AUTODETERMINATION INFORMATIONNELLE ET PATRIMONIALISATION DES DONNEES

Be secure,

Be informed

De l'extension du droit de propriété aux données à caractère personnel

Auteur : Aurélie BAYLE, WG-5 EFCSE
Faculté de Droit et Science politique - Université de Montpellier

« Si les données sont, selon la formule convenue, le pétrole du 21ème siècle, il est temps de poser la question : à qui appartient le pétrole ?[1] »

[1] Mes data sont à moi – Pour une patrimonialité des données personnelles, Génération libre, generationlibre.eu janvier 2018.

6 juin 2013

Des milliers de documents confidentiels issus du dispositif de surveillance massive de la NSA fuitent. Chefs d'états, fonctionnaires, militaires, citoyens lambdas, des millions d'individus ont été surveillés et écoutés en toute impunité pendant des années, sous le couvert d'une finalité d'espionnage déguisée en but anti-terroriste. Ces révélations déclenchaient un véritable ouragan médiatique, politique, diplomatique, et suscitaient de nombreuses questions sur les prérogatives et moyens octroyés aux Etats ou leurs institutions quant au contrôle et à l'utilisation des données des citoyens du monde entier.

L'heure de la prise de conscience mondiale

A cette époque, le temps d'utilisation moyen des réseaux sociaux était de 45 minutes par jour, bien moindre donc que les statistiques actuelles qui avoisinent désormais 3 heures. Malgré cela, un grand nombre d'individus ont véritablement intégré l'ampleur de l'utilisation faite de leurs données - ou des dérives en découlant - et, pour beaucoup, 2013 marquait le début d'une prise de conscience internationale sur l'importance de protéger les individus et leurs données à caractère personnel.

C'est précisément dans cette logique que s'est inscrite la volonté européenne lorsque les premiers balbutiements du Règlement Général sur la Protection des Données (ci-après « RGPD ») ont commencé.

Désireux de mettre à jour la législation antérieure (Directive 95/46/CE sur la protection des données personnelles) et prendre en compte ce type d'utilisation des données ainsi que les progrès technologiques, ce dernier entrait en application au 25 mai 2018.

« La mécanique des fuites »

Près de 10 ans séparent les premiers scandales concernant la protection des données de notre quotidien, pourtant, force est de constater que les incidents concernant des fuites massives de données ne cessent de faire couler l'encre et agiter la presse internationale : Wikileaks, Panama papers, Cambridge Analytica, et tous les nouveaux ransomwares rendus publics chaque semaine.

A l'heure où de multiples scandales ont mis en lumière l'incapacité chronique des technologies et réseaux sociaux quant à la protection des individus et de leurs droits, leurs

données à caractère personnel continuent de faire l'objet de collectes et traitements massifs, un peu plus intensément à chaque instant. Objets de droit bien particuliers pour lesquels l'attention de la scène internationale croît de manière significative, ces données constituent un véritable combustible pour l'économie numérique, et en seront peut-être son alpha et son oméga.

La data economy : équilibrée ?

Robotisation, Internet des objets (IoT), Big Data, blockchain, intelligence artificielle (machine et deep learning), cloud, outils de reconnaissance faciale étatisés, chatbots, les deeptech et leurs évolutions permanentes intensifient chaque jour le volume de données échangées et traitées dans le monde. Dans le même sens, la finalité mercantile des données n'est plus à prouver : qu'il s'agisse en échange d'accès aux services et plateformes, de nouvelles ou meilleures fonctionnalités et parcours utilisateurs fluidifiés, de « sécurité » ou d'innovations, les données sont devenues une source de gains inestimable, créant des business modèles inédits. Pour autant, l'interrogation sur l'équilibre entre ces rapports connaît elle aussi une croissance exponentielle, dans le même temps que la prise de conscience des utilisateurs et consommateurs.

Peut-on considérer que ces contreparties suffisent ? L'utilisateur, source des données, peut-il exiger davantage sans mettre en péril la data economy telle qu'elle s'établit à ce jour ? Un paradoxe est né, et mérite analyse : les exigences toujours plus pointues des utilisateurs peuvent-elles aller de pair avec la volonté de reprendre le contrôle sur leurs données ?

