachant (hébergement, collecte, etc.) ; ou encore le droit de la propriété intellectuelle pour les plateformes de streaming (« *YouTube* », etc.). Est en réalité faite l'invitation à, notamment dans le cadre de la recherche (fondamentale ou appliquée), élargir l'horizon d'appréciation. L'une des beautés du « droit de l'internet » réside notamment dans la multiplicité des matières qu'il peut aborder. Invitant à une constante réflexion et à une adaptation quasi en temps réel aux évolutions de ce réseau.

387. La détermination d'un droit commun et donc la création d'un régime général, avec comme satellites différents droits spéciaux se confronte à des matières juridiques déjà existantes. Par exemple, le droit commun des obligations pouvant déjà trouver application à un éventuel droit commun de l'internet. Il reviendrait alors à reprendre des dispositions ci-et-là qui auraient vocation à s'appliquer de manière commune au droit de l'Internet. Emportant alors peut d'intérêt pour une telle compilation de textes. Au surplus, et pour reprendre des développements qui ont été rédigés pour la consécration ou non d'un droit de la donnée[958], la création de droits spéciaux de manière déconnectée des objectifs économiques des acteurs visés par eux (la donnée pouvant avoir une valeur pour leur propre création *per se*, soit en tant qu'expression d'une autre activité économique) peut emporter la constitution de monopoles au profit des acteurs principaux ou ceux pour lesquels ce droit est créé. De plus, la création d'une matière dédiée à la *blockchain* ou même à ses applications reviendrait à devoir créer une infinité de droits dérivés d'objets, et si l'opportunité de telles créations peut se justifier au regard des potentiels d'un objet, une telle création ne resterait qu'éphémère car encadrée par la temporalité de son utilisation. Aurait-on dû créer un droit du Minitel ?

[958] ZOLYNSKI C., *Un nouveau droit de propriété intellectuelle pour valoriser les données : un miroir aux alouettes ?,* Dalloz IP/IT 2018 p.94

388. La démocratisation constante de « nouvelles technologies » entraine des changements rapides et souvent difficilement prévisibles[959]. De la même façon, les secteurs juridiques font face aujourd'hui à des changements radicaux portant sur les outils utilisés, mais également les défis auxquelles ils font face. Des initiatives nées de ce constat existent, et l'une d'entre elles met en avant une nécessaire transformation du monde juridique, notamment en ce qu'elle requière l'avènement de juristes amènent d'appréhender la technique, au point même d'en faire partie. Les juristes-codeurs sont annoncés[960].

389. Plusieurs raisons peuvent pousser à accepter de telles transformations, et même à les encourager. Si le champ de la présente étude démontre notamment que l'appréciation d'une technologie peut transcender une seule matière juridique et aborder ainsi plusieurs spécialisations (droit des logiciels, protection des données), le dépassement de conceptions juridiques unitaires n'est pas novateur en tant que tel (par exemple, l'étude du blanchiment d'argent conduit à s'interroger aussi bien sur le droit des affaires que sur le droit pénal). Si la *blockchain* peut se distinguer, c'est par son appartenance indispensable au monde de la technique (sécurité informatique, algorithmes, ou encore architecture de systèmes d'information). Insistant alors, pour son appréciation, à un socle de connaissances non plus juridiques, mais techniques.

L'avènement d'autres technologies disruptives, tels que l'Intelligence artificielle ou encore une hégémonie grandissante des *Big data* conduit à la conceptualisation et à la création de nouveaux ensembles de données particuliers. Par exemple, les *legaltechs*[961] conduisent à un amoncellement de données juridiques, dont l'intervention de seuls juristes ne saurait être suffisante pour l'essor. Pourtant, et pour prendre l'exemple du *Big data* juridique, il est « indispensable que les juristes restent présents et actifs[962] ». Notamment pour des raisons d'éthique et d'exactitude dans l'analyse de telles données, les juristes doivent s'intéresser aux nouvelles technologies. En particulier celles ayant trait, de près ou de loin, à leurs compétences.

---

[959] CREUX-THOMAS F., *Transition numérique et diffusion de l'information juridique : de nouveaux défis*, Revue pratique de la prospective et de l'innovation n° 2, Oct. 2017, dossier 14

[960] DANGEARD M., *Il est temps que les juristes deviennent des juristes-codeurs, et se mettent à collaborer sur les contrats*, Revue pratique de la prospective et de l'innovation n° 2, Oct. 2017, entretien 5

[961] CASSAR B., *La transformation numérique du monde du droit*. Thèse Droit. Université de Strasbourg, 2020.

[962] CROZE H., *Comment être artificiellement intelligent en droit*, La Semaine Juridique Edition Générale n° 36, 4 Sept. 2017, 882

Au point qu'une « nécessaire distinction entre recherche fondamentale et recherche (peut être) appliquée[963] ». L'un des premiers augments en faveur d'une telle consécration d'interdisciplinarité, voire d'une transdisciplinarité est d'assurer une conformité des usages technologiques à des règles juridiques préétablies, ou, de surcroît, à appréhender, proposer, imaginer des solutions existantes ou nouvelles. Non pas pour inviter les juristes à s'approprier sans cesse de nouveaux savoirs sortant continuellement de leurs compétences initiales, mais faire « dialoguer - leurs - savoirs[964] ».

390. L'évolution des cursus universitaires et autres formations juridiques se heurtent à l'étude d'objets pouvant toucher une grande diversité de questionnements juridiques distincts. La *blockchain* en reste un bon exemple : abordant la sécurité informatique ou encore le droit des contrats, il faut avoir conscience du potentiel éclatement des questionnements juridiques quelle peut amener[965]. Si un éloge du doute[966] est permis voire même recommandé face à des technologies disruptives, ce n'est pas tant par opportunité intellectuelle que par intérêt. Si une inflation législative ne saurait être encouragée[967], la prise en compte d'un contexte global est nécessaire à des fins de qualité législative. La teneur des présents travaux en est un exemple. Si la rédaction de ces propos a débuté en 2016, certains éléments de contextes ont été affinés depuis. Par exemple, l'importance des cryptoactifs (explosions des prix *Bitcoin* en 2017 et 2021), l'apparition de la finance décentralisée[968], ou l'expérimentation de nouveaux cas d'usages (par exemple l'agro-alimentaire[969]). Or, une réglementation précipitée n'aurait pu tenir compte de ces futures pratiques, et aurait pu même les limiter. Il ne convient pas de punir « l'informatique pour les services qu'elle aurait rendus[970] », et l'élaboration d'une

[963] *Ibid*.

[964] GESLIN A., *La circulation des modèles normatifs ou la pensée juridique du mouvement*. In. BOURGUES P., MONTAGNE C. (dir.), La circulation des modèles normatifs, PUG, 2016 en l'espèce, l'auteur visait les dialogues entre savoirs juridiques et les autres sciences sociales. Or, il ne paraît pas trop ambitieux de considérer un dialogue avec l'ensemble des sciences ; sont visées ici les sciences dites « dures », comme l'informatique.

[965] CAPRIOLI E., Dalloz IP/IT 2019 p.429, précité

[966] GAUTRAIS V. *Les sept péchés de la blockchain : éloge du doute !*, Dalloz IT/IP 2019, p.432

[967] Cf. *Supra*, p.58

[968] ou *DeFi* (pour plus d'informations : https://en.wikipedia.org/wiki/Decentralized_finance, consulté le 14/08/2021).

[969] HOFMANN F., *Malongo lance un café chez Carrefour avec la technologie blockchain*, Linéaires, 11 juin 2021, disponible à https://www.lineaires.com/les-produits/malongo-lance-un-cafe-chez-carrefour-avec-la-technologie-*blockchain*, (consulté le 14/08/2021)

[970] BRAIBANT G., *Questions d'ordre politique soulevées par la protection des données et des libertés individuelles*, p178. OCDE

réglementation de manière trop hâtive peut provoquer l'appauvrissement des processus d'innovation[971].

Former le « juriste de demain », le « juriste augmenté[972] », former des juristes technophiles, pouvant appréhender des problématiques sous-jacentes à la démocratisation de la *blockchain* et des *smart contracts* mais pouvant également transformer leur appétence pour le numérique en véritable levier de compétence. Face à l'innovation, le juriste est souvent vu comme « l'empêcheur de tourner en rond », la personne mettant un frein aux développements techniques.

Toutefois, même si le concept d'innovation est difficilement appréhendé par la doctrine juridique[973], cet objectif ressort d'un enjeu, actuel, commun aux professionnels, à savoir la demande de profils pouvant faire le lien entre technique et juridique, pour justement pallier l'opposition classique entre ces deux fondamentaux.

391. Le juriste de demain, grâce à l'avènement de technologies telles que la *blockchain* et de ses *smart contracts*, pourra cultiver son appétence pour le numérique au-delà de ses compétences juridiques, au point qu'il en ressortira une compétence transdisciplinaire, d'ailleurs attendue par la pratique[974]. De surcroît, cela ne serait qu'un prolongement logique, né de la pratique contractuelle, consistant à concevoir le contrat non plus comme un simple acte juridique, mais comme partie essentielle d'un projet[975].

Il est important de relever que ce qui s'apparente aujourd'hui à un défi, à une (r-)évolution pour nombre de juristes est en fait une réalité depuis près de 50 ans : « Aux yeux du juriste français, les transformations du droit par l'informatique s'inscrivent dans une double perspective. D'un côté, la nécessité d'un encadrement de l'informatique par le droit afin de

---

[971] La présence de « zones grises » peut permettre le développement de d'innovation technologiques. Par exemple, l'émergence de nouvelles plateformes comme Uber ou Blablacar ont su profiter de ces zones grises (de manière positive ou non, en reste que l'innovation est présente). France Stratégie, « Répondre à l'innovation disruptive », Étude, Janv. 2017

[972] SERRANO E. *Village Legaltech 2019 : En marche vers le juriste « augmenté »*, Revue Option Droit et affaires, 04/12/2019, 471, pp.2-3

[973] F. SCHULTZ M., *L'innovation : une véritable poule aux œufs d'or*, OMPI Magazine, juin 2017, disponible à https://www.wipo.int/wipo_magazine/fr/2017/03/article_0003.html, cité par : *Propriété intellectuelle - Réflexion autour du concept d'innovation*, Veille, CCE n°10, Oct. 2017, alerte 67

[974] LATIL A., *L'interdisciplinarité chez les juristes*, Revue pratique de la prospective et de l'innovation n° 2, Oct. 2019, dossier 17

[975] BÜKLE J., MAHIEU R., *Le "contract management" : une vision innovante des contrats d'affaires,* Revue Lamy Droit civil, n°158, 1er avril 2018

maîtriser les dangers que recèlent les possibilités nouvelles de classement, de tri, de recoupement et de transmission des informations. (…) D'un autre côté, le souci d'une adaptation du droit à l'‘informatique, car il est indispensable que les règles juridiques soient en harmonie avec les pratiques engendrées par l'utilisation de l'informatique, qu'elles ne viennent pas freiner une évolution qui se manifeste dans tous les secteurs de la vie économique[976] ». En ce sens, une approche purement disciplinaire pourrait être réductrice[977], et la prise en compte d'horizons disparates correspond à une dimension essentielle du droit, prise comme l'idée d'une connaissance du phénomène juridique à partir de ce que le droit a de spécifique, par rapport à d'autres champs de connaissance avec lesquels il a en partage les caractères communs de normativité[978].

392. Une approche du droit des nouvelles technologies, en ce que sa complexité amène à la prise en compte de régimes et éléments de contextes divers, pourrait s'inspirer de la transsystémie[979]. À savoir une prise en compte de contextes non entendues par les catégories préexistantes de la connaissance juridique seule. L'étude, croisée ou recoupée du droit des nouvelles technologies se prêtant facilement à l'exercice. Par exemple, une approche par la gestion de projet (cycle en « V[980] », ou méthode *scrum*[981]) pourrait avoir comme bénéfice d'études en premier lieu les étapes fondamentales (négociation, caractérisation du besoin), les étapes relatives à l'exécution, (implantation, tests et recettes) et enfin les contours de la fin de la relation contractuelle (fin d'exécution, responsabilités, etc.). Outre une opportunité pour des applications professionnelles directes, une telle approche n'est pas exclusive de la réalisation de recherches en amont ou en aval de la réalisation d'un objet donnée. Au contraire, une telle approche encourage la recherche notamment en ce qu'elle permet la critique potentielle d'une

[976] HUET J., *La modification du droit sous l'influence de l'informatique : aspects de droit privé* ; JCP G 1983 n°I, 3095

[977] BARBAROUX N., BARON R. FAVREAU A., *Blockchain et finance – approche pluridisciplinaire,* 2020, p.125.

[978] *Ibid*.

[979] CASTILLO-WYSZOGRODZKA S., RIFFARD J-F., *"Introduction", Le Dossier : La transsystémie. Pour une approche rénovée de la conception et de l'enseignement du droit*, Actes du colloque de Clermont-Ferrand des 12 et 13 déc. 2016, textes réunis par J-F. Riffard et S. CastilloWyszogrodzka, La Revue du Centre Michel de l'Hospital [édition électronique], 2019, n° 17, pp. 8-10. La Revue du Centre Michel de l'Hospital - édition électronique, Centre Michel de l'Hospital CMH EA 4232, 2019, pp. 8-10.

[980] https://fr.wikipedia.org/wiki/Cycle_en_V, (consulté le 30/09/2021)

[981] https://fr.wikipedia.org/wiki/Scrum (consulté le 30/09/2021)

régulation, tant sa bonne application découle de « l'existence de l'objet justifiant la régulation[982] ».

L'émergence actuelle des *smart contracts* encodés sur une *blockchain* est un exemple révélateur des compétences que devra mettre en œuvre le juriste de demain[983]. Tout juriste connait les conditions de validité classiques d'un contrat[984], auxquelles s'ajoutent notamment, par exemple dans le cadre d'un contrat de cession de droits d'auteur, des exigences en termes de durée du contrat, ou encore de rémunération. Ce formalisme à respecter fait partie des fondamentaux pour tout juriste. Demain, à l'occasion de la rédaction d'un *smart contract*, ces fondamentaux vont devoir trouver leur équivalent dans le code informatique. D'une part, pour s'assurer de la correcte traduction en langage informatique, et d'autre part pour s'assurer de la conformité du code à la loi (renversant, pour cet exemple la célèbre maxime « *Code is Law* »[985]). Une question se soulève alors : comment le juriste pourra-t'il s'assurer de la conformité du langage informatique à défaut de compétences adéquates ?

