Qu'est-ce que le droit à la protection des données à caractère personnel ?

Julien Rossi

▶ **To cite this version:**

Julien Rossi. Qu'est-ce que le droit à la protection des données à caractère personnel ?. Geopolitics of Risk Working Papers, 2018, Février (1). hal-02100554

HAL Id: hal-02100554

https://univ-rennes2.hal.science/hal-02100554

Submitted on 16 Apr 2019

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.

Chaire
Géopolitique
du risque

Qu'est-ce que le droit à la protection des données à caractère personnel ?

Julien Rossi

Geopolitics of Risk Working Papers
1/2018 - February 2018

Qu'est-ce que le droit à la protection des données à caractère personnel ?

Julien Rossi

Qu'est-ce que le droit à la protection des données à caractère personnel ?

La question proposée ci-dessus peut paraître stupide à quiconque s'intéresse, même depuis peu et superficiellement, à la protection des données. Y répondre est pourtant bien complexe.

Si la protection des données, traduction française de la « Datenschutz » née avec Spiros Simitis dans le Land de Hesse en 1970, évoque souvent auprès du public des notions de sécurité des données[1], voire un imaginaire des agences de renseignement, elle est un droit qui, s'il a pris son autonomie par la suite, est né du besoin de renforcer la protection de la vie privée des individus (Gonzalez Fuster, 2014b).

Différents travaux de recherche ont mis en évidence un « *privacy paradox* » (Norberg, Home, et Home, 2007) (Acquisti et Gross, 2006). dans lequel les enquêtés manifestaient un comportement de divulgation de soi en contradiction apparente avec la valeur qu'ils affirmaient accorder à la vie privée. Mais qu'est-ce que la vie privée ? Ces différents travaux omettent de demander aux enquêtés ce qu'est pour eux la vie privée ou de véritablement prendre le temps d'étudier leurs réponses (selon les articles), ce qui introduit un biais important dans leur recherche. L'incohérence démontrée est donc plutôt entre les pratiques des enquêtés et la vie privée telle que définie par les chercheurs, et non entre ces pratiques et la définition donnée par les enquêtés eux-mêmes.

Protection de la vie privée, et protection des données personnelles ne sont cependant pas, du point de vue du droit de l'Union européenne et notamment de sa Charte des droits fondamentaux, la même chose. Ils sont situés respectivement à ses articles 7 et 8.

Or, comme l'a pointé Gloria González Fuster (Gonzalez Fuster, 2014a), la Cour de justice de l'Union européenne (CJUE) est incapable de proposer une doctrine claire expliquant la relation entre l'article 7 de la Charte européenne des droits fondamentaux (Charte), qui protège le droit à la vie privée, et l'article 8 de cette même Charte, qui protège le droit à la

[1] Ainsi, parmi les élèves ingénieurs d'un cours sur la protection des données donné à l'Université de technologie de Budapest interrogés en 2017, à peu près 75 % définissaient la notion de « protection des données » (*adatvédelem*) comme étant avant tout un ensemble de techniques de contrôle d'accès. La plupart font ensuite le lien entre la protection des données et la vie privée, mais une minorité considérait que la protection des données s'appliquait même aux secrets industriels et situait donc clairement la protection des données hors du champ du droit à la vie privée.

protection des données à caractère personnel. Rajoutons à cela que ce dernier droit n'existe pas en tant que tel dans la Convention européenne des droits de l'Homme (Convention EDH) mais qu'il ne fait que dériver, pour la Cour européenne des droits de l'Homme (CEDH) de son article 8 protégeant le droit à la vie privée, et le fait que la CJUE a explicitement évité de répondre à une question préjudicielle sur la relation entre ces différents articles de droit fondamental2.

Les maux de tête pourraient s'arrêter là si la littérature académique dans au moins trois disciplines directement intéressées par la question se mettaient d'accord sur des approches et définitions communes. Or, nous pouvons lire régulièrement que droit et informatique ont une approche différente (Mascetti *et al.*, 2013) voire irréconciliable[3]. Impression corroborée par des personnes interrogées dans le cadre de notre propre enquête. Quant aux sciences de l'information et de la communication, que nous n'aurons pas la place de traiter ici plus amplement, celles-ci préfèrent parler de « trace numérique » (Collomb, 2016 : Merzeau, 2013 : Jeanneret, 2011) sans reprendre suffisamment à son compte les apports théoriques du droit sur cette question.