Partant de ces interrogations, deux conceptions s'opposent, notamment marquées par les différences géographiques : d'un côté, l'espace européen, pragmatique et protecteur, figé sur l'extra-patrimonialité des données, et opposé pour l'heure à toute rétribution purement financière ; et l'espace américain, fief incontesté des géants du Web et dont les régulations permettent à ce jour de mettre en œuvre de nombreuses initiatives liées à la vente de données à caractère personnel, de quelque nature qu'elles soient.

Définitions

Sans pour autant les qualifier, le RGPD, entré en application le 25 mai 2018, a le mérite de figer une définition harmonisée de ce que sont les données à caractère personnel : « toute

information se rapportant à une personne physique identifiée ou identifiable (...)[2] ». Par extension, toute information peut finalement devenir une donnée à caractère personnel dès lors que, par recoupement ou regroupement, elle peut permettre de remonter à l'identité de la personne visée, personne physique au sens juridique du terme. Cette définition, guère rénovée lorsque l'on prête attention aux définitions issues des anciennes versions de la Loi Informatique et Libertés de 1978, ou aux diverses documentations de la Commission Nationale de l'Informatique et des Libertés (ci-après « CNIL »), peut parfois sembler éloignée de la pratique et pourrait appeler à la création de sous-catégories de données.

Notamment, il serait envisageable de distinguer les données dites « sources », fournies par les personnes concernées dans leurs activités quotidiennes quelle qu'elles soient, apanage de leur personnalité propre, comme peuvent l'être les données d'identité, les coordonnées, les informations patrimoniales et bancaires, les prolongements de la personnalité avec les opinions de tous niveaux, et plus généralement l'ensemble des données sensibles telles que décrites à l'article 9 du RGPD, qu'il nomme « catégorie particulière » (santé, convictions, appartenance syndicale, orientation sexuelle, etc.) ; des données « générées », dont le terme est emprunté au rapport[3] de Génération Libre, regroupant l'ensemble des données de navigation, historiques d'achats et de comportements, ou encore les éléments d'ordre financier (aspects de suivi et statistiques).

La donnée personnelle, ce drôle d'objet

Indissociable de toute question de propriété et débattue depuis de nombreuses années, la qualification juridique des données personnelles reste à ce jour une question en perpétuelle remise en cause, ce d'autant plus au regard des volumes croissants traités dans notre société et de l'éducation des utilisateurs aux prérequis de la protection des données personnelles.

Abordée dans un premier temps sous le terme d' « information[4]», la donnée en tant que telle commençait à interroger les juristes avant même le scandale SAFARI à l'origine de la loi Informatique et Libertés de 1978, dont notamment P. Catala[5] et P. Leclercq[6] au début des

2 Article 4.1 du Règlement 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)

3 Mes data sont à moi – Pour une patrimonialité des données personnelles, Génération libre, generationlibre.eu janvier 2018, p. 43

4 Sur ce point, voir l'introduction de thèse de Philippe JOUGLEX, La protection de l'information dans les nouvelles technologies, Faculté de droit et de science politique d'Aix-Marseille, soutenue le 20 septembre 2002.

5 CATALA P. « Ebauche d'une théorie juridique de l'information », Rev. de droit prospectif 1983, n°1, p. 185 ; D. 1984, chron p. 975

6 LECLERCQ P., « Essai sur le statut juridique des informations », Ministère de la Justice, 1980

années 1980. Elle était d'ailleurs mentionnée au sein d'une loi en 1986[7] comme assimilée aux « sons, images, documents, données ou messages de toute nature ». Pour autant, cette mention semblait incomplète dans la mesure où l'information peut être publique, résumer des faits, tout comme peut le faire aujourd'hui ce que recouvre le terme « donnée », au sens large et commun du terme. C'est à partir de là qu'est intervenu le qualificatif « personnel » pour différencier ce que beaucoup appellent désormais l'« open data » des données à caractère personnel, qui elles permettent d'identifier une personne physique, directement ou indirectement.

L'extra-patrimonialisation au sens européen.

« Les données personnelles relèvent à la fois de l'être et de l'avoir », disait Philippe Mouron[8]. Entre personnalité et chose, le débat se cristallise. Si à ce jour la propriété des données n'a pas de statut juridique en tant que tel, les évolutions réglementaires ont conféré aux personnes de nombreux droits sur « leurs » données (accès, rectification, portabilité, suppression, opposition, etc.). Pour autant, cette logique revêt davantage les caractéristiques de droits attachés à l'individu (comme le droit à l'image ou au respect de la vie privée), que des biens véritablement possédés par l'individu. En effet, les données demeurent indisponibles et n'entrent pas dans le patrimoine, étant incessibles, imprescriptibles, et hors du commerce par principe. C'est précisément cette qualification hors-commerciale qui élève le débat, à l'heure où les données sont monétisées davantage chaque jour.