393. Cette réflexion peut trouver de nombreux parallèles, notamment avec la mise en œuvre du RGPD. Norme faisant état d'un lien permanent entre technique et juridique, le juriste spécialisé en protection des données personnelles se devra de travailler de concert avec les développeurs informatiques afin de pouvoir assurer la conformité des traitements de données personnelles aux différentes normes applicables[986]. Au point qu'il pourra faire partie intégrante des stratégies d'entreprise autour de la sécurité de l'information. Comme en témoignait Bruno Rasle[987], la sécurité des systèmes d'information ne doit pas être l'apanage des seules DSI[988], invitant la gestion de prérogatives informatiques à prendre en compte une collaboration d'autres services. L'une des innovations du RGPD est aussi le renforcement des prérogatives

[982] MBIDA ELONO T., *Débat doctrinal sur la juridicité et l'hypothèse d'une appréhension tridimensionnelle du droi*t, Revue Pluridisciplinaire Africaine de l'environnement, Association Jeunesse Africaine pour l'environnement, 2021, La sécurité alimentaire et les défis agricoles en temps de crise : regards croisés Afrique-Europe. ⟨ halshs-03226635v2⟩

[983] GUERLIN G., *Considérations sur les smarts contracts*, Dalloz IP/IT, p.512

[984] Art. 1128, C. Civ. « Sont nécessaires à la validité d'un contrat : le consentement des parties, leur capacité de contracter, un contenu licite et certain ».

[985] LESSIG L., précité

[986] A cet égard la CNIL a d'ailleurs publié plusieurs documentations à l'attention des développeurs (par exemple : https://www.cnil.fr/fr/la-cnil-publie-un-guide-rgpd-pour-les-developpeur, consulté le 23/03/2020).

[987] RASLE B. a été Délégué Général de l'AFCDP (Association Française des Correspondants à la protection des Données Personnelles) entre 2008 et 2020.

[988] RASLE B., PSSI : Contraire ou opportunité ?, Linkedin, 15 mai 2021, disponible à : https://www.linkedin.com/pulse/pssi-contrainte-ou-opportunit%C3%A9-bruno-rasle/, (consulté le 15/05/2021)

et des contrôles du sous-traitant de données personnelles[989], invitant alors à un contrôle en partie purement juridique en ce qu'il doit porter le contrôle de la répartition des rôles et responsabilités entre responsable de traitement et sous-traitant, mais invitant une nouvelle fois à rationaliser ce contrôle au biais de considérations stratégiques (choix du sous-traitant, dimensions financières).

Ce renforcement pourra se faire en deux temps. D'une part, par une mise à jour contractuelle des obligations du sous-traitant, et d'autre part *via* un audit des traitements de données personnelles effectuées. Le juriste se verra ainsi confier une double mission : une mission purement juridique inhérente à la gestion contractuelle des relations avec le sous-traitant, et une mission à vocation technique afin de s'assurer de l'effectivité du RGPD chez ce dernier. L'ensemble de ses missions revêtira ainsi un caractère transdisciplinaire voué à la protection des données personnelles, au service, notamment, d'un renforcement de la conformité.

Ceci met en exergue le fait que le juriste de demain, afin d'assurer des missions essentielles, comme contrôler la conformité d'un contrat, devra travailler de concert avec des développeurs, et *a minima* posséder une appétence pour l'informatique et le code afin de pouvoir travailler non pas, cette fois, dans un but de limitation du développement technique, mais dans un but de coopération avec les techniciens[990]. Cette prise de position est révélatrice d'un véritable défi, celui d'une collaboration entre deux mondes, avec l'émergence de juristes transdisciplinaires, pouvant utiliser leurs compétences juridiques et techniques dans la création de nouveaux outils.

394. L'avènement de juristes naviguant aussi bien dans le monde juridique que dans le monde technique est une conséquence naturelle de l'émergence de solutions digitales, dont fait partie la démocratisation de la technologie *blockchain* et des *smart contracts*. Une normalisation du langage juridique et du langage technique ne peut être qu'à souhaiter pour permettre de véritables ponts linguistiques et faciliter ainsi la transposition de la loi en code et réciproquement. La présente étude se situe alors dans cette optique d'accompagnement dans

[989] https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf, précité
[990] DANGEARD M., *précité*

la transformation des juristes œuvrant dans l'univers numérique, afin de faire du juriste un levier au profit de l'innovation[991], et en devenir moteur.

395. L'encouragement de cette transformation peut être à l'initiative d'ordres professionnels ; le Conseil supérieur du notariat a su, par exemple, prendre acte de ces enjeux. Considérée pour ses fonctions de registre et de traçabilité, la technologie *blockchain* a sans nul doute des avantages pour faciliter et sécuriser les échanges d'actes. Il est d'autant plus aisé de comprendre les intérêts d'un POC d'une *blockchain* notariale[992], véritable exemple de collaboration entre un monde technique et juridique. D'une manière parallèle à l'utilisation de la *blockchain* au sein des greffes des Tribunaux de Commerce[993], l'utilisation de cette technologie par les notaires permettrait des gains d'efficacité, d'harmonisation et de dynamisation des différents outils qu'ils utilisent. Son actuelle conception a pour but de réaliser une nouvelle utilisation de la *blockchain* pour ses caractéristiques en tant que registre décentralisé, au service d'une modernisation de la transmission d'actes dématérialisés. Comme il est entendu, le but est de parvenir, dans un premier temps, à un réseau uniformisé et décentralisé de données notariales, afin d'en augmenter la traçabilité et favoriser l'échange d'informations, dans l'idée de favoriser l'ouverture et la réutilisation de données avec d'autres professions et services administratifs, notamment les services de publicité foncière. Dans un second temps, profiter de cette traçabilité au bénéfice de la circulation d'actes (sont ici envisagée les copies exécutoires, entendues comme copie d'un acte notarié). Pour prendre un exemple, un notaire dressant un acte de vente pourrait directement se connecter aux services de publicité foncière afin d'accélérer la reconstitution de l'origine de propriété du bien en question. Puis ce même acte de vente serait directement partagé entre l'ensemble des notaires et autres services fonciers concernés. L'utilisation d'une telle *blockchain* permettrait de s'assurer de la fiabilité de l'information ; les caractéristiques d'un tel réseau permettant également de s'assurer de la traçabilité de l'accès aux données.

---

[991] FEUGERE W. *Avocats : développer notre activité, aujourd'hui et demain,* JCP G Semaine Juridique (édition générale), 07/10/2019, 41, pp.1820-1823

[992] Pour plus d'information : Présentation de la *blockchain* notariale (BCN) - Communiqué de presse - Notaires du Grand Paris - 7 juil. 2020, disponible à https://notairesdugrandparis.fr/sites/default/files/2020-07-07%20-%20DP%20-%20Pr%C3%A9sentation%20de%20la%20*Blockchain*%20Notariale%20VF2.pdf (consulté le 08/08/2020)

[993] *Cf. Supra*, p.38

Conclusion du Chapitre 2

396. La complémentarité entre Droit et technique, dans le cadre du droit des nouvelles technologies, et plus largement le droit du numérique, n'est pas superflue, elle est indispensable. Appréhender des objets juridiques, dont la première utilisation se trouve dans un univers numérique, nécessite la compréhension de cet univers. Si cette affirmation porte en premier sur une conception culturelle du numérique, elle doit porter également sur ses caractéristiques techniques. La mise en place d'un dialogue et d'une collaboration entre technique et juridique est un moyen indispensable à la conformité des différents acteurs voguant dans cet univers. La création et la démocratisation des échanges électroniques actuels ont nécessité l'adaptation de règles particulières. La multiplication et l'importance de ces échanges ont nécessité ensuite la construction de nouvelles matières, propres à la sauvegarde des intérêts sociétaux en présence (gouvernance stratégique des données, libres circulations et protection des données). La protection de ces intérêts revenant notamment aux professions juridiques, leur appréhension, voir leur domestication, nécessite alors l'appréhension de compétences nouvelles, gommant petit à petit des frontières pourtant perçues comme hermétiques. L'appréhension du droit pour sa nature linguistique invite alors à l'évolution de ce dernier, et si le code informatique ne peut être aussi qu'un langage, alors l'atténuation des frontières entre les deux ne peut être alors qu'un travail de traduction. Malgré une rapide compréhension de ses intérêts linguistiques, la pierre de Rosette a mis plus de 20 ans à délivrer ses secrets pour permettre la traduction des hiéroglyphes égyptiens. Il peut être permis de s'accorder encore quelques temps pour établir ces éléments de langage commun.

Conclusion du Titre 2

397. L'irruption de l'informatique dans nos sociétés modernes a provoqué des changements profonds de notre société. Les rapports entre individus, entre entreprises, et entre États peuvent être considérés comme reposant sur une seule dimension comportementale. Cette dimension était uniquement fondée sur les rapports entre individus, influencés par des contextes humains, sociaux, culturels ou encore économiques. La démultiplication des supports électroniques, des échanges, et autres moyens techniques, aujourd'hui, guident et influencent ces contextes. Depuis la démocratisation de l'informatique, ces contextes revêtent une nouvelle expression, déterminée radicalement par un amoncellement de 0 et de 1. L'informatique permet, dans une dimension qui lui est propre, une rationalisation des rapports humains et cherchant sans cesse à les exprimer à travers différentes données. La *blockchain*, notamment pour ses fonctionnalités autour des *smart contracts*, peut être entendue comme un de ces nouveaux moyens techniques pour informatiser, automatiser ou encore contrôler ces rapports, cherchant à les exprimer d'une manière aussi radicale que peut l'être l'informatique.

398. Or, une approche fonctionnelle de la donnée est une notion évidemment ambivalente. Si la construction du droit de la donnée peut être discutée, ne serait-ce que pour son opportunité, l'étude et l'appréhension des objets issus de l'univers numérique implique une approche multidisciplinaire pour comprendre et appréhender correctement les conséquences d'une telle volonté de radicalisation. Cette approche est liée à la maîtrise de l'objet en lui-même et aux objets découlant de son utilisation, à savoir les données, personnelles ou non personnelles. Pouvoir manœuvrer dans cet univers numérique et dans la gestion de ces données en appelle alors à un ensemble de cadres, à la fois techniques et juridiques. Si les premiers volumes de données ne pouvaient être que de simples répliques informatiques d'informations « papier », l'économie de la donnée invite au contraire à une utilisation autonome des données, dans un but de création de valeur. L'appréhension de cette nouvelle économie, avec les répercussions sociales ou culturelles qu'elle puisse avoir, doit être prise en compte par les juristes. Si ces derniers ont su progresser en parallèle des changements de la société, il est nécessaire qu'ils entretiennent cette capacité d'évolution propre au numérique.

Conclusion de la Partie 2

399. Si le caractère disruptif de la *blockchain* a pu amener une approche désorganisée, c'est en raison de la multiplicité de ses usages. Néanmoins, une approche ordonnée du droit positif devient limpide lors de la prise en compte du fait que la *blockchain* ne reste qu'un outil au service d'applications pratiques. La *blockchain* pouvant alors être considérée comme disruptive pour l'étendue de ses applications, mais également pour les impacts sociétaux ou juridiques qu'elle peut avoir, éclatant les différentes approches que l'on peut faire d'elle. Toutefois, cet éclatement ne peut être satisfaisant, et le choix d'une approche ordonnée doit être réalisé pour des raisons d'efficacité. La question est alors de savoir de quelle manière construire un raisonnement clair et logique. C'est en ce sens qu'une application sémantique, c'est-à-dire centré sur la définition même des termes et la prise en compte du sens littéraire fondamental d'une notion, trouve intérêt.

Cette application ordonnée se réduit alors sur les fondamentaux d'une *blockchain*, à savoir l'utilisation conjointe d'un logiciel et d'une base de données. S'agissant de ses caractéristiques logicielles, peu d'originalité est à relever. Si l'utilisation de logiciels libres est connue depuis plusieurs décennies[994], la *blockchain* ne fait pas exception dans son utilisation. Et dans le cadre d'une *blockchain* développée à titre privé, le régime classique du logiciel trouvera application. Toutefois, concernant l'aspect relatif aux bases de données, certaines particularités invitent à une nouvelle réflexion, en particulier sur la potentielle cotitularité de qualité de producteur de base de données. À ce titre, la *blockchain* retrouve son caractère disruptif, dans le sens où elle bouscule nos conceptions établies, sur la propriété d'une base de données d'une part, et sur un affaiblissement des monopoles conférés par le droit d'autre part.

400. Toutefois, l'étude seule des fondamentaux d'une technologie n'apparaît pas comme suffisant pour un protocole informatique tel que la *blockchain*. En effet, une application fonctionnelle, qui reste témoin des interactions que la *blockchain* peut avoir, est également nécessaire. Ceci pourrait apparaître comme contraire à la volonté de déconnecter un outil de

[994] MASUTTI C., STALLMAN R., WILLIAMS S., *Richard Stallman et la révolution du logiciel libre*, Eyrolles, 2013

ses applications, néanmoins, ces interactions se situent toujours à un niveau en amont de l'utilisation d'une technologie. Une *blockchain* pouvant être réduite à une technique de gestion de données, ce sont elles qui feront l'objet d'applications. Dès lors, une telle approche fonctionnelle n'est que le prolongement logique d'une approche ordonnée du droit.

401. Les données, si elles peuvent être souvent considérées comme un nouvel « or noir », sont une nouvelle fois ambivalentes, en particulier compte tenu des outils technologiques qui les exploitent. Ces outils peuvent être aussi bien « séduisants[995] » que « menaçants[996] », et une approche protectionniste de la donnée est une notion évidement ambivalente. Une première nuance pouvant s'incarner dans la nature de la donnée, personnelle ou non, et une seconde pouvant s'entendre sur la notion même de protection. Cette protection des données pouvant alors s'analyser d'une part comme corolaire des libertés fondamentales, et d'autre part comme actif essentiel des opérateurs économiques.

S'agissant de la préservation des libertés fondamentales, la *blockchain* peut offrir des garanties supplémentaires à la gestion des données personnelles, notamment en s'assurant de la traçabilité d'accès et d'usage de telles données. Les caractéristiques d'une *blockchain* ne s'opposant pas aux règles de protection des données personnelles. De manière parallèle, la *blockchain* offre également des garanties intéressantes sur le partage de données non personnelles et le respect du récent principe de libre flux des données non personnelles.