Selon Sergio Mascetti, Anna Monreale, Annarita Ricci et Andrea Gerino (Mascetti *et al.*, 2013), dans le langage commun, et de façon étymologique, ce qui est anonyme est ce qui est « sans nom » (Mascetti, Monreale, Ricci et Gerino, 2011:88). « Ce mot dénote un concept absolu : une personne anonyme est une personne sur laquelle rien n'est su, quelqu'un qu'on ne peut reconnaître ou identifier » (Finocchiaro et Vishik, 2010, cité par : Mascetti, Monreale, Ricci et Gerino, 2011:88).

Or il arrive souvent que l'anonymisation soit perçue comme une solution aux problèmes de protection des données. Ainsi, Ainsi, Vance Packard, auteur de *The Naked Society* (Packard, 1965), répondait à une question du président du sous-comité de la Chambre des Représentants sur l'invasion de la vie privée lui demandant quelles mesures adopter pour sauvegarder la vie privée des citoyens américains de la façon suivante :

« Mr. GALLAGHER. Is it your feeling that any central data bank should confine itself to statistics that are sanitized of individual identification ?

Mr. PACKARD. That is certainly correct, sir, yes. » (US House of Representatives, 1966)

De même, en entretien, une des juristes interrogées a dit :

> […] sur la recherche médicale [...] où on voit quand même le vrai intérêt pour une société... [...] Si les données étaient anonymisées et que justement y avait pas de possibilité de

---

[2] CJUE 21 décembre 2016 « Tele2 Sverige », aff. jointes C-203/15 et C-698/15, pts. 126-133.

[3] Voir par exemple le discours porté par TechCongress, une initiative financée par le Open Technology Institute incluant parmi ses bailleurs Google et Microsoft, qui définit sur son site Internet sa mission comme étant : « TechCongress brings diverse tech talent, ideas and training to Congress and to build a practical and pragmatic understanding of Washington within the tech community. We bridge the divide of knowledge and experience between DC and Silicon Valley for better outcomes for both. » (voir : https://www.techcongress.io/the-fellowship/, page consultée le 12 septembre 2017).

> remonter à la personne, on peut envisager que ce soit peut-être ... [possible]. (entretien réalisé avec une juriste en ONG à Paris le 17 octobre 2016)

Ce « mythe de l'anonymat robuste » est dénoncé par Paul Ohm (Ohm, 2010) pour les différentes recherches en informatique montrent qu'une information est soit absolument anonyme, soit utile, mais jamais (ou presque jamais) les deux à la fois. Et que, dès lors, il convient de prendre compte l'existence permanente d'un risque de ré-identification.

Mais Sergio Mascetti, Anna Monreale, Annarita Ricci et Andrea Gerino (Mascetti et al., 2013), la principale différence entre le droit et l'informatique dans la définition de ce qu'est une donnée à caratère personnel résiderait dans ce qui est considéré dans l'emploi du terme « information personnelle » qui, en informatique, ne recouvrirait pas l'ensemble des données se rapportant de façon directe ou indirecte à une personne physique identifiée ou identifiable, mais uniquement les informations d'ordre personnel dont il paraît, intuitivement, que l'utilisateur ne souhaite pas la divulgation (Mascetti et al., 2013, pp. 108-111).

Enfin : la protection des données est-elle bel et bien un droit ou simplement une technique de gestion du risque ? Selon Claudia Quelle (2017) la réponse donnée par le législateur de l'Union européenne – principale source d'inspiration du droit des données personnelles en Europe et dans le monde à en croire les travaux d'Abraham Newman (Newman, 2008) – est ambigüe. D'un côté, le Règlement général de protection des données de l'Union européenne[4] accorde des droits absolus aux personnes concernées, notamment en matière de droit d'accès. De l'autre, il impose aux responsables de traitement de calibrer les mesures de protection qu'ils adoptent en fonction de l'évaluation qu'ils font des risques que ce traitement fait subir aux personnes concernées.