En effet, la doctrine européenne, empreinte des préceptes issus du Traitement sur le Fonctionnement de l'Union Européenne (TFUE[9]), garantit la libre circulation des données à caractère personnel, tout en contrebalançant cet objectif avec l'octroi de garanties aux personnes concernées, dans la vue de reconquérir la maîtrise sur l'utilisation de leurs données. Une conception parfois jugée comme étant paradoxale, et permettant la faille dans laquelle s'engouffrent aujourd'hui les plateformes « privacides[10] ».

7 Loi du 30 septembre 1986, article 2, reprenant l'article 2 de la loi du 29 juillet 1982.

8 MOURON P., « Pour ou contre la patrimonialité des données personnelles », Revue Européenne des Médias et du Numérique, n° 46-47, printemps-été 2018, pp. 90-96

9 Traité sur l'Union européenne et du traité sur le fonctionnement de l'Union européenne 2012/C 326/01

10 Expression notamment issue du rapport sur l'application des principes de protection des données aux réseaux mondiaux de télécommunications par le comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatise des données à caractère personnel, publié 18 avril 2004

L'autodétermination informationnelle : rempart à l'utilisation commerciale des données ?

L'environnement technologique en perpétuelle et rapide évolution fait croître au quotidien les risques d'atteinte aux libertés individuelles et à la protection de la vie privée des personnes. Pour pallier ces risques et leur croissance exponentielle, la consécration de garde-fous réglementaires a été la solution primée au sein des pays européens. Ces remparts, dont « l'autodétermination informationnelle » fait partie, doivent être de véritables moyens de rendre plus responsables les individus, désormais réinvestis de leur pouvoir sur leurs données. Elle signifie simplement de confier à l'individu le droit de décider de l'utilisation et de la communication des données le concernant. On parle parfois d'« empowerment » ou d'« empouvoirement [11]».

Ce terme, peu connu du grand public, n'est pourtant pas nouveau, puisque ses premières apparitions datent de 1983 au sein d'une décision de la Cour Constitutionnelle allemande[12]. Ce concept avait d'ailleurs été repris dans un rapport du Conseil d'Etat en 2004[13], précisant « Le Conseil d'Etat (…) préconise de renforcer la dimension de l'individu acteur dans le droit à la protection des données, (…), en envisageant celui-ci comme un droit à l'autodétermination plutôt que comme un droit de propriété (…), tendant à garantir en principe la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel ».

A la lumière de ce rapport, le législateur fermait la porte à toute notion de vente des données, et réaffirmait ce principe au sein de la loi pour une République Numérique du 7 octobre 2016. Réaffirmer la primauté de la personne et rappeler les principes édictés à l'article 1 de la loi Informatique et Libertés avait été préféré à toute logique patrimonialiste.

La diminution de l'opacité des traitements opérés et le renforcement des obligations des responsables de traitements, de pair avec la réaffirmation des droits des personnes, créent l'équilibre recherché et auquel appelle l'autodétermination informationnelle.

Malgré les revenus tirés par certaines activités de la data economy, les données ne peuvent être traitées comme un bien ordinaire, et leurs titulaires peuvent disposer de prérogatives sur

11 C. BERTHET, C. ZOLYNSKI, N. ANCIAUX, P. PUCHERAL, « Contenus numériques, récupération des données et empouvoirement du consommateur », Dalloz IP/I7 2017. p29

12 Arrêt du 15 décembre 1983 relatif à une loi sur le recensement, avec le terme « Informationnelle Selbstbestimmung ».

13 Le numérique et les droits fondamentaux, Étude annuelle 2014 du Conseil d'État, La Documentation française, 2014

la communication ou leur usage, mais pas en disposer à titre définitif. Le droit à l'autodétermination informationnelle tel que consacré est donc lui aussi un droit extrapatrimonial, tout comme l'est celui du « droit à la protection des données ».