402. L'ambivalence de la protection des données dans le cadre de la *blockchain* n'est pas seulement juridique. Elle possède des attributs sociaux, en particulier sur l'évolution des activités juridiques, de plus en plus innervées par la technique. Disruptive également à cet égard, elle invite à une constante adaptation, aussi bien au bénéfice d'une constante et nécessaire sécurisation des échanges électronique, qu'au bénéfice d'une collaboration entre droit et technique.

---

[995] MARINO L., *Le big data bouscule le droit*, Revue Lamy Droit de l'Immatériel, n°99, 1er dec. 2013

[996] *Ibid.*

Conclusion générale

403. Le Droit face aux technologies disruptives sous-entend une réaction singulière face à des régimes existants. Le cas de la *blockchain* ne reste ainsi qu'une application de cette réaction, que cette étude s'est appliquée à circonscrire. L'utilisation de l'adjectif « disruptif » démontre un caractère lié à une temporalité particulièrement courte, car rattachée à la notion de « nouvelles » technologies, et, dans le cadre de cette étude, circonscrite une dimension numérique. Ainsi toute méthodologie d'étude d'objet numérique doit pouvoir répondre à des approches particulières. Cette méthodologie s'illustre à travers un phénomène d'expansion-réduction (I.), desservant un nuage d'interactions (II.).

I. Phénomène d'expansion-réduction

466. Appliqué à un objet, un phénomène d'expansion-réduction peut se définir comme une situation dans laquelle cet objet voit ses applications continuellement étendues, au point qu'une nécessaire circonspection de son champ d'étude est nécessaire pour en réaliser une appréciation qualitative. L'univers numérique, incontestablement, est proéminent. Il fait partie de notre quotidien, et son influence est de plus en plus grande, étendant continuellement ses impacts. L'étude de la *blockchain*, en raison de ce caractère disruptif, possède cette facette expansive, compte tenu de la multiplicité des interactions sociétales qu'elle peut aborder.

467. La *blockchain* peut être considérée comme disruptive du fait qu'elle trouve des applications multiples, le tout dans un but pionnier : finance, contrats, assurance, gestion de données de santé, IA, etc. Ces applications peuvent avoir comme conséquences soit une création d'acquis (par exemple la création du statut du PSAN, ou encore la modernisation des registres notariaux), soit l'avènement de débats plus profonds (disparition des tiers de confiance, automatisations contractuelles, ou encore affranchissement du pouvoir étatique pour la gestion monétaire). Ainsi, la liste des influences, sociales, juridiques, économiques, paraît tellement étendue qu'elle pourrait faire l'objet d'incessantes études. Au-delà, cette expansion induit également la prise en compte d'éléments à caractère politiques, approfondissant encore plus les répercussions possibles. En ce sens, la *blockchain*, en tant que technique d'organisation des données, peut être un argument en faveur de la gouvernance des données, à un niveau national ou européen. La gestion d'une *blockchain* peut être aussi un

témoin de la montée en puissance des régimes de conformité. La possibilité de coder des conditions contractuelles invite également à prendre en compte une numérisation des rapports civils. Néanmoins, cette expansion, gargantuesque, se trouve limitée par elle-même. La conceptualisation de l'ensemble des possibilités d'une *blockchain* se trouve réduite de manière pragmatique. Il importe, pour cela, de dissocier l'outil concerné de ses usages : si la *blockchain* est l'outil visé, le *Bitcoin* n'en est qu'un usage.

468. Invitant à segmenter l'amont et l'aval d'une technologie, la réduction du champ des possibles d'une *blockchain* peut alors s'obtenir par l'étude de ses caractéristiques techniques. Ces dernières pouvant être mises en lumière grâce à la prise en compte du droit positif. Par exemple, soutenir que la *blockchain* peut donner une valeur authentique aux actes enregistrés sur elle revient à nier l'évidence que c'est la qualité seule de son auteur qui peut conférer le caractère authentique d'un acte. Aussi, la gouvernance des données et les régimes de conformité des données se bornent par leur essence : ils restent rattachés à l'acteur qui les met en place, et peuvent donc être cantonnés de la même façon que ses activités le sont. Ainsi, cette expansion doit faire l'objet d'une réduction, même si la tentation de l'exhaustivité n'est pas, et ne doit pas, être un obstacle à son étude. En réalité, l'étude de technologies disruptives s'inscrit dans ce phénomène d'extension-réduction, et permet la définition d'un nuage d'interactions, nécessaire à leur appréhension.

II. Définition du nuage d'interactions

468. L'idée d'un nuage d'interaction n'est pas choisie au hasard. Elle fait directement écho à la notion de *cloud*. Arbitrairement, un *cloud* consiste en la mise en lien de divers matériels, logiciels, et données, interagissant ensemble, selon des caractéristiques propres. Appliqué aux technologies disruptives, ce nuage d'interactions va permettre de circonscrire le précédent phénomène d'expansion-réduction, et ainsi permettre de réduire le champ d'études à ce qui est nécessaire pour l'appréciation d'un objet donné, en particulier lorsqu'il peut être qualifié de disruptif. Un tel nuage peut présenter trois thématiques : sémantique, fonctionnelle, et expérimentale.

469. L'approche sémantique invite à revenir aux fondamentaux : qu'est-ce qu'une *blockchain* ? L'association d'une base de données et d'un logiciel. L'approche fonctionnelle revient à déterminer la vocation d'usage : qu'est-ce que gère une *blockchain* ? Une *blockchain*

gère des données. L'approche empirique conduit à placer l'objet considéré dans un cadre plus sociétal : qu'est-ce qui change ou qu'est-ce qui peut changer grâce à la *blockchain* ?

470. L'idée d'un nuage d'interactions consiste à considérer que ces thématiques s'entrechoquent, se lient, et se complètent. Si la *blockchain* peut être réduite à l'utilisation d'un logiciel et d'une base de données, alors les problématiques liées à l'application des régimes inhérents doivent trouver réponse. En l'occurrence, cette approche sémantique a pu conduire, dans le cadre de cette étude, à réaliser que le droit positif est capable d'appréhender cette technologie, même si certaines adaptations ou réserves peuvent être formulées, par exemple sur la titularité des droits *sui generis* portant sur une base de données. Du fait que la *blockchain* a pour objectif de gérer des données, l'approche fonctionnelle conduit alors logiquement à se poser la question de l'applicabilité des régimes de protection des données personnelles et non personnelles. Pour autant, s'interroger de manière fonctionnelle à propos d'une *blockchain* reste bien déconnecté de l'usage en tant que tel : il n'est pas question de l'utilisation de données, mais bien de leur existence. Dans ce cadre, la *blockchain*, si elle est novatrice pour la méthode de gestion des données, reste parfaitement compatible avec ces régimes. Enfin, l'approche empirique permet de sortir du seul cadre juridique. Si être disruptif provoque une rupture, alors la méthodologie d'approche doit être considérée comme pouvant faire l'objet, elle aussi, d'une rupture. La *blockchain* est un exemple positif en ce sens. Ainsi, la possibilité de *smart contracts* renouvelle le débat « *Code is Law* », et peut d'ailleurs le transcender. L'étude de la *blockchain*, dans cette approche expérimentale, invite non plus à se poser la question de l'existence d'une possible équivalence ou d'un rapport de soumission entre code et droit, mais à considérer et encourager les travaux qui vont dans un sens de collaboration entre droit et technique.

Bibliographie

Textes législatifs et autres normes

1/ Sources officielles françaises

Arrêté du 22 déc. 1981 relatif à l'enrichissement du vocabulaire de l'informatique, JONC 17 janv. 1982, p. 624

Arrêté du 27 juin 1989 pour l'enrichissement du vocabulaire informatique, JO 16 septembre 1989, p11725

Arrêté du 22 mars 2017 relatif au référentiel de sécurité applicable au Système national des données de santé

Ordonnance n°2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations

Ordonnance n°2016-520 du 28 avril 2016 relative aux bons de caisse

Ordonnance n°2018-1125 du 12 décembre 2018

Décret d'application n°2018-1226 du 24 décembre 2018, Journal Officiel du 26 Décembre 2018, texte n° 33

Décret du 30 mars 2001, JO 31 mars 2001, pp. 5070-5072

Décret n°2007-663 du 2 mai 2007 pris pour l'application des articles 30, 31 et 36 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et aux prestations de cryptologie

Décret n° 2019-1118 du 31 octobre 2019 relatif à la dématérialisation des registres, des procès-verbaux et des décisions des sociétés et des registres comptables de certains commerçants

Décret n° 2019-1213 du 21 novembre 2019 relatif aux prestataires de services sur actifs numériques

Décret n° 2020-395 du 3 avril 2020 autorisant l'acte notarié à distance pendant la période d'urgence sanitaire

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

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

Loi n°2004-575, loi pour la confiance dans l'économique numérique du 21 juin 2004, dite loi LCEN

Loi n°2004-800 du 6 août 2004 relative à la bioéthique

Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé

Loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique

Loi n° 2018-670 du 30 juillet 2018

Loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises (1)

Déclaration des Droits de l'Homme et du Citoyen, 1789

Amendement n°CF2, relatif à la transparence, à la lettre contre la corruption et à la modernisation de la vie économique, (N° 3623), Assemblée nationale

Amendement n°227, projet de loi relatif à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique (N°3785), Assemblée nationale

JORF n°0121 du 23 mai 2017 - texte n° 20 - Vocabulaire de l'informatique (liste de termes, expressions et définitions adoptés)

BOFIP-BOI-BNC-CHAMP-10-10-20-40, 03/02/2016

2/ Sources officielles européennes

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

Directive 96/9/CE du Parlement européen et du Conseil du 11 mars 1996 concernant la protection juridique des bases de données, JOCE 27 mars 1996, nº L 77, p. 20

Directive 2001/29/CE relative à l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information

Directive 2004/39/CE du Parlement européen et du Conseil du 21 avril 2004 concernant les marchés d'instruments financiers, modifiant les directives 85/611/CEE et 93/6/CEE du Conseil et la directive 2000/12/CE du Parlement européen et du Conseil et abrogeant la directive 93/22/CEE du Conseil

Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites (Texte présentant de l'intérêt pour l'EEE)

Directive (UE) 2019/790 du Parlement européen et du conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE

OEB, Directives, Partie G, Chapitre II-3 ; version de novembre 2017

OEB, Directives, Partie G, Chapitre II-15, version de novembre 2019

Règlement (UE) 910/2014 du Parlement Européen et du Conseil du 24 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE

Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 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)

Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne

Règlement (UE) 2019/881 du Parlement Européen et du Conseil du 17 avril 2019, relatif à l'ENISA - l'agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n°526/2013 (règlement sur la cybersécurité), dit règlement ENISA.

Encyclopédies et dictionnaires

Algorithme, *Wikipédia* [en ligne], 2021 disponible à l'adresse : https://fr.wikipedia.org/wiki/Algorithme

Attaque des 51%, *Wikipédia* [en ligne], 2021 disponible à l'adresse : https://fr.wikipedia.org/wiki/Attaque_des_51_%25

BATX, *Wikipédia* [en ligne], 2021 disponible à l'adresse : https://fr.wikipedia.org/wiki/BATX

Bitcoin Core, *Wikipédia* [en ligne], 2021 disponible à l'adresse : https://fr.wikipedia.org/wiki/Bitcoin_Core

Chiffrement par décalage, *Wikipédia* [en ligne], 2021 disponible à l'adresse : https://fr.wikipedia.org/wiki/Chiffrement_par_d%C3%A9calage

Crise financière de 2007-2008, *Wikipédia* [en ligne], 2021 disponible à l'adresse :
https://fr.wikipedia.org/wiki/Crise_financi%C3%A8re_mondiale_de_2007-2008,
Cycle en V, *Wikipédia* [en ligne], 2021 disponible à l'adresse :
https://fr.wikipedia.org/wiki/Cycle_en_V
Disponibilité, Wikipédia [en ligne], 2021 disponible à l'adresse :
https://fr.wikipedia.org/wiki/Disponibilit%C3%A9
Free Software Foundation, *Wikipédia* [en ligne], 2021 disponible à l'adresse :
https://fr.wikipedia.org/wiki/Free_Software_Foundation
Histoire des langages de programmation, *Wikipédia* [en ligne], 2021 disponible à l'adresse :
https://fr.wikipedia.org/wiki/Histoire_des_langages_de_programmation
Hyperledger, *Wikipédia* [en ligne], 2021 disponible à l'adresse :
https://fr.wikipedia.org/wiki/Hyperledger
Internet des objets, *Wikipédia* [en ligne], 2021 disponible à l'adresse :
https://fr.wikipedia.org/wiki/Internet_des_objets
Internet, *Wikipédia* [en ligne], 2021 disponible à l'adresse :
https://fr.wikipedia.org/wiki/Internet
Moteur d'inférence, *Wikipédia* [en ligne], 2021 disponible à l'adresse :
https://fr.wikipedia.org/wiki/Moteur_d%27inf%C3%A9rence
Organisation autonome, *Wikipédia* [en ligne], 2021 disponible à l'adresse :
https://fr.wikipedia.org/wiki/Organisation_autonome
Preuve de concept, *Wikipédia* [en ligne], 2021 disponible à l'adresse :
https://fr.wikipedia.org/wiki/Preuve_de_concept
Protocole informatique, *Wikipédia* [en ligne], 2021 disponible à l'adresse :
https://fr.wikipedia.org/wiki/Protocole_informatique,
Révolution numérique
https://fr.wikipedia.org/wiki/R%C3%A9volution_num%C3%A9rique
Scrum, *Wikipédia* [en ligne], 2021 disponible à l'adresse :
https://fr.wikipedia.org/wiki/Scrum
Solidity, *Wikipédia* [en ligne], 2021 disponible à l'adresse :
https://fr.wikipedia.org/wiki/Solidity