Si, dans la pratique, le droit à la protection des données a toujours fonctionné selon une évaluation des risques[5] (risques pour les personnes concernées, degré de sensibilité des traitements, mais aussi risque financier et réputationnel en cas de contrôle pour le responsable de traitement), nous verrons que le risque – et son corollaire, la prescription de la confiance – ont servi de justification à l'invention du nouveau droit qu'est le droit à la protection des données à caractère personnel.

Nous remonterons pour montrer cela dans un premier temps à l'origine du droit à la vie privée, puis du droit à la protection des données à caractère personnel. Nous verrons qu'une évolution historique de la notion de vie privée, qui a marqué la jurisprudence et le droit de son empreinte, a contribué à la naissance du droit nouveau qu'est celui à la protection des données. Nous verrons enfin que si le droit à la vie privée est né, déjà, suite à la perception de risques, son évolution a renforcé la relation entre les deux notions. Cela

---

[4] Règlement 2016/679/UE 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 (RGPD).

[5] Voir à ce sujet les travaux de Raphaël Gellert (Gellert, 2016).

est notamment vrai pour la protection des données, qui si elle est un droit, n'en est pas moins un droit qui se concrétise par des pratiques de gestion des risques (Gellert, 2016).

Aux origines du droit à la vie privée

L'histoire de la vie privée est inséparable de l'évolution des éléments matériels qui lui permettent d'exister. Ainsi, des historiens comme Philippe Ariès et Georges Duby (1985) font remonter la vie privée moderne à la naissance de la cellule monastique, suivie de la chambre de lecture à la Renaissance, puis de la chambre à coucher individuelle qui se généralise dans la sphère bourgeoise autour du XIXe siècle (Guerrand, 1987 ; Prost, 1987 ; Riehl, 1889 ; Mumford, 1938). L'émergence d'un espace privé physique a accompagné celle de l'espace public bourgeois (Habermas, 1988). Comme le rappelait Stefano Rodotà, ce n'est qu'au XXe siècle que les conditions matérielles de l'accès à la vie privée se généralisent à l'ensemble de la population (Rodotà, 1974, pp. 151-155). C'est alors qu'a d'abord été reconnu le droit à l'inviolabilité du domicile, espace privé par excellence, avec par exemple le quatrième amendement de la Constitution des Etats-Unis adopté en 1791, près d'un siècle avant les premiers efforts de théorisation d'un droit général à la vie privée.

De nouvelles évolutions techniques et matérielles vinrent plus tard bouleverser l'équilibre garanti par la protection du domicile :

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone". (Warren et Brandeis, 1890)

Ces évolutions évoquées dans l'extrait sont à la fois matérielle – avec l'invention de la presse rotative puis de la photographie instantanée – et sociale – avec l'expansion des médias et de la presse écrite de masse. C'est en réaction à cela que sont théorisées formellement les craintes autour d'une nouvelle valeur sociale (et bourgeoise, à l'époque) : le droit à la vie privée. Cette dernière, selon sa définition classique, la vie privée recouvre trois dimensions : le secret, la quiétude et l'autonomie (Rochelandet, 2010).

Cette vie privée est-elle désirable ?

S'il semble exister un consensus apparent tendant à répondre à la question par l'affirmative, il n'est pas pour autant parfaitement unanime. Par exemple, pour l'Ecole de Chicago, protéger la vie privée nuit à l'économie car, pour résumer, elle va à l'encontre du principe de transparence des marchés (Posner, 1981), laquelle est l'une des conditions de la concurrence pure et parfaite théorisée par les économistes néoclassiques comme garante de l'efficience allocative du Marché (Knight, 1921).

Une autre critique de la vie privée vient de la littérature féministe. Elle est particulièrement utile pour cerner les évolutions dans la notion de vie privée.

Le point de départ de cette critique est l'analyse que la vie privée est le corollaire de la sphère publique habermassienne (Habermas, 1988). Or, l'universalisme supposé de l'espace public est entravée par des inégalités d'accès et sert selon Nancy Fraser à masquer

et à valider des logiques de domination (Fraser, 1990). Ces logiques sont encore renforcées par l'imposition d'un style de discours supposé rationnel mais limitant en pratique la palette d'expression des intervenants en restreignant la possibilité d'énoncer des opinions radicales. Des sujets (comme l'homosexualité) sont alors considérés comme indignes de l'espace public.