Le rapport susmentionné en tirait la conclusion suivante : « Là où le droit de propriété prétend faire des individus des gestionnaires d'un patrimoine, le droit à l'autodétermination rappelle qu'ils doivent demeurer en mesure de décider de leur existence. L'un se situe sur le plan de l'avoir, l'autre sur celui de l'être. ». De quoi faire écho aux propos précédemment évoqués de Philippe Mouron, et ponctuer le rapport d'une recommandation on ne peut plus claire : « Ne pas faire entrer les données personnelles dans le champ du droit de propriété patrimonial des personnes ».

Des militants européens pour la patrimonialisation des données.

Là où certains considèrent l'autodétermination informationnelle comme un rempart suffisant aux dérives en matière de protection des données, d'autres élèvent la voix en proposant une version décapée de l'objet si particulier qu'est la donnée à caractère personnel.

Partant du constat selon lequel les données font bel et bien partie des objets de droit ayant une valeur financière, certains partisans dont fait partie le think thank Génération Libre[14] estiment légitime de pouvoir en tirer profit, tout comme il est possible de le faire aujourd'hui notamment avec un droit d'exploitation d'image, du nom, d'une œuvre ou de la voix. On parlerait alors d'un bien incorporel (immatériel).

D'autres auteurs optent pour la même opinion libérale depuis de nombreuses années : Alain Bensoussan et son évocation du « passage d'un droit à la protection des données en faveur d'un « droit à la propriété des données personnelles[15] », ou encore Isabelle Landreau[16] avec un reversement proportionnel issu de l'exploitation faite des données des personnes.

Cette conception rompt avec les caractéristiques découlant de l'extrapatrimonialité d'un droit, le rendant incessible, intransmissible et insaisissable. Pour autant, l'article 17 du RGPD octroie un « droit à l'effacement de la donnée », sous entendant sa destruction. N'est-ce pas rappeler ici les notions juridiques d'usus, abusus et fructus, pour lesquelles la personne peut librement user, jouir et disposer des choses.

14 Mes data sont à moi – Pour une patrimonialité des données personnelles, Génération libre, generationlibre.eu janvier 2018.
15 A. BENSOUSSAN, Informatique et libertés, Ed. Francis Lefebvre, n° 280 2008. 39.
16 V. infra Note n°14

Seulement, ces points de touche avec le régime des biens patrimoniaux suffit-il à établir la patrimonialité des données à caractère personnel ?

En répondant par la positive, cette affirmation soulève néanmoins d'autres questions sur la nature du régime à appliquer, oscillant entre propriété intellectuelle ; droit des biens et autres pans du Droit. La propriété intellectuelle a été choisie en 2018 lors de la transposition en droit français du RGPD au sein de la Loi Informatique et Libertés, pour laquelle un amendement de reconnaissance d'un nouveau droit de propriété intellectuelle sur les données à caractère personnel avait été déposé, sans suites cependant, eu égard à la levée de boucliers opérée par la CNIL.

Une autre problématique soulevée serait celle des données elles-mêmes, et de l'étendue de la qualification qu'elles peuvent recevoir. Au regard de la multiplication des sources et des typologies de données, notamment grâce – ou à cause – de la définition extensive issue du RGPD (directement ou indirectement identifiante), il n'est pas toujours simple de déterminer qui est le « propriétaire » ou a minima « titulaire » de la donnée en elle-même[17].

La donnée qui valait un million d'euros.

Dans la plupart des études récentes, les pourcentages oscillent entre 65 et 80% pour estimer le volume de personnes préoccupées par la confidentialité et la sécurité de leurs données, et considérant qu'elles perdent, ou plutôt, ont perdu, le contrôle sur leurs données. Et s'il était possible de vendre leurs données, le cautionneraient-elles ? Si oui, combien les vendraient-elles ? L'idéal de sécurité et confidentialité poursuivi par ces individus sondés, ne fait-il pas échec à toute volonté de vente des données, non sans rappeler l'idée de vouloir le beurre et l'argent du beurre ?