Larousse. (s.d.). Algorithme. dans LAROUSSE *en ligne*,
Larousse. (s.d.). Disruptif. dans LAROUSSE *en ligne*,
Larousse. (s.d.). Juriste. Dans LAROUSSE *en* ligne,
Larousse. (s.d.). Moderniser. Dans LAROUSSE *en ligne* :
Larousse. (s.d.). Procédé. Dans LAROUSSE *en ligne*,
Larousse. (s.d.). Protection. dans LAROUSSE *en ligne*,
Larousse. (s.d.). Sécuriser. dans LAROUSSE *en ligne*,
Larousse. (s.d.). Technologie. dans LAROUSSE *en ligne*,
Le Robert. (s.d.). Achèvement. dans LeRobert *en ligne*,

Ouvrages encyclopédiques

Fiches d'orientations, Dalloz :

- Secret des affaires, juin. 2019,
- Circonstances aggravantes, sept. 2020
- Concurrence déloyale, juil. 2019
- Gouvernement d'entreprise, juil. 2019
- Preuve (Droit civil), avr. 2020

GUINCHARD S., *Répertoire de procédure civile, Procès équitable* – Contenu du droit à un juge, Dalloz, Mars 2017 (actualisation : juil. 2020)

LARDEUX G., Répertoire de droit civil, Preuve : modes de preuve, Dalloz, oct. 2019

LATINA M., Répertoire de droit civil, Contrat : généralités - Classifications des contrats, mai 2017 (actualisation : fév. 2020)

LEAGEAIS D., JurisClasseur commercial, Fascicule *Blockchain*, LexisNexis, mai 2018

LUCAS A., Jurisclaseur Propriété littéraire et artistique, Lexisnexis, en ligne

SIRINELLI P. Le Lamy Droit des médias et de la communication, Wolters Kluwer, en ligne

VIVANT M., Le Lamy droit du numérique, Wolters Kluwer, 2020, en ligne

Rapports, délibérations, études et avis

1/ Rapports et études

ADAN, Rapport sur l'état de l'industrie crypto/*blockchain* pendant la crise du Covid-19, juin 2020

AEPD (Agence espagnole pour la protection des données), Introduction to the hash function as a personal data pseudonymisation technique, nov. 2019

ANSSI, Guide agilité & sécurité numériques – méthode et outils à l'usage des équipes projets, oct. 2018

BENSAMOUN A., GABLA E., LEFORESTIER G., Note d'étape, Mission Bases de données, CSPLA, avril 2021

CE, Internet et les réseaux numériques, Collection Études du Conseil d'état, La Documentation française, 1998

CE, Le droit souple, Étude annuelle, 2013

CE, Le numérique et les droits fondamentaux, Étude annuelle 2014

CNIL, Rapport d'activité, La Documentation française, 2017

COMMISSION EUROPÉENNE, Livre vert de la Commission des Communautés européennes sur le droit d'auteur et les droits voisins dans la société de l'information, 1995

DALMAS S., DUVAUT P., GONTHIER G., JACOVETTI G., LANUSSE A., MEMMI G., TUCCI-PIERGIOVANNI S., Les Verrous Technologiques des blockchains, BCom de la DGE, Avril 2021

DARDAYROL J.-P., MARTIN J., ASTOFLI C.-P., BEAUFILS C., Rapport d'information, CSPLA, L'état des lieux de la *blockchain* et ses effets potentiels pour la propriété littéraire et artistique, fév. 2018

DE LA RAUDIERE L., MIS J.-M., Assemblée Nationale, Rapport d'information sur les chaînes de blocs, n°1501, mai 2018

European Parliamentary Research Service, *Blockchain* and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law ? Study - juil. 2019

FAURE-MUNTIAN V., MM. DE GANAY C, LE GLEUT R., Rapport n° 584 (2017-2018),., fait au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, déposé le 20 juin 2018

FFPB, Rapport, Chiffres clés, oct. 2020

France Stratégie, Répondre à l'innovation disruptive, Étude, janv. 2017

MATHIEU B., Réflexions en guise de conclusion sur le principe de sécurité juridique, Cahiers du Conseil Constitutionnel n°11 (Dossier : le principe de sécurité juridique), déc. 2001

MM. MARINI P. et MARC F., Rapport d'information n° 767 (2013-2014), fait au nom de la commission des finances, déposé le 23 juil. 2014, Recommandation du Conseil et annexe (lignes directrices régissant la sécurité des systèmes d'information), 26 nov. 1992

OEB, Talking about a new revolution : *blockchain*, Conference report, dec. 2018

THYRAUD J., Rapport relatif à l'informatique et aux libertés, Senat, Rapport n°72, rapport annexé au procès-verbal de la séance du 10 nov. 1977

Tracfin, Rapport d'activité, ministère de l'Économie et des finances, 2011

TROPER M. Le réalisme et juge constitutionnel, Cahiers du Conseil constitutionnel, n°22 juin 2007

2/ Avis, Délibérations et Propositions

Assemblée nationale, Question n°7619, 24 avril 2018 ; JOAN 9 juil. 2019, p.6465

Avis n°01/2010, Groupe de travail article 29, WP 169

Avis n°05/2014, Groupe de travail article 29, sur les techniques d'anonymisation, adopté le 10 avril 2014

DUBOC S., NOËL D.-J., *Économie et gouvernance de la données*, Avis du Conseil économique, social et environnemental, JO, 10 fév. 2021

Délibération n° 2018-326 du 11 oct. 2018 portant adoption de lignes directrices sur les analyses d'impact relatives à la protection des données (AIPD) prévues par le règlement général sur la protection des données (RGPD)

Délibération n° 2018-327 du 11 oct. 2018 portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise

NAIH, The *opinion of the Hungarian National Authority for Data Protection and Freedom of Information on Blockchain Technology in Contexte of Data Protection,* juil.. 2017, p. 4

OCDE. (2016), *Manuel de Frascati 2015*, : *Lignes directrices pour le recueil et la communication ds données sur la recherche et le développement expérimental*, Mesurer les activités scientifiques, technologiques et d'innovation, OECD Publishing, Paris.

Proposal for a regulation of the european parliament and of the concil laying down harmonised rules on artificial intelligence act and amending certain union legislative acts, 2021/0106 (COD), 21 avr. 2021

Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), 15 déc. 2020

Proposition de Règlement du Parlement européen et du Conseil sur la gouvernance européenne des données (acte sur la gouvernance des données), Bruxelles, le 25/11/2020, final 2020/0340(COD)

Proposition de résolution du Parlement Européen sur les monnaies virtuelles, 2016/2007(INI) - 26/05/2016 Texte adopté du Parlement, lecture

Règlement sur la gouvernance des données – Questions et réponses, Bruxelles, le 25 nov. 2020

Réponse ministérielle., n° 14570 : JO Assemblée Nationale 27/11/2018, page : 10556

Travaux universitaires et de recherche

1/ Mémoires et thèses universitaires

BAUGRAND T., *Le copyleft et la licence art libre,* Mémoire Master Paris II, 2002

BRONZO N., *Propriété intellectuelle et valorisation des résultats de la recherche publique*, Thèse Droit, Université Aix-Marseille, 2011

CASSAR B. *La transformation numérique du monde du droit.*, Thèse Droit, Université de Strasbourg, 2020

CAUSSÉ N., *La valeur juridique des chartes d'entreprises au regard du droit du travail français*, Thèse Droit, Université Aix-en-Provence-Marseille, 1999

DRILLON S., La *protection des logiciels par brevet d'invention*, Thèse Droit, Université de Strasbourg, 2012

RICHARD J., *La divulgation de l'information protégée et les libertés économiques*. Thèse Droit. Université Paris-Saclay, 2018

SELLET E, *Blockchain : vers une upérisation des Offices de propriété industrielle ?* Mémoire de recherche, CEIPI, Université de Strasbourg, 2018

ZLOTYKAMIEN C., *Blockchain et Propriété Littéraire et Artistique*, Mémoire de recherche, CEIPI, 2017

2/ Travaux de recherche

BARBAROUX N., BARON R. FAVREAU A., *Blockchain et finance – approche pluridisciplinaire,* 2020

DE COËTLOGON P., DURAND M., JEANTET M., GÉNON C., RAMON R. Et al. P, *Les technologies blockchain au service du secteur public.*, Rapport de recherche, Université de Lille, juin 2021

FINCK M., *"Blockchain Regulation", Max Planck Institute for Innovation and Competition* Research Paper Series No 17-13 SSRN Network, 2017

GESLIN A., *La circulation des modèles normatifs ou la pensée juridique du mouvement. In.* BOURGUES P., MONTAGNE C. (dir.), La circulation des modèles normatifs, PUG, 2016

GOEDERT N., MAILLARD N., *Énoncer le droit, représenter le droit*., Le droit en représentation(s), Mare et Martin, coll. "Libre-droit", 2017

KONDRATUK L., *Disputer, codifier, coder*. 2018

LAUF A., *Propagation du buzz sur Internet - Identification, analyse, modélisation et représentation dans un contexte de veille. Institut National des Langues et Civilisations Orientales* – Inalco Paris – Langues O', 2014

MOULIN F., *Innovation et invention, comparaison du point de vue juridique*, janv. 2010

Policy Department for Economic, Scientific and Quality of Life Policies, Cryptocurrencies and blockchain,, July 2018

SERVERIN E., BEROUJON C. BRUXELLES S., *Classer, coder,* Rapport de recherche, Ministère de la Justice. 1988

W. CHOHAN U., *The Double Spending Problem and Cryptocurrencies*, UNSW Business School ; Critical Blockchain Research Initiative (CBRI) ; Centre for Aerospace & Security Studies (CASS), dec. 19, 2017

WRIGHT A. et DE FILIPPI P., *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, 10 mars 2015

Monographies

ANTONOPOULOS A., *Mastering Bitcoin : Programming the Open Blockchain*, 2ème édition, 2017

ASIMOV I., *Le cycle de Fondation, tome 1 : Fondation*, Galimard-Jeunesse, 1951

ATIAS C., *Droit civil, les biens*, Litec, 2000

BARBET-MASSIN A., FLEURET F., LOURIMI A., O'RORKE W, PION C., *Droit des cryptoactifs et de la blockchain*, Lexisnexis, 2020

BENSOUSSAN A., *Informatique Télécoms Internet*, 5ème édition, Editions Francis Lefebvre, 2012

BERTRAND A-R., *Droit d'auteur*, Dalloz action, 2020

BETBÈZE J-P., *Les 100 mots de l'économie*, collection Que sais-je, PUF, 2019

BINCTIN N., *Droit de la propriété intellectuelle*, LGDJ, 4e éd., 2016

BITAN H., *Droit des créations immatérielles*, Wolters Kluwer, 2010

BLOCKCHAIN FRANCE, *La blockchain décryptée - les clefs d'une révolution*, Netexplo, juin 2016.

BODIN J., *Les six livres de la République*, 1576

BUFFARD P., préface, *Code Informatique, Fichiers et Libertés*, Editions Larcier, 2014

CARBONNIER J., *L'inflation des Lois, in Essais sur les lois*, Defrénois, 1979

CORNU G., *Vocabulaire juridique*, PUF, collec. Quadrige, 8e éd., 2007

DE FILIPPI P., REYMOND M., *La blockchain : comment réguler sans autorité* ? In : NITOT T. (dir.) & CERCY N., Numérique : reprendre le contrôle, Framabook 2016

DOUEIHI M., Qu'est-*ce que le numérique ?*, PUF, 2013

DULONG DE ROSNAY M., *Les Golems du numérique. Droit d'auteur et Lex Electronica*, Paris, Presses des Mines, Collection Sciences sociales, 2016

EDELMAN B., *Le triomphe des investisseurs*, La propriété littéraire et artistique, PUF, 2008

ÉLOI L., *Économie de la confiance*, collection Repères, 2019,

FERAL-SCHUHL C., *Praxis Cyberdoit*, Dalloz, 2020-2021

FRAYSSINET E., *La cybercriminalité en mouvement*, Hermès, 2012

GAUDRAT P., SARDAIN F., *Traité de droit civil du numérique - Tome 1 - Les biens*, éditions Larcier, 2015

GAUTIER P.-Y., *Propriété littéraire et artistique*, 11ème édition, 2019, éditions PUF

GAY C., Management de l'innovation, Dunod, 2017

GHERNAOUTI S., *Sécurité informatique et réseaux*, Paris, Dunod, 2013

GRYNBAUM L., LE GOFFIC C., MORLET-HAÏDARA L., *Droit des activités numériques*, 1ère édition, Dalloz, 2014

H. CORMEN T., *Algorithmes - Notions de bases*, DUNOND, 2013

HAURIOU M., *Précis de droit administratif et de droit public*, 1ère édition 1892, rémiz. Dalloz 2002

HOBBES T., *Léviathan*, 1651

KINSCH P., *Entre certitude et vraisemblance, Le critère de la preuve en matière civile, in* De Code en Code, Mélanges en l'honneur de G. Wiederkehr, Dalloz, 2009

LAVOISIER A., *Traité élémentaire de Chimie*, 1789

LE TOURNEAU P., *Contrats informatiques et électroniques*, Dalloz Référence, 10ème édition, 2018-2019

LESSIG L.,

- *Code, and Other Laws of Cyberspace*, Basic Books, 1999
- *L'Avenir des idées : Le sort des biens communs à l'heure des réseaux numériques*, Presses universitaires de Lyon, sept. 2005

LOQUIN E., *L'amiable composition en droit comparé et international*, Litec, 1980

MACREZ F., *Créations informatiques : bouleversement des droits de propriété intellectuelle ? Essai sur la cohérence des droits*, collection CEIPI, 2011, Lexisnexis

MALINVAUD P., *Introduction à l'étude du droit*, LexisNexis, 8e éd., 2018

MARINO L., *Droit de la propriété industrielle*, Les mémentos Dalloz, 8ème édition, 2013

MARTIAL M., *État-gendarme*, dans : KADA N., éd., *Dictionnaire d'administration publique*, Presses universitaires de Grenoble, Droit et action publique, 2014

MÉADEL A., MUSIANI F., *Abécédaire des architectures distribuées*, Presse des Mines, 2015

MEKKI M., *Le droit de l'intelligence artificielle*, Lextenso, 2019

MERRIEN F.-X., *L'État-providence.*, Presses Universitaires de France, Que sais-je ?, 2007

MOATTI A., *Le numérique rattrapé par le digital ?*, Le Débat, Gallimard, 2016.