La lecture de l'article de Louis Brandeis et Samuel Warren (Warren et Brandeis, 1890) publièrent en 1890 définit certes un droit fondamental à la vie privée, mais précise qu'une des fonctions d'un tel droit est bel et bien de protéger la limite « sacrée » (Warren et Brandeis, 1890) entre public et privé :

> Even gossip apparently harmless, when widely and persistenly circulated, is potent for evil. It both belittles and perverts. It belittles by inverting the relative important of things, thus dwarfing the thoughts and aspirations of a people. When personal gossip attains the dignity of print, and crowds the space available for matters of real interest to the community, what wonder that the ignorant and thoughtless mistake its relative importance (Warren et Brandeis, 1890).

C'est cette séparation entre le public et le privé qui justifia la non-ingérence dans la sphère privée, qui a abouti à la reconnaissance constitutionnelle, aux Etats-Unis, du droit à la vie privée. Cette reconnaissance était d'ailleurs intervenue dans une affaire bien distincte du droit à la protection des données. En 1965, la Cour Suprême des Etats-Unis d'Amérique jugea[6] que les couples *mariés* avaient le droit à la « vie privée conjugale », ce qui implique que la puissance publique ne saurait sans outrepasser son droit leur interdire d'avoir recours à des moyens de contraception. Ce droit est absolu. Et il est un droit en soi : le but du droit à la vie privée est ici de garantir l'inviolabilité de la frontière public / privé, comme l'on garantirait l'inviolabilité du domicile ou le secret des correspondances. Il n'est pas dépendant au degré de risque (par exemple de calomnie) auquel la personne concernée fait face en cas de violation de cette barrière infranchissable.

Comme l'ont fait remarquer d'autres critiques féministes de la vie privée (Allen, 1988 ; MacKinnon, 1989 ; Fraser, 1990), l'envers de la médaille de cette conception – peut être d'exclure de la sphère publique des discours et des représentations issues de groupes sociaux dominés. Dans le contexte spécifique de la critique féministe, il s'agit notamment des discours qui dénoncent les violences ayant lieu dans la sphère domestique, qu'une certaine conception de la vie privée essentialise comme étant apolitique, privée, taboue.

Cette exclusion, comme le rappelle Catharine MacKinnon, est basée sur la théorie énonçant un principe de liberté négative selon laquelle « the government best promotes freedom when it stays out of existing social relationships » (MacKinnon, 1989). Elle va donc jusqu'à proposer de faire exploser la distinction entre public et privé pour détruire le fondement idéologique – basé sur l'argument de la vie privée – qui pouvait aller jusqu'à empêcher les

---

[6] Cour Suprême des Etats-Unis d'Amérique, 7 juin 1965 « Griswold contre Connecticut », 381 US 479.

femmes mariées de poursuivre en justice leur mari si ce dernier les violent. Il fallut attendre 1992 pour que la Cour de cassation rende possible de telles poursuites France[7].

Une telle réalité n'aboutit pas nécessairement par toute l'ensemble des critiques féministes de la vie privée à rejeter, à l'instar de Catharine MacKinnon, l'idée d'un droit à la vie privée (DeCew, 2015). Par ailleurs, l'évolution de la jurisprudence, qui désormais en France rejette la référence à la notion de vie privée pour justifier la non-intervention de la puissance publique dans des affaires de violence se déroulant dans la sphère privée, semble montrer une évolution dans la conception même de la vie privée.

Une évolution de la notion de vie privée (et de sa place) semble se refléter également dans plusieurs éléments de la vie courante.

Aujourd'hui, presque tout le monde possède son propre téléphone portable. Il nous paraît presque inconcevable d'accéder au téléphone d'autrui, même à celui de son conjoint voir de ses enfants. Avant, le modèle de téléphone standard SOCOTEL S63, très largement distribué entre 1963 et 1985, en France, par les PTT, disposait d'un combiné et d'un deuxième haut-parleur pour permettre à deux personnes d'écouter une conversation. De plus, dans les maisons avec plusieurs téléphones branchés sur une même ligne, il était aisément possible d'écouter les conversations téléphoniques d'une pièce à l'autre.