La question de la valeur d'un profil, d'un individu-utilisateur isolé, avait déjà été abordée par le Financial Times[18] dès 2013, très peu de temps après l'éclatement de l'affaire Snowden. A cette époque, la valeur moyenne d'un profil d'utilisateur sur les réseaux sociaux avoisinait 1$. Plus la personne délivrait d'informations sensibles (dont notamment des informations relatives à sa santé), plus la valeur du profil augmentait, pouvant atteindre jusqu'à 4$. Le Financial Times proposait même un simulateur permettant d'évaluer la valeur d'un profil en fonction des typologies d'informations injectées. Pour autant, il s'agissait ici de la vente d'un

17 D. BOURCIER, P. DE FILIPPI, « Vers un droit collectif sur les données de santé », RDSS 2018, p444
18 https://ig.ft.com/how-much-is-your-personal-data-worth/#axzz2WfFmKwic

profil (comme un pack) effectuées par les célèbres data brokers[19] qui ne sont très largement multipliés ces dernières années, et non des informations isolées en tant que telles.

Du point de vue consommateur et vente de leurs données, la question pourrait sembler simple, mais une fois avancée, force est de constater que l'idée d'une estimation objective est loin d'être aisée. En 2015, le Ponemon Institute a pourtant lancé une étude[20] pour quantifier et tenter de poser des chiffres sur la valeur des données personnelles, en interrogeant près de 2 000 personnes de tous âges, venues du monde entier (Allemagne, Belgique, Danemark, Espagne, États-Unis, France, Grèce, Irlande, Italie, Japon, Luxembourg, Pays-Bas, Pologne, Royaume-Uni, Russie, Slovénie, Suède et Suisse). Les résultats sont pour le moins surprenants : le coût moyen d'une donnée personnelle serait de. 18€20.

N'en déplaise à ceux qui se voyaient millionnaires en branchant des capteurs jusque dans leur sommeil ou salle de bain pour valoriser leur « patrimoine informationnel », les données les plus 'exposées' telles que le nom, prénom, genre et numéro de téléphone se vendraient respectivement 2€70, 3€60 et 5€50. Les enchères montent quelque peu lorsqu'il s'agit de données commerciales, où les historiques d'achats pourraient coûter 18€90. La courbe s'élève encore en matière bancaire, pour lesquelles le coût s'élève quant à lui à près de 33€. La gamme « luxe » des données personnelles recouvre quant à elles deux typologies de données bien particulières : les données de santé, évaluées à quasiment 55€, et comble de richesse, les identifiants et mots de passe, estimés enfin à près de 70€.

Le Data Dollar Store.

Fin 2017, Kaspersky, célèbre société spécialisée dans la sécurité informatique, a mené un projet étonnant, et étonnamment révélateur des tendances actuelles concernant les comportements des utilisateurs. Le 6 et 7 septembre 2017, l'enseigne ouvrait en Angleterre l'éphémère « Data Dollar Store », un mystérieux magasin commercialisant des mugs, posters et t-shirts griffés par un célèbre street artiste de Londres, mais n'acceptant pas d'argent. Pour autant, les objets vendus n'étaient pas gratuits, et laissaient un choix cornélien aux clients du store : payer leurs achats avec des captures d'écrans de sms, des historiques de conversation WhatsApp, des photographies de leurs galeries mobiles, ou encore quelques mails qui seraient publiés sur des écrans dans le magasin. Beaucoup ont pu hésiter, mais nombreux

19 Courtiers de données personnelles dont l'activité principale se focalise sur la revente de paquets de données à des annonceurs ou marketeurs.

20 http://www.trendmicro.com/us/security-intelligence/research-and-analysis/internet-of-things-connected-life-security/index.html

furent ceux qui ont cédé en l'échange de précieux objets édités en série limitée par l'artiste. Ce projet n'avait d'autre ambition que créer un électrochoc chez les consommateurs, et leur faire prendre conscience de la valeur de leurs données : « Ce que vous devez comprendre, c'est que vos données valent le prix que vous leur accordez. Alors, donnez-leur un prix assez élevé et protégez-les correctement pour que la confidentialité et les informations personnelles existent encore à l'avenir. [21]». Malgré les initiatives de sensibilisation comme celle-ci, force est de constater que beaucoup d'utilisateurs demeurent encore de « mauvais cyber-citoyens », la majorité d'entre eux n'étant simplement pas informée de leurs prérogatives et éduquée aux comportements et bonnes pratiques à adopter.

To win or not to win (and ensure confidentialiy), that is the question.

L'étude Ponemon Institute, autant que l'initiative du Data Dollar Store, bien qu'éphémères ou basée sur un panel de 2 000 individus pour l'étude, ont pour autant le mérite de soulever un paradoxe conséquent : les personnes sont prêtes à délaisser leur ambition de sécurité et confidentialité au profit d'une rétribution financière, ou a minima, souhaitent obtenir paradoxalement, les deux à la fois. On en revient donc au beurre et à l'argent du beurre.