MONJEAN-DUCAUDIN S., *De la jurilinguistique à la juritraductologie. Comparaison des approches canadienne et européenne. Coder-décoder : linguistique et concepts juridiques*, Éditions Yvon Blais, 2019

NETTER E., *Droit et numérique, Numérique et grandes notions du droit privé*, CEPRISCA, 12 fév. 2019

NOCETTI J., *La gouvernance mondiale d'Internet à la croisée des chemins*, Enjeux numériques, n° 4, Annales des Mines, déc. 2018

SADIN E., *La silicolonisation du monde : l'irrésistible expansion du libéralisme numérique*, L'échappée, 2016

SUPIOT A.,

- *Homo juridicus, essai sur la fonction anthropologique du Droit*, Essais, Editions du Seuil, 2005
- *La gouvernance par les nombres* (Essais), Fayard, 18 mars 2015

SWARTZ A., *Celui qui pourrait changer le monde*, préface LESSIG L., B42, 2017

SZABO N., *Formalising and securing relationships on public networks*, *First Monday*, Volume 2, Number 9 - 1 sept. 1997

TOULLIER C., BONAVENTURE M., Le droit civil français, suivant l'ordre du code…, Paris, Warée, 1824, n° 3

TOULLIER C., BONAVENTURE M., *Le droit civil français, suivant l'ordre du code…,* Paris, Warée, 1824, vol. n° 3

VIVANT M. et BRUGUIERE J.-M., *Droit d'auteur*, Précis, Dalloz, 2009, 1re éd.

WIENER N., *Cybernétique et société. L'usage humain des êtres humains*, 10-18, 1962, 250 p., édition originale : Cybernetics and Society, 1954

Doctrine et chroniques

AKODAH A., *La preuve des actes juridiques sous le prisme des contrats électroniques*, Revue Lamy Droit de l'immatériel, 45, 1er sept. 2009

AKSABI M., *Le droit financier au défi de l'IA et de la cybersécurité*, Revue Droit et patrimoine, 1 janv. 2020, n°298, pp.51-55

AMMAR D., *Preuve et vraisemblance. Contribution à l'étude de la preuve technologique*, RTD civ. 1993. p.499

ARROW K., *Economic welfare and the allocution of ressources for invention. The rate and direction of inventive activity : economic and social factors*, National Bureau of Economic Research, 1962

ATSARIAS-DUMAS S., *Le contrôle du contrat par l'Autorité de la concurrence*, AJ Contrat 2020, p.474

AUDIT M., *Le droit international privé confronté à la blockchain*, Revue critique de droit international privé 2020, p.669

BARBET-MASSIN A. DAHAN V., *Les apports de la blockchain en droit d'auteur*, BRDA n°8-2018, Francis Lefebvre, pp.21-25

BARBET-MASSIN A., KHATAB A., *Les « brevets blockchain » : état des lieux et perspectives*, 2018, Expertises, 435, p.176

BARRAUD Boris, *Les blockchains et le droit*, Revue Lamy droit de l'immatériel, n° 147, avr. 2018, pp. 48-62.

BARSAN I., *Blockchain et propriété intellectuelle*, Revue Communication et commerce électronique, Lexisnexis, Avril 2020, n°4

BENHAMOU Y., *Réflexions sur l'inflation législative*, Recueil Dalloz 2010 p.2303

BENSAMOUN A., GROFFE J., *Création numérique – L'influence du numérique sur l'objet du droit*, Répertoire Dalloz IP/IT et Communication / Création numérique Civ., oct. 2013

BENSSOUSSAN A., *Risque juridique, conformité, diversité et classification des risques*, https://www.alain-bensoussan.com/wp-content/uploads/22919251.pdf

BINCTIN N., *TDM : un enjeu de l'intelligence artificielle*, RIDA 2019, nº 262, p. 5.

BOCQUILLON S., CAMUS R., *L'opportunité d'une gouvernance transverse des données*, Revue Banque, n°810, Juillet-Août 2017

BOEV I., *Le nouveau règlement : un 5e principe de libre circulation ?*, Dalloz IP/IT 2020, p.223

BOUGEARD A. *Les dispositions relatives à l'accès et au portage des données : code de conduite et bonnes pratiques*, Dalloz IP/IT 2020, p.408

BOUGLON T., Obligation *de déchiffrement d'un moyen de cryptologie et respect du droit de ne pas contribuer à sa propre incrimination : quelle issue à prévoir en cas de contentieux français devant la CEDH ?*, Revue Lamy droit de l'immatériel, n°181, 1er mai 2021

BOUNOT V., La *blockchain, outil de gouvernance et de traçabilité du processus créatif (R&D)*, Revue Lamy Droit des affaires, 1er septembre 2019, n°151, pp. 41-48

BRAIBANT G., questions *d'ordre politique soulevées par la protection des données et des libertés individuelles*, p178. OCDE

BRUGIERE J-M., FAUCHOUX V., QUIQUEREZ A., *Actualité du droit des technologies nouvelles*, Revue Lamy Droit civil, n°184, 1er sep. 2020

BRUNELLE A., *Éloge de la confiance : la Blockchain, l'entreprise et le droit de la concurrence*, Revue Lamy de la Concurrence, 01/12/2019, 89, pp.31-36

BÜKLE J., MAHIEU R., *Le "contract management" : une vision innovante des contrats d'affaires*, Revue Lamy Droit civil, n°158, 1er avril 2018

BYK C., La *souveraineté numérique à l'heure de la gouvernance mondiale*, Dalloz IP/IT 2020 p.337

CANAS S., *Blockchain* et preuve. Le point de vue du magistrat, Dalloz IP/IT, 01/02/2019, 2, pp.81-84

CAPRIOLI E.,

- *La blockchain ou la confiance dans une technologie*, La Semaine Juridique, édition générale, n°23, 6 juin 2016, 672
- *Mythes et légendes de la blockchain face à la pratique*, Dalloz IP/IT 2019, p.429

CARON C.,

- À *la recherche d'un jus unum de l'Internet*, Communication Commerce électronique n° 6, Juin 2017, repère 6
- *Les licences de logiciels dits ''libres'' à l'épreuve du droit d'auteur français* - Recueil Dalloz 2003, p.1556

CARRE S., Libre *circulation des données, propriété et droit à l'information : à propos du règlement (UE) 2018/1807 du 14 novembre 2018*, Dalloz IP/IT 2020, p.228

CASTETS- RENARD C., La *protection des producteurs de bases de données contre l'extraction des données par un logiciel*, Revue Lamy Droit de l'Immatériel, n°56, 1er janv. 2010

CASTILLO-WYSZOGRODZKA S., RIFFARD J-F., *"Introduction", Le Dossier : La transsystémie. Pour une approche rénovée de la conception et de l'enseignement du droit, Actes du colloque de Clermont-Ferrand des 12 et 13 décembre 2016*, textes réunis par J-F. Riffard et S. CastilloWyszogrodzka, La Revue du Centre Michel de l'Hospital [édition électronique], 2019, n° 17, pp. 8-10. La Revue du Centre Michel de l'Hospital - édition électronique, Centre Michel de l'Hospital CMH EA 4232, 2019, pp. 8-10.

CHANTEPIE G., Le *droit en algorithmes ou la fin de la norme délibérée ?*, Dalloz IP/IT 2017. 522

CHARPIAT V., *Le Bitcoin devient monnaie courante : les monnaies digitales entre transparence, régulation et innovation*, Revue des Juristes de Sciences Po, n°9, juin 2014, 96

CIRAY H., *Du contrôle de loyauté d'un système de traitement automatisé de données personnelles*, Dalloz actualité, 02 juil. 2018

CLÉMENT-FONTAINE M., *Le smart-contract et le droit des contrats : dans l'univers de la mode*, Dalloz IP/IT 2018, p.540

CREUX-THOMAS F., Transition *numérique et diffusion de l'information juridique : de nouveaux défis*, Revue pratique de la prospective et de l'innovation n° 2, oct. 2017, dossier 14

CROZE H., Comment *être artificiellement intelligent en droit*, La Semaine Juridique Edition Générale n° 36, 4 sept. 2017, 882

CULLAFFROZ-JOVER S., BACQ E., *Blockchain et données à caractère personnel, l'improbable conciliation ?* Droit et patrimoine, 01/04/2019, 290, pp.28-30

DANGEARD M., *Il est temps que les juristes deviennent des juristes-codeurs, et se mettent à collaborer sur les contrats*, Revue pratique de la prospective et de l'innovation n° 2, oct. 2017, entretien 5

DE QUENAUDON R., *Un code de conduite des affaires en quête de statut juridique, commentaire de l'arrêt rendu par la Cour d'appel de Versailles, 17 avril 2008*, RDT 2009, pp.311-315.

DE VAUPLANE H.,

- *Blockchain : la question de la preuve par consensus au cœur de la gouvernance*, Revue Banque, n°796
- *Blockchain and Conflict of Laws*, RTDF 2017, pp.50-52
- *Financement des entreprises par la blockchain*, RTDF 2016, n°2, p.64
- *Introduction Blockchain, cryptomonnaies, finance et droit : état des lieux*, Revue Lamy droit des affaires, n°140, 1er sep. 2018

DEJEAN S, PENARD T. et SUIRE R., Une *première évaluation des effets de la loi Hadopi sur les pratiques des internautes français*, 2010

DELZANNA C., Trois *questions à Caroline Jeanson*, Droit et patrimoine l'hebdo, 1052, 18 avril 2016

Dépêches JurisClasseur, *La fédération des tiers de confiances lance un groupe de travail sur la blockchain*, 29 avril 2016

DERIEUX E., *Souveraineté à l'ère du numérique*, Revue Lamy Droit de l'immatériel, 156, 1er fév. 2019

DEROULEZ J., *L'actualisation des enjeux liés aux données personnelles*, Revue Lamy Droit de l'Immatériel, n°156, 1er fév. 2019

DESCHANEL C., *L'instauration d'un droit de propriété des données personnelles : vrai danger ou fausse utilité ?*, Revue Lamy Droit de l'Immatériel, n°156, 1er fév. 2019

DEVEZE J., *vive l'article 1322 !, Commentaire critique de l'article 1316-4 Code civil, in* Études offertes à P. CATALA, Litec 2001 p.531.

DIALLO, M., *L'intelligence artificielle et le dispositif de conformité des banques*, RISF, 01/01/2020, 2020-1, pp.88-94

DOISY M., DAOUD E., *La violation des règles éthiques internes peut justifier un licenciement pour faute grave*, Editions Législatives, juil. 2020

DOUVILLE T.,

- *Blockchain et protection des données à caractère personnel*, AJ Contrats d'affaires-concurrence-distribution, 01/07/2019, 7, pp.316-323
- *Blockchains et preuve*, Recueil Dalloz, D. 2018. 2193
- *Le contrat en matière de responsabilité conjointe de traitement des données*, Dalloz IT/IP 2021, p.188

DRILLON S., La *révolution blockchain. La redéfinition des tiers de confiance*, RTD com. 2016. 893.l

DUPAYS A., Transmission *au CSE d'une information précise et écrite*, Le Lamy social, §4496

ELVY T.-A., Paying *for Privacy and personal data economy*, Columbia Law Review, Vol. 117, nº 6, oct. 2017, p.1405 et s.

ENCINAS DE MUNAGORRI R., *Qu'est-ce que la technique juridique ? : Observations sur l'apport des juristes au lien social*. Recueil Dalloz, Dalloz, 2004, pp.711-715

ÉRÉSÉO N., Libre *circulation des données et droit de la concurrence (à propos du règlement du 14 novembre 2018 relatif à la libre circulation des données non personnelles)*, Dalloz IP/IT 2020, p.414

F. MACLEAN, *Governing The Blockchain : How to determine applicable law*, (2017), 6 JIBFL 359, spéc. p. 361

FAUCHOUX V., GOUAZÉ A., *Pourquoi la blockchain va révolutionner la propriété intellectuelle ? Application pratique au secteur de la mode*, Propriétés intellectuelles, oct. 2017, n°65

FAVREAU A.,

- *Blockchain – Aspects techniques*, Répertoire IP/IT Communication, Dalloz, sept. 2021
- *L'état au défi des blockchains, régulation(s) et usages publics de la technologie blockchain*, RFPI, numéro spécial, fév. 2021
- Les *outils technologiques de légitimation de la propriété intellectuelle*, Légipresse 2019, p.21

FAVRO K.,

- *Introduction, Open Data : une révolution en marche*, Legicom 2016, p.3
- *La démarche de compliance ou la mise en œuvre d'une approche inversée*, Legicom 2017, p.21
- Les *données non personnelles : un nouvel objet juridique*, Dalloz IP/IT 2020, p.234

FENOUILLET D., *La loi, le juge et les mœurs : la Cour de cassation aurait-elle emménagé rive gauche ?*, RDC 2005. 1284

FEUGERE W. *Avocats : développer notre activité, aujourd'hui et demain*, JCP G Semaine Juridique (édition générale), 07/10/2019, 41, pp.1820-1823

FONTAINE M.,

- *L'acte authentique électronique : état des lieux et perspective*, Revue Lamy Droit civil, 01/11/2019, 175, pp.32-34
- *La donnée numérique : l'or noir du XXIe siècle ?* LPA 8 sept. 2017, n° 129, p. 90

FRISON-ROCHE M.-A.,

- *Du Droit de la Régulation au Droit de la Compliance*, Working Paper, http://mafr.fr/fr/article/du-droit-de-la-regulation-au-droit-de-la-compliance/
- *Le Droit de la compliance, D.*2016, Chron., 29 sept. 2016, n°3

G'SELL F.,

- *Remarques sur les aspects juridiques de la souveraineté numérique*, Revues des Juristes de Sciences Po n°19, Oct. 2020, 13
- *Vers l'émergence d'une responsabilité numérique ?*, Dalloz IP/IT 2020. p.153

GAUDEMET A., *Qu'est-ce que la compliance ?*, Revue Commentaire 2019/1 (Numéro 165), pp.109-114,

GAUDRAT P.,

- *Droit des nouvelles technologies*, RTD Com. 1999, p.104
- *Droits et obligations de l'utilisateur d'une banque de données*, Brise, n^{O} 12, CNRS éd., nov. 1988
- *La protection des logiciels par le droit d'auteur : Bilan et perspectives*, RIDA oct. 1988, p. 77, no °19 et n°22.

GAUTRAIS V. *Les sept péchés de la blockchain : éloge du doute !*, Dalloz IT/IP 2019, p.432

GIRAUD T., *Vie culturelle - La blockchain est-elle l'avenir de la culture ?*, JAC 2017, n°51, p.35

GOSSA J., Les *données non personnelles : un tech checking.*, *Dalloz IP/IT*, Dalloz, 2020, pp.213-217

GUERLIN G., *Considérations sur les smarts contracts*, Dalloz IP/IT, p.512

GUICHARDAZ R, PÉNIN J., *L'économie de la réutilisation des données (non personnelles)*, Dalloz IP/IT 2020, p.218

HAAS G., TORELLI M., *Annonceurs et RGPD : faux amis, frères ennemis, l'exemple des cookies publicitaires*, Revue Lamy Droit des affaires, n°168, 1er mars 2021

HADDAD S., CARLER F., CASANOVA A., Le *débat est (enfin) tranché : le non-respect des termes du contrat de licence de logiciel est une contrefaçon*, Revue Lamy Droit de l'Immatériel, n°167, 1er fév. 2020

HAGEL F., Secrets *et droits de propriété intellectuelle : un tour d'horizon*, Revue Lamy Droit de l'immatériel, n°53, 1er oct. 2009

HASSLER T., *Qualification du multimédia : plaidoyer pour une méthode de qualification*, CCC nov. 2000, p.10

HIELLE O., La *technologie Blockchain : une révolution aux ombreux problèmes juridiques*, Dalloz Actualités, 31 mai 2016

HUET J., *La modification du droit sous l'influence de l'informatique : aspects de droit privé* ; JCP G 1983 n°I, 3095

IDOT L., *Information et droit de la concurrence*, Revue Lamy droit des affaires, n°60, 1er mai 2003

ISAAC H. *La donnée, une marchandise comme les autres* ?, Annales des Mines - Enjeux Numériques, Conseil général de l'Économie, ministère de l'Économie et des Finances, 2018

JAULT-SESEKE F., La *blockchain au prisme du droit international privé, quelque remarques*, Dalloz IP/IT 2018, p.554

JEAN B., DE FILIPPI P. *Les Smart contracts, les nouveaux contrats augmentés ?* Conseils et Entreprises, Avocats Conseils d'Entreprise, 2016

JOURDAIN P., Clauses *restrictives de responsabilité et obligation essentielles : une précision et des incertitudes*, RTD Civ. 2008, p.310

JULLIEN N., ZIMMERMANN J.-B. *Le logiciel libre : une nouvelle approche de la propriété intellectuelle.* In : *Revue d'économie industrielle*, vol. 99, 2e trimestre 2002

LABBE T., *L'état au défi des blockchains, régulation(s) et usages publics de la technologie blockchain*, RFPI, numéro spécial, fév. 2021

LAFAYE L., Pour *l'ouverture des données privées*, Expertises, avril 2020

LAMPORT L., SHOSTAK R. et PEASE M., The *Byzantine Generals Problem*, ACM Transactions on Programming Languages and Systems, vol. 4, no 3, juil. 1982

LATIL A., *L'interdisciplinarité chez les juristes*, Revue pratique de la prospective et de l'innovation n° 2, oct. 2019, dossier 17

LAURENT-BONNE N., *La re-féodalisation du droit par la blockchain*, Dalloz IP/IT 2019, p.416

LAVAYSSIERE X., L'émergence *d'un ordre numérique*, AJ Contrat 2019, p.328

LE CLAINCHE J., *Données personnelles, vie privée, et non-discrimination : des protections complémentaires, une convergence nécessaire*, Revue Lamy Droit de l'Immatériel, n°90, 1er fév. 2013

LE GOFFIC C., *Licences libres et copyleft : la contractualisation du droit d'auteur*, Revue Lamy Droit de l'immatériel, n°77, 1er déc. 2011

LE TOURNEAU P., *Du particularisme de l'obligation de conseil*, Dalloz référence Contrats du numérique, Chap. 014, 014.11 - 014.14, 2021/22

LE TROCQUER A-H., *Blockchain, gouvernance d'entreprise et infrastructures de marché*, Revue Lamy droit des affaires, n°129, 2017

LEBKIRI A., *La propriété industrielle et la transformation numérique de l'économie*, Regards d'experts, INPI, 2015

LEFEVRE A. *La mise à disposition de copies de logiciels (…) de l'éditeur sur ces copies*, Revue Lamy Droit de l'Immatériel, n°85, 1er août 2012

LEGEAIS D. *Pool bancaire*, RTD Com 2007, p.429

LÊMY G., La *gouvernementalité de blockchains publiques*, Dalloz IP/IT, 01/09/2019, 9, pp.497-502

LOCKETT-YEUNG, K., *'Regulation by blockchain : the emerging battle for supremacy between the code of law and code as law'* Modern Law Review, 2018

LOUVET N., *Les apports de la blockchain et des actifs numériques au secteur financier*, Dalloz IP/IT 2019 p.546

MACREZ F.,

- *Logiciel : le cumulard de la propriété intellectuelle*, Thèmes et commentaires, Dalloz, 2011
- *Logiciel et brevetabilité : Recherche clarté désespérément*, RLDI 2019/51, nº 1663

MAGNIER V., Enjeux *de la blockchain en matière de propriété intellectuelle et articulation avec les principes généraux de la preuve*, Dalloz IT/IP 2019, p.76

MAKROUM N., FONTAINE C., *La prise en compte de la blockchain par l'arbitrage international en ligne*, Club de l'arbitrage, 7 oct. 2020

MALAURIE-VIGNAL M., *Enjeux et défis de la blockchain dans ses relations avec la propriété intellectuelle*, Dalloz IP/IT 2018 p.531

MARINO L., *Le big data bouscule le droit*, Revue Lamy Droit de l'Immatériel, n°99, 1er déc. 2013

MBIDA ELONO T., Débat *doctrinal sur la juridicité et l'hypothèse d'une appréhension tridimensionnelle du droit*, Revue Pluridisciplinaire Africaine de l'environnement, Association Jeunesse Africaine pour l'environnement, 2021, La sécurité alimentaire et les défis agricoles en temps de crise : regards croisés Afrique-Europe.

MEKKI M.,

- Le *contrat, objet des smart contracts (Partie 1)*, Dalloz IP/IT 2018, p.409
- Le *juge et la blockchain : l'art de faire du nouveau vin dans de vieilles outres*, disponible à https://mustaphamekki.openum.ca/files/sites/37/2019/10/5.Mekki-juge-et-*blockchain*.pdf,
- *Le smart contract, objet du droit (Partie 2)*, Dalloz IP/IT 2019, p.27

MERCIER D-J., *Du chiffrement de César à la mathématique de la carte bancaire.* Repères IREM, 2002, pp.59-90

MIS J-M., *Les technologies de rupture à l'aune du droit* – Dalloz IP/IT 2019. p.425

MONTANT L., *Legal design : vers une transformation radicale de l'expérience client des cabinets d'avocats*, Dalloz Actualité, 17 déc. 2020

MOULY-GUILLEMAUD C., *Nul ne peut se constituer de titre à soi-même... C'est-à-dire ?* RTD civ. 2018. 45

MOUNOUSSAMY L., *Le smart contract, acte ou hack juridique ?* LPA 20 févr. 2020, n° 150, p.12

MOUSSERON J.-M., *La gestion des risques par le contrat*, RTD civ. 1988. 481

NAVARRO P., ZANNOTTI F., Souveraineté *et surveillance, les enseignements tirés de l'affaire du Health Data Hub,* Revue Lamy droit de l'immatériel ex Lamy droit de l'informatique, 01/12/2020, 176, pp.9-12

NETTER E. *Le code du travail numérique. Intelligence artificielle, gestion algorithmique et droit du travail*. Les travaux de l'AFDT, Dalloz, 2020

NEVEJANS N., *Le robot, responsable ? À propos de la Première Loi de la Robotique d'Asimov,* Revue Francophone de la Propriété Intellectuelle, 01/03/2020, NS, pp.15-29

O'RORKE W., L'émergence *d'un droit de la blockchain*, Dalloz IP/IT 2019. p.422

PADOVA Y., Entre *patrimonialité et injonction au partage : la donnée écartelée ?*, Revue Lamy Droit de l'Immatériel, n°155, 1er janv. 2019

PEREIRA B., Chartes *et codes de conduite : le paradoxe éthique*, La Revue des Sciences de Gestion, 2008/2 (n° 230), pp.25-34.

PETEL A., Publication *de l'Acte sur la gouvernance des données : les propositions de la Commission européenne*, Revue Lamy Droit de l'Immatériel, n°176, 1er déc. 2020

PETIT A., *Visite guidée du Darkweb cybercriminel*, Dalloz IP/IT 2017 p.86

PFISTER C., *Monnaies digitales : du mythe aux projets innovants*, Le Bulletin de la Banque de France n°230 : Article 1

POUILLET Y., *La troisième voie, une voie difficile*, Revue Lamy Droit de l'Immatériel, n°182, 1er juin 2021

QUÉMÉNER M., Virus *et pandémie numériques : actualités en matière de cyberattaques*, RPPI n°2, oct. 2020, dossier 14

RANÇON E., Nouvelle *précision sur le champ du droit de communication au public*, CJUE, 2 avr. 2020, aff. C-753/18, Revue Lamy Droit de l'Immatériel, n°171, 1er juin 2020

RAYNARD J.,

- *Le tiers au pays du droit d'auteur*, JCP, 1999 I 138, n°7 et suiv.
- *Le contenu et la particularité de la protection*, Propriété industrielle, 2018, dossier 3

RAYNOUARD A., *Adaptation du droit de la preuve aux technologies de l'information et à la signature électronique. Observations critiques*, Defrénois 2000. 593.

RODA J-C., *Smart contracts, dumb contracts ?* Dalloz IP/IT 2018, p.397

ROUSSILLE M., Le *Bitcoin : objet juridique non identifié*, Revue Banque & Droit, n°159, janv.-fév. 2015

ROUVROY A., BERNS T., *Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ?, Réseaux*, 2013/1 (n° 177), pp.163-196

SAENKO L., *Le Darkweb : un nouveau défi pour le droit pénal contemporain*, Dalloz IP/IT 2017 p.80

SCHREPEL T. *Ententes algorithmiques et ententes par blockchain*, Recueil Dalloz, D. 2020, 1244

SERRANO E. *Village Legaltech 2019 : En marche vers le juriste augmenté*, Revue Option Droit et affaires, 04/12/2019, 471, pp.2-3

SOULAS DE RUSSEL D, RAIMBAULT P. *Nature et racines du principe de sécurité juridique : une mise au point. In* : Revue internationale de droit comparé. Vol. 55 N°1, jan.-mars 2003. pp. 85-103

SOUTY F., *Entreprises, concurrence, conformité : définition empirique de la compliance*, Revue Lamy de la concurrence, Nº 55, 1er nov. 2016

TAMBOU O. *L'Introduction de la certification dans le règlement général de la protection des données personnelles : quelle valeur ajoutée ?* Revue Lamy Droit de l'immatériel, Lamy (imprimé) / Wolters Kluwer édition électronique 2016, 2016 (126), pp.43-48

THEOCHARIDI E., *La conclusion des smart contracts : révolution ou simple adaptation ?*, Revue Lamy Droit civil, n°161, 1er juillet 2018

TOUATI A., *Tous les contrats ne peuvent être des smarts contracts,* Revue Lamy Droit civil, n°147, 1er avril 2017

VABRES R., *Bons de caisse, minibons, blockchain…résurrection ou révolution*, Revue droit des sociétés 2016, repère n°7

VAMPARYS X., *Blockchain* : quelques réflexions sur la confiance 2.0, JCP E Semaine Juridique (édition entreprise) - 11/10/2018, 41, pp.47-49

VERBIEST T., RICHEBOURG D., Blockchains et financement de l'immobilier, AJDI 2019. 423

WATIN-AUGOUARD M., *La cybersécurité, enjeu de la souveraineté à l'ère numérique*, Dalloz IT/IP, 2021, p.130

WICKERS T., *Peut-on coder le droit* ?, Cahier de droit de l'entreprise, n°4, juil.-août 2019

ZOLYNSKI C.,

- La *place du règlement (UE) 2018/1807 dans la construction du droit des données de l'Union européenne*, Dalloz IP/IT 2020 p.429
- *Un nouveau droit de propriété intellectuelle pour valoriser les données : un miroir aux alouettes ?*, Dalloz IP/IT 2018 p.94

ZORN C., Le *jeu de données composites : données personnelles et (en même temps) non personnelles ?*, Dalloz IP/IT 2020 p.420

Articles de presse

BOBÉE F., *Blockchain et santé : présentations et cas d'usages,* Bitconseil, 3 juil. 2019

BOHIC C., *LaBChain : le consortium blockchain de la Caisse des dépôts joue sur l'effet de masse, ITespresso, 17 fév. 2017*

BOSSARD O., Que savons-nous de Satoshi Nakamoto, l'inventeur du Bitcoin ?, Forbes, 23 avr. 2019

CHICHEPORTICHE O., La Chine provoque une nouvelle chute du bitcoin, BFM Business, 24/05/2021

CLARK B. Blockchain et droit de la propriété intellectuelle : une combinaison idéale au pays de la cryptographie ?, OMPI Magazine, fév. 2018

D'ASSIGNIES R., LECARDONNEL M. *Responsabilités et logiciels libres,* Agence pour la Protection des Programmes, 2021

DAOUI L., *Notaires du Grand Paris : présentation du tout premier dispositif de blockchain notariale,* Affiches Parisiennes, 7 juil. 2020

DAVID F., *Un économiste accuse Elon Musk d'avoir manipulé le prix du bitcoin,* Clubic, 16 fév. 2021

DE POORTERE C., *Gouvernance algorithmique : 3 questions à Antoinette Rouvroy et Hugues Bersini*, Pointculture, 2 déc. 2019

DE VAUPLANE H., *La Blockchain et la loi,* Alternatives économiques, 14 fév. 2016

DELAHAYE J.-P., *L'attaque Goldfinger d'une blockchain*, SCILOGS.fr, 13 janv. 2015

F. SCHULTZ M., L'innovation : une véritable poule aux œufs d'or, OMPI Magazine, juin 2017

FAURE L. *Google va mettre en place un nouveau portail permettant aux employés de signaler les problèmes sur leur lieu de travail,* ITsocial.fr, 26/04/2019

Federal Information Processing Standards (FIPS) Publication 180-1, Secure Hash

FRISON-ROCHE M-.A., *Compliance : Avant, maintenant, après ?, MAFR, 12 déc. 2017*

GARAPON A., La *blockchain* va-t-elle remplacer tous les tiers de confiance ?, Matières à penser, France Culture, 05/08/2018

GRIFFIN A., *Ethereum to change technology underpinning its cryptocurrency to dramatically cut its energy use,* Independent.co.uk, 21 mai 2021

HOFMANN F., Malongo lance un café chez Carrefour avec la technologie blockchain, Linéaires, 11 juin 2021

In world first, Danemark to name a digital ambassador, The Local, 27 janv. 2017.