Pour le territoire européen, à ce jour, l'accueil est néanmoins négatif. Pour le continent américain, la réalité est autre, et les initiatives ou concepts fleurissent : Datacoup, MoviePass, Embleema, Take 5 Solutions, Acxiom ou encore Bluekai, célèbres data brokers.

Il faut préciser dans ce contexte que la mentalité américaine est bien différente de la vision européenne : l'Etat y est perçu comme une menace pour la vie privée des personnes, à l'inverse des entreprises, faisant in fine des données personnelles une marchandise comme le seraient un paquet de sucre ou un aspirateur.

Et le darknet, dans tout ça.

Darknet, Darkweb, Deepweb, Internet caché, les appellations diffèrent, mais désignent toutes la partie immergée de l'ice berg qu'est l'Internet. Ecosystème anonyme et superposé au fonctionnement de l'internet que nous connaissons tous, ce dernier est réputé pour être le berceau de nombre d'activités illicites, puisqu'il ne connaît ni régulations n censure. Cet internet caché et anonyme est notamment réputé pour son marché noir concernant les données à caractère personnel : il est effectivement possible d'usurper l'identité d'un individu

21 https://www.kaspersky.fr/blog/data-dollar-store/9622/

en quelques minutes pour la modique somme de 100€ à débourser lors de l'achat d'un pack. Ce fameux pack comprendra : nom, prénom, date de naissance, numéro de sécurité sociale, numéro de téléphone, de permis, de passeport, et quelques informations bancaires limitées. Pour s'emparer des comptes bancaires d'un individu, le prix du pack augmentera proportionnellement au solde présent sur le compte à usurper, et pourra évoluer jusqu'à 1 000€. Des sommes qui peuvent sembler dérisoires au regard des conséquences qui peuvent découler d'une utilisation malveillante.

Pour faire écho aux notions juridique d'usus, abusus et fructus susmentionnées, la vente de données rendrait possible le « fructus »[22], avec une contrepartie financière octroyée au « producteur des données », ou « propriétaire » ; qu'elle soit effectuée sur le web classique ou sur le darknet.

Les dérives d'une éventuelle rétribution.

En cas de consécration d'une patrimonialité des données, quand bien même les utilisateurs pourraient être plus concernés et impliqués dans les traitements effectués sur leurs données, force est de constater que des abus pourraient cependant en découler.

Certains des plus fervents partisans de la patrimonialisation des données à caractère personnel vont au-delà des préconisations et hypothèses formulées dans le rapport de Génération Libre, et considèrent qu'une approche patrimoniale de la donnée implique un vol des données dès lors qu'une modification ou utilisation unilatérale des données interviendrait[23]. Dans cette perspective quelque peu extrême, un professionnel modifiant sa politique de confidentialité commettrait un « vol » de données.

Dans le même sens, il serait possible de s'interroger sur les conséquences de la vente d'une donnée. Le fait de « vendre » une donnée à une entreprise ne lui octroierait-il pas davantage de prérogatives, induisant une renonciation d'exercer ses droits à la personne « propriétaire » ? La vente de la donnée entraînerait assurément la perte des droits d'une personne sur ses données.

Plus loin encore, et sur le plan socio-éthique, ne pourrait-on pas penser qu'une monétisation des données entraînement un accroissement encore plus marqué du clivage

22 MATTATIA (F.), « Être propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété ? (partie I) », RLDI, avril 2015, n°114, p. 61.

23 L. LESSIG, "Privacy as property, Social Research: An International Quarterly", 69(1), 2002

richesse/précarité, avec un monde où les personnes les plus défavorisées se dépouillent totalement de leurs données pour espérer une rétribution en retour. Dans un article du Figaro en 2014, près de la moitié des français « confierait volontiers les clés de leur vie privée (…) s'ils sont dédommagés à hauteur de 500 euros par an [24]». Un paradoxe présenté à son plus haut niveau lorsque l'on sait que les français se disent méfiants et inquiets concernant les abus mis en œuvre par les Géants sur leurs données à caractère personnel.

---------- Fin de document ----------

24 http://www.lefigaro.fr/secteur/high-tech/2014/09/26/32001-20140926ARTFIG00032-les-francais-prets-a-monnayer-leurs-donnees-personnelles.php