IPTRUST, *Blockchain et smarts contracts*, quid de la suppression du tiers de confiance ?, IPTRUST, 4 juil. 2017

JOST C., *Monétisation des données : un nouveau modèle économique en préparation,* Archimag, 02/10/2019

LARS L., *Qu'est-ce qu'un bloc dans la technologie blockchain,* Cryptoast, 27 janv. 2019

LAW J., *You can't beat the numbers, signs of the times, and full marx for bitcoin*, Coindesk, 28 fév. 2014

LELOUP D., *Dix ans après la loi Hadopi, que reste-t-il du téléchargement illégal*, Le Monde, 12 juin 2019

LEVY-GARBOUA V., *La compliance : au-delà des sentiers bancaires,* SciencesPo, 5 fév. 2016

MARRAUD DES GROTTES G., *Preuve blockchain : et si la soft law était une première étape ?,* Wolters Kluwer, 9 déc. 2019

OCEAN PROTOCOL, SECRET NETWORK, *Ocean and Secret: Collaborating on Access Control and Private Compute for datatokens,* OCEAN PROTOCOL TEAM, 19 nov. 2020

PANETTA K., *5 Trends Emerge in the Gartner Hype Cycle for Emerging Technologies,* Gartner, 05 nov. 2019

PERREAU C., *R3, le consortium blockchain qui divise les banques,* Journal du Net, 18 juil. 2017

POLROT S.

- *Les oracles, lien entre la blockchain et le monde,* Ethereum-France, 13 sept. 2016
- *Smart contrat ou le contrat auto-exécutant,* Ethereum France, 20 mars 2016

RANDALL P., *Le Salvador devient le premier pays à adopter le bitcoin comme monnaie légale,* Les numériques, 7 juin 2021

RASLE B., *PSSI : Contraire ou opportunité ?,* Linkedin, 15 mai 2021

RENAUDIN H., *Des investisseurs institutionnels dans le bitcoin,* Finance Mag, 21 oct. 2019

ROCHE L. *Elon Musk dans le viseur des autorités US,* Journal du Coin, 26 fév. 2021

TARNOPOLSKAYA D., *Blockchain : révolution annoncée de la pratique juridique ?,* Village de la justice, 8 sept. 2017

TETEREL N., *Bruno Le Maire, financement du terrorisme et bitcoin,* Cointribune, 21 oct. 2020

WARDZALA C., Deskoin signe un accord avec la Caisse d'Epargne Grand Est, Cryptoast, 14 sept. 2021

Communications et colloques

BEN HENDA M., L'enseignement du code informatique à l'école : Prémices d'un humanisme numérique congénital. Chaire Unesco-ITEN. Actes de la 5e rencontre annuelle d'ORBICOM, Les éditions de l'immatériel, 2017

CNIL, Les enjeux de 2016 : quelle position de la CNIL en matière de chiffrement ?, 8 avril 2016

CNIL, Premiers éléments d'analyse de la CNIL, Septembre 2018

Communication conjointe au Parlement Européen, au Conseil, au Comité Économique et social européen et au Comité des régions - Stratégie de cybersécurité de l'Union européenne : un cyber espace ouvert, sûr, et sécurisé, fév. 2013, JOIN (2013) 1 final, p. 2

Communication conjointe au Parlement Européen, au Conseil, au Comité Économique et social européen et au Comité des régions - Stratégie de cybersécurité de l'Union européenne : un cyber espace ouvert, sûr, et sécurisé, fév. 2013, JOIN (2013) 1 final

Conseil de l'UE, Cybersécurité : le Conseil adopte des conclusions sur la stratégie de cybersécurité de l'UE, Communiqué de presse, 22 mars 2021

DENIS J.D., GOËTA S., "Les facettes de l'Open Data : émergence, fondements et travail en coulisses », MENGER P-M., PAYE S., « Big data et traçabilité numérique. Les sciences sociales face à la quantification massive des individus », Conférences du Collège de France, Collège de France, 2017

JUSPI, 2020, ou encore Du *punisher* au *Lawyer* : les super héros au prisme du droit, soirée d'études, Université de Strasbourg - Association Mediadroit, 25/05/2016

Les enjeux et les défis des infrastructures de données utilisant la *blockchain* selon l'Open data institute, LINC (Laboratoire d'Innovation Numérique de la CNIL), 02 août 2016

LESSIG L., The Architecture of Privacy, Conference Taiwan Net, 1998

MEKKI M. - Colloque *Blockchain* et métiers du droit : “La fin des tiers de confiance ?” - 21 mars 2019

MENGER P-M., PAYE S., Big data et traçabilité numérique. Les sciences sociales face à la quantification massive des individus, Conférences du Collège de France, Collège de France, 2017

National Institute of Standards and Technology, Standard (SHS), U.S. DoC/NIST, FIPS 180-1, 17 avr. 1995

Présentation de la *blockchain* notariale (BCN) - Communiqué de presse - Notaires du Grand Paris - 7 juillet 2020,

SMATT PINELLIET S., DAMELETET L., SOMONONT M., PAILLAT R., Conférence annuelle de l'Incubateur du barreau de Paris, La Semaine Juridique Edition Générale n° 49, 5 décembre 2016, 1333

Table de jurisprudences

CJCE, 23 avr. 1991, aff. C-41/90, Höfner et Elser, ECLI :EU :C :1991 :161

CJCE 29 avr. 2004, IMS Health, aff. C-418/01, D. 2004. 2366, note SARDIN

CJCE, 9 nov. 2004, arrêt Opap, n°C-444/02

CJCE, 9 nov. 2004, C-203/02

CJCE, 9 nov. 2004, C-338/092

CJCE, 9 nov. 2004, C-46/02

CJCE, 9 oct. 2008, C-304/07

CJUE 18 déc. 2019, C-666/18, *IT Development c. Free Mobile ;*

CJUE 5 juin 2018, aff. C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c/ Wirtschaftsakademie Schleswig-Holstein GmbH, pt 29, D. 2018

CJUE, 1 mars 2012, arrêt Football Dataco c/ Yahoo, C-604/10

CJUE, 13 mai 2014, aff. C-131-12, arrêt Google Spain

CJUE, 15 janv. 2015, n°C-30/14, arrêt Ryanair,

CJUE, 1er mars 2021, aff. C-604/10

CJUE, 3 juill. 2021, aff/ C-128/11, arrêt dit UsedSoft/Oracle ;

CJUE, 9 mars 2017, n°C-398/15, dit arrêt Manni

CJUE, gr. ch., 5 juin 2018, aff. C-210/16

Cass. Plén., 7 mars 1986, D. 1986. 405, n°14713

Cass. Plén., 30 oct. 1987, n°86-11.918

Cass. 1ère Civ., 8 nov. 1989, nº 86-16.196

Cass. 1ère Civ, 5 mars 2009, n°07-19.735

Cass, 1ère Civ., 25 juin 2009, n°07-20.387

Cass. 1ère Civ., 25 juin 2009, RIDA 2009, n°221, p509

Cass., 1ère Civ., 30 sept. 2010, n°09-68.555

Cass. 1ère Civ., 22 sept. 2011, nº 10-23073

Cass. 1ère Civ, 17 oct. 2012, n°11-21.641

Cass. 1ère Civ., 14 nov. 2013, RLDI 2013, 999, n°3281

Cass, 1ère Civ., 13 mai 2014, arrêt Xooloo/Optenet

Cass. 1re Civ., 13 mai 2014, nº 12-27.691

Cass. Com. 4 déc. 2001, n°99-16.642, arrêt France Telecom

Cass. Com., 29 mars 2011, n°10-12.046

Cass. Com, 8 nov. 2017, n°16-17.296

Cass. Com. 29 juin 2010, nº 09-11.841

Cass. Crim., 13 oct. 2020, n°20-80.150, n°JurisData 2020-015967

Cass. Soc., 8 déc. 2009, n°08-17191, Bull. 2009 V n°276

Cass. Soc. 13 juin 2018, FS-P+B, n° 16-25.301

CA Aix en Provence, 28 mars 2012, n°10/21745

CA Caen, Ch. Corr., 18 mars 2015, *Skype Ltd.*, RLDI 2015/116, nº 3771

CA Paris, 15 juin 1981, PIBD 1981, nº 285, III, p. 175 et PIBD 1983, nº 318, III, p. 45

CA Paris, 4 juin 1984, JCP 3, 1985, p88, note M. Vivant

CA Paris, 1er juin 1994, arrêt GPL Système

CA Paris, 23 janv. 1995, LPA, 19 avril 1996

CA Paris, 4e ch., 29 oct. 1997, Biolase Technology Inc., PIBD 1998, n°646, III, p30

CA Paris, 12 sept. 2001, jurisdata n°2001-155210

CA Paris, 27 juin 2002, RLDI 2012/85, n°2850

CA Paris, 18 juin 2003, CCE 2003

CA Paris, 20 fév. 2004, jurisdata n°2004-235866

CA Paris, 13e ch., 20 sept. 2005, nº 04/0237

CA Paris, 28 fév. 2007, voir com. RIDA 2007, n°212, p.150

CA Paris, 4e ch., Sec. A, 28 fév. 2007, n°06/01801

CA Paris, 4e ch. sect. B, 5 juin 2009, Kone (venant aux droits de la SAS Ascenseurs Cierma) c. J.-P. Azpitarte, PIBD 2009, n°903, III, p. 1332

CA Paris, 11 mai 2011, RLDI 2011/72, n°2382

CA Paris, 27 juin 2012, RLDI 2012/85, n°2850

CA Paris, pôle 5, ch. 2, 20 déc. 2013, n°12/20260, sté Protagoras

CA Paris, pôle 5, ch. 1, 27 oct. 2015, n°14/14239

CA Paris, 10 mai 2016, n° 14/08976.

CA Paris, pôle 5, 2e ch., 16 déc. 2016, JurisData nº 2016-027594

CA Paris, 2 fév. 2021, n° 17/17688

CA Paris, 24 mars 2021, n°19/15565

CA Paris, 5 mai 2021, n°19/15680

CA Versailles, 11 avr. 2002 : LPA 2003, n° 105, p. 11, obs. DAVERAT X.

CA Versailles, 4 déc. 2019, n° 17/01989 ou encore CA Paris, 21 févr. 2018, n° 15/01893

T. com. Nanterre, 7e ch., 16 mai 2000, Rev. Lamy dr. aff. 2000, no 29, no 1843, obs. Costes L.
T. com. Nanterre, 9 février 2007, RLDI 2008/36

T. com. Paris, 15e ch., 19 mars 2004, Rev. Lamy dr. aff. 2004, no 73, no 4576

TGI Paris, 4 oct. 1995, JCP 1996, II, 22673
TGI Paris, 5 sep. 2001, arrêt Keljob
TGI Paris, 20 juin 2007, arrêt PMU
TGI Paris, ch. 3, sect. 3, 6 déc. 2013, arrêt Auto Look Perfect
TGI Paris, 3e ch., 1re sect., 18 juin 2015, no 14/05735
TGI Paris, 12 fév. 2019, n° 14/07224, Jugement Google/UFC-que-choisir,

CE, ass., 27 oct. 1995, Cne de Morsang-sur-Orge
CE, sect., 18 déc. 1959, Sté Les films Lutétia
CE, 10ème - 9ème ch. réunies, n°412589, 6 juin 2016, Publié au recueil Lebon
CE 10ème - 9ème ch. réunies, 8 fév. 2017, no 389806 arrêt Notrefamille. com / Département de la Vienne
CE, 19 juin 2020, n°434684

CEDH, Grande Chambre, arrêt *Jalloh c. Allemagne*, no 54810/00, 11 juil. 2006
CEDH, Grande Chambre, *O'Halloran c. Royaume-Uni*, no 15809/02, 29 juin 2007
CEDH, 2 sept. 2010, Uzun c. Allemagne, Req. n° 35623/05
CEDH, 18 sept. 2014, Brunet c. France, Req. n° 21010/10

CNIL, délib. n°SAN-2020-012, 7 déc. 2020

OEB, 25 sept. 1987, T385/86, JO OEB 1988, p308
OEB, 3 oct. 1990, JO OEB 1990, p476
OEB, CRT, 21 févr. 1995, « Plant Genetics Systems », JO OEB 1995. 545
OEB, 17 sept. 1999, T1171/97
OEB, 25 janv. 2007, T121/06
OEB, gde ch. rec., 12 mai 2010, G3/08

Webographie

http://fntc-numerique.com
http://laminutedroit.com
http://www.gnu.org
http://www.scilogs.fr
https://acpr.banque-france.fr
https://bitcoin.org
https://bitconseil.fr
https://blockchainfrance.net
https://blog.oceanprotocol.com
https://cryptoast.fr
https://csrc.nist.gov

https://developer.apple.com
https://digiconomist.net/bitcoin-energy-consumption
https://elysee.fr
https://en.wikipedia.org
https://enetter.fr
https://ethereum.org/fr
https://euipo.europa.eu
https://finance-mag.com
https://fr.cryptonews.com
https://fr.wikipedia.org
https://github.com
https://guides.etalab.gouv.fr
https://itsocial.fr
https://journalducoin.com
https://mafr.fr/fr
https://mastermsi.fr
https://openlaw.fr
https://r3cev.com
https://sites.ina.fr
https://slock.it
https://solutions-opensource-pour-collectivites.fr
https://telegram.org
https://ujomusic.com
https://www.actualitesdudroit.fr
https://www.affiches-parisiennes.com
https://www.app.asso.fr
https://www.archimag.com
https://www.axa.com/
https://www.bcdiploma.com
https://www.bfmtv.com
https://www.caselawanalytics.com
https://www.clubdelarbitrage.com
https://www.clubic.com
https://www.cnil.fr
https://www.conseil-etat.fr
https://www.culture.gouv.fr
https://www.economie.gouv.fr
https://www.economist.com
https://www.epo.org
https://www.ethereum-france.com
https://www.facebook.com
https://www.federation-blockchain.fr
https://www.forbes.fr
https://www.gartner.com
https://www.health-data-hub.fr
https://www.ibm.com
https://www.ig.com
https://www.independent.co.uk
https://www.inpi.fr
https://www.itespresso.fr
https://www.journaldunet.com
https://www.larousse.fr
https://www.lemonde.fr
https://www.lesnumeriques.com
https://www.lineaires.com
https://www.linkedin.com
https://www.oecd.org
https://www.pointculture.be
https://www.sciencespo.fr
https://www.ssi.gouv.fr
https://www.thecointribune.com
https://www.vie-publique.fr
https://www.village-justice.com

Index

A

Acte authentique 99, 94, 364
ADAN 49, 251
Algorithme 8, 22, 55, 76, 193, 259, 373
AMF 232, 242
Anonyme 224, 262
Anonymisation 337
Application distributive 257, 282
Arbre de *Merkle* 19, 88, 337
Arrêt Cryo 31, 32, 36, 53, 255
Articulation des protections 77
Attaque des 51% 11
Autorégulation 220, 233, 248, 249, 346

B

Balance is code and law 203
Base de données 9, 15, 28, 54, 255, 256, 276, 277, 278, 279, 281, 285, 291, 301, 313, 373, 469
Big data 53, 389
Bitcoin 39, 45, 46, 48, 76, 82, 94, 204, 224, 244, 251, 261, 262, 264, 271, 467
Brevetabilité 40, 51, 54, 55, 57, 59, 61, 68, 72, 76, 79

C

CADA 353
Certification 96, 209, 224, 230, 368, 369, 371, 371, 372
Chiffrement 337, 365, 366, 373, 377
CNIL 232, 242, 243, 246, 324, 331, 332, 340, 351, 357
Code de conduite 228, 233, 235
Code is law 20, 196, 203, 363, 392, 470
Conformité 212, 219, 220, 221, 231, 237, 239, 241, 245, 341, 366, 369, 371, 378, 392
Contrefaçon 47, 102, 264, 275, 282
Convention de preuve 85
Copie de sauvegarde 271, 273
Cotitularité 283, 286, 293, 293, 293
Crypotactifs 82, 83, 208, 390
Cryptologie 366, 367, 372, 375

D

Dark web 82
Déloyal 221, 302, 334
Disponibilité 345, 356, 362
Double dépense 1, 46, 47
Droit à l'oubli 321, 340, 341
Droit à la modification 338, 339
Droit d'utilisation 270, 271
Droit de décompilation 271, 274
Droit de modification 272
Droit de reproduction 267, 350
Dualité de protection 313

E

Écrit électronique 86, 88, 89, 364
eIDAS 98, 348
ENISA 368, 369, 371, 374
Éthique 207, 220, 207
Étude d'impact 378
Expansion-réduction 466
Extraction 299, 306, 308, 339

F

Finalité 239, 327, 329, 330, 333
Fork 272, 304

G

G29 329
GAFAMI 209, 213, 241, 251, 261
Gouvernance algorithmique 227

H

Hash 99, 100, 102, 337, 361
Hybride 15, 18, 368

I

Innovation 23, 51, 53, 249, 252, 346, 348, 350, 390, 394
Interopérabilité 274, 352
Investissement 292, 294, 295
Investissement substantiel 291
Investissement sustantiel 293

L

LCEN 367, 375, 376
Lex cryptographia 282, 382
Lex electronica 214, 382
Licence libre 257, 261, 269, 272, 275, 286
LIL 292, 326, 333
Loot box 384

M

Mineurs 11, 18, 51, 94, 265, 268, 293, 331, 332, 356
Minibons 23
Monétisation 354

N

Nœud 9, 11, 15, 44, 105, 270, 293, 303
Non-localisation 347, 353
Nuage d'interactions 468

O

Œuvre anonyme 264
Œuvre orpheline 264
Open data 308, 351, 353
Oracle 188
Originalité 66, 259, 260, 279, 280, 281

P

Parasitisme 302
Paternité 263, 263, 264
Patrimonialisation 324
Principe de libre flux 345, 349, 356, 358, 401
Principe de transparence 49, 334
Producteur base de données 299
Producteur de base de données ... 53, 290, 293, 294, 296, 300, 399
Pseudonyme 264, 360

R

Responsable de traitement ..321, 327, 329, 330, 332, 333
Réversibilité 356, 357
Rival 46, 47, 50, 95, 323, 354

S

Satoshi nakamoto 39, 46, 264
Scrum 392
Secret des affaires 54, 346, 348
Signature 43, 88, 89, 93, 96
Soft law 241, 245, 247
Sous-traitant 327, 331, 393

T

Tiers de confiance 39, 43, 44, 47, 80, 206, 467
Titularité 99, 258, 261, 298, 470
Transdisciplinarité 380, 386

Table des matières

REMERCIEMENTS **4**

SOMMAIRE **5**

LISTE DES PRINCIPALES ABREVIATIONS UTILISEES **7**

INTRODUCTION **9**

A. Définitions techniques 12
1. Concept général : présentations 12
2. Typologies de blockchains 18
3. Fonctionnement d'une blockchain 21
B. Définitions juridiques 22

PREMIERE PARTIE : LE CONSTAT D'UNE APPROCHE DESORDONNEE **28**

TITRE 1 : UN ECLATEMENT DU CADRE JURIDIQUE APPLICABLE **29**

CHAPITRE 1 : APPROCHES JURIDIQUES ET ECONOMIQUES ANARCHIQUES 31
Section 1 : Émergences de nouvelles économies de la confiance *32*
§1 : L'idéologie de décentralisation de la *blockchain Bitcoin* 35
§2 : L'effervescence des nouvelles relations de confiance dans l'univers numérique 37
Section 2 : Une validité contestable du monopole économique du brevet d'une blockchain *42*
§1 : Les exclusions préalables d'une brevetabilité d'une *blockchain* 45
A/ Les exclusions liées aux traitements thérapeutiques, méthodes de diagnostic 46
B/ Les exclusions liées aux bonnes mœurs et à l'ordre public 47
C/ Les exclusions liées corps humain, aux obtentions végétales et aux races animales 48
§2 : Une application inadéquate de la construction du brevet à la *blockchain* 49
A/ Construction nationale. 49
B/ Construction européenne 51
§3 : Le caractère technique discutable de la *blockchain* 52
§4 : Les incertitudes parasites restantes 54
A/ La *blockchain* comme élément essentiel d'un ensemble brevetable 54
B/ La question de l'algorithme 55
Conclusion du Chapitre 1 57
CHAPITRE 2 : TRANSFORMATIONS TECHNIQUES SUBIES DES RAPPORTS CIVILS 58
Section 1 : Chamboulement des régimes de preuve face à la blockchain *59*
§1 : L'admission crédible de la preuve par *blockchain* 64
§2 : Une force probante mesurée de la preuve par *blockchain* 69
A/ Le degré d'autorité relatif de la preuve par *blockchain* 69
B/ Limites de la force probante de la *blockchain* 74
Section 2 : Une modernisation partielle des rapports contractuels *77*
§1 : Une adaptation des rapports contractuels grâce aux *smart contracts* 78
A/ Présentations techniques 79
B/ Appréciations juridiques 81
§2 : Un entérinement relatif des *smart contracts* dans nos rapports contractuels contemporains 84
Conclusion du Chapitre 2 89

Conclusion du Titre 1 ... *90*

TITRE 2 : UNE EMERGENCE PERTURBEE D'UN NOUVEAU MODELE DE GOUVERNANCE ... 92

CHAPITRE 1 : DES LACUNES ETATIQUES SUR LA GOUVERNEMENTABILITE DES DONNEES ... 94

Section 1 : De l'abandon de prérogatives étatiques a priori ... *94*

§1 : Une dévolution de prérogatives étatiques dans le monde numérique ... 95

§2 : L'inertie législative apparemment contrôlée comme axe d'évolution ... 98

Section 2 : Vers un contrôle de la gouvernance a posteriori ... *100*

§1 : Un nouveau concept de gouvernance au sein de l'univers numérique ... 101

§2 : Le caractère utilitaire de la *blockchain* au service de la gouvernance ... 103

Conclusion du Chapitre 1 ... 107

CHAPITRE 2 : AU PROFIT DES STIMULATIONS DE LA GOUVERNANCE PRIVEE DES DONNEES ... 108

Section 1 : Un encouragement des initiatives privées de gouvernance ... *110*

§1 : La validité logique d'un consensualisme privé ... 110

§2 : La matérialisation des initiatives induite par le principe de conformité ... 114

Section 2 : Le soutien des régimes de conformité des données ... *116*

§1 : L'immersion critiquable du pouvoir privé dans la sphère publique ... 117

§2 : Le contrepoids insuffisant par le droit souple ... 119

Conclusion du Chapitre 2 ... 121

Conclusion du Titre 2 ... *123*

CONCLUSION DE LA PARTIE 1 ... 125

SECONDE PARTIE : POUR UNE APPLICATION ORDONNEE ... 128

TITRE 1 : D'UNE APPLICATION SEMANTIQUE DES REGIMES DE PROPRIETE LITTERAIRE ET ARTISTIQUES ... 129

CHAPITRE 1 : L'ADEQUATION DE LA PROTECTION DU LOGICIEL A LA *BLOCKCHAIN* ... 130

Section 1 : La banale titularité des blockchains ... *130*

§1 : L'originalité ordinaire d'une *blockchain* ... 131

§2 : L'alternance de l'auteur du logiciel *blockchain* ... 132

Section 2 : L'exploitation délicate de logiciels blockchain ... *136*

§1 : La gestion patrimoniale émoussée d'une *blockchain* ... 137

§2 : Les aménagements d'exploitation nécessaires à la *blockchain* ... 140

Conclusion du Chapitre 1 ... 144

CHAPITRE 2 : LA CONCORDANTE PROTECTION DE LA *BLOCKCHAIN* PAR LE DROIT DES BASES DE DONNEES ... 145

Section 1 : Application légitime du régime de propriété littéraire et artistique ... *146*

§1 : Les attributs classiques de la base de données *blockchain* ... 146

§2 : L'exploitation routinière des droits d'auteur d'une base de données *blockchain* ... 150

A/ Contenu de la protection ... 150

B/ Exceptions et particularités ... 152

Section 2 : Reconquêtes du régime sui generis au bénéfice de la blockchain ... *153*

§1 : Le producteur particulier d'une base de données *blockchain* ... 153

§2 : L'exploitation étonnante d'une *blockchain* ... 160

§3 : Limites fonctionnelles de la protection d'une *blockchain* ... 165

Conclusion du Chapitre 2 ... 168

Conclusion du Titre 1 ..... *170*

TITRE 2 : VERS UNE APPRECIATION FONCTIONNELLE DU DROIT DE LA DONNEE..... 171

CHAPITRE 1 : DUALISME D'UNE APPROCHE PROTECTIONNISTE DE LA DONNEE 173

Section 1 : Compatibilité de la protection des données personnelles avec la blockchain..... *174*

§1 : La nécessaire minutie dans la qualification des acteurs d'une *blockchain* 177

§2 : La comptabilité technique de la *blockchain* avec le respect des règles de protection des données personnelles 184

Section 2 : Valorisation des données non personnelles grâce à la blockchain *193*

§1 : L'habilité de la *blockchain* pour la protection des données non personnelles 194

§2 : La libéralisation contrôlée des données grâce à la *blockchain* 204

Conclusion du Chapitre 1 212

CHAPITRE 2 : COMPLEMENTARITE NATURELLE ENTRE DROIT ET TECHNIQUE..... 213

Section 1 : L'originelle sécurisation des échanges électroniques *213*

§1 : Une tendance induite vers la conformité de la sécurité des systèmes d'information..... 215

§2 : Les régimes de responsabilité informatique face à la *blockchain*..... 221

Section 2 : Atténuation des oppositions entre droit et technique..... *227*

§1 : Construction continue d'un langage commun 227

§2 : Avènement symbiotique de la transdisciplinarité juridique..... 234

Conclusion du Chapitre 2 243

Conclusion du Titre 2 ..... *244*

CONCLUSION DE LA PARTIE 2 245

CONCLUSION GENERALE 247

BIBLIOGRAPHIE..... 250

INDEX 273

TABLE DES MATIERES 275

Université de Strasbourg

Thibaut LABBÉ

Le droit face aux technologies disruptives : le cas de la *blockchain*

Résumé

La place de l'informatique dans nos sociétés actuelles est indiscutable, et ne fait que se renforcer au quotidien. Sans cesse, des technologies de l'information et de la communication poussent nos conceptions juridiques et sociales dans de nouveaux retranchements. Faire face à ces technologies signifie alors de pouvoir appréhender ces changements, et les accompagner. Pouvoir construire un raisonnement reproductible à l'essor de toute nouvelle technologie devient alors indispensable pour pouvoir anticiper ces changements induits et déterminer l'opportunité ou non de réguler.

Depuis plus de 10 ans, la *blockchain*, protocole informatique, peut bouleverser nos systèmes actuels, qu'ils soient financiers ou juridiques. Pourtant, déconnecter l'outil de l'application est essentiel pour sa bonne appréhension et ne pas limiter l'innovation.

Technologie pouvant faire le lien entre monde technique et juridique, elle invite à une collaboration entre deux mondes qui restent et seront toujours liés.

Mots-clés :

Blockchain / Propriété intellectuelle / Gouvernance des données

Abstract

The place of IT in our current societies is indisputable, and is getting stronger every day. Information and communication technologies are constantly pushing our legal and social conceptions to new limits. Facing these technologies then means being able to understand these changes, and support them. Being able to build a reproducible reasoning for the rise of any new technology then becomes essential in order to be able to anticipate these induced changes and determine whether or not to regulate.

For more than 10 years, the *blockchain*, a computer protocol, can disrupt our current systems, whether financial or legal. However, disconnecting the tool from the application is essential for its proper understanding and not to limit innovation.

A technology that can make the link between the technical and legal worlds, it invites collaboration between two worlds which remain and will always be linked.

Keyword :

Blockchain / IP-IT / data governance