Figure 1 : Photographie du téléphone SOCOTEL 63

Une évolution similaire, qui mériterait d'être confirmée par une étude scientifique, est parfois suggérée pour les comptes de messagerie électronique. Comme rappelé par un enquêté pendant une campagne d'entretiens récente, les adresses e-mail ont pendant un temps été des adresses familiales :

> La sociologie de l'e-mail je pense que c'est très intéressant. Parce qu'on sait tous que notre réel identifiant virtuel c'est l'e-mail. […] Moi je fais partie de la génération [qui] est une

[7] Cour de cassation, Ch. Crim. du 11 juin 1992. En 1984 (C. Cass. Ch. Crim. 17 juillet 1984), la Cour de Cassation avait déjà ouvert la possibilité de porter plainte pour viol contre son conjoint ou sa conjointe uniquement à des époux en instance de divorce.

> génération où l'e-mail … on n'utilisait pas l'e-mail de nos parents, qui était l'e-mail associé à la box. C'est les gens qui, quand ils ont reçu Internet, étaient propriétaires de leur logement.[8]

La vie privée aujourd'hui

Bien entendu, la frontière entre « vie publique » et « vie privée » n'a pas entièrement disparu, la distinction proposée dans le présent article étant éminemment idéaltypique. Il existe d'ailleurs dans la loi, par exemple à l'article 8 de la loi informatique et libertés française,[9] des catégories particulières de données considérées d'emblée par la loi comme sensibles, comme celles portant sur les opinions politiques ou la vie sexuelle des personnes. Mais l'émergence du droit à la protection des données personnelles semble faire émerger une autre conception de la vie privée, plus centrée sur les choix de l'individu.

En 1983, le Tribunal constitutionnel fédéral de République fédérale d'Allemagne a rendu une décision au sujet d'une loi sur le recensement de la population (décision Volkszählungsurteil)[10], prévoyant un traitement informatisé des données recueillies. Si l'objectif de cette loi a bien été jugé conforme à la Loi fondamentale allemande, le juge constitutionnel a demandé de meilleures garanties pour protéger un droit nouveau, dérivé du droit général de la personne (allgemeinen Persönlichkeitsrecht) et du droit à la dignité (der Würde des Menschen) : le droit à l'auto-détermination informationnel (informationelle Selbstbestimmung). Ce droit consiste à permettre au citoyen, en règle général, de décider lui-même des informations personnelles qu'il souhaite partager avec l'Etat. Seule la poursuite d'un objectif constitutionnel d'intérêt général permet d'y déroger.

Pour le juge constitutionnel allemand, ce droit était rendu nécessaire par un nouvel état des choses. Dans une décision précédente datant de 1969[11], il avait déjà indiqué que les données statistiques collectées par l'Etat devaient, en règle générale, être anonymes. Or, il nota en 1983, conformément à une intuition qui confirmée par divers travaux de recherche (Ohm, 2010) que l'informatique facilite grandement la réidentification de jeux de données dont il pouvait pourtant sembler que, ne contenant pas le nom de la personne concernée, ils fussent anonymes.

Dans cette optique, une donnée n'est pas personnelle en vertu du fait qu'elle se rapporte à la vie privée, comme l'avait proposé Jean-Paul Costa pendant une réunion en 1972 du

---

[8] Entretien avec P. C. le 30 mai 2016 à Paris.

[9] Loi 78-17 du 6 janvier 1978 dite loi informatique et libertés.

[10] Décision du Tribunal constitutionnel fédéral allemand BVerfG Urteil vom 15. Dezember 1983 Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83 (Volkszählungsurteil).

[11] Entscheidung vom 16. Juli 1969 zur Verfassungsmäßigkeit einer Repräsentativstatistik (BVerfGE 27, 1 - Mikrozensus).

groupe de travail du Conseil de l'Europe[12] dont le travail a abouti, en 1981, au texte de la Convention 108. Elle l'est, depuis la loi sur la protection adoptée en Suède[13] puis dans toutes les définitions européennes qui ont suivi depuis[14], dès lors qu'elle peut être liée à une personne physique identifiée ou identifiable, directement ou indirectement.

Cela signifie d'abord, comme la Cour constitutionnelle fédérale allemande l'avait précisé dès ses arrêts de 1969[15] et 1983[16], qu'il ne suffit pas qu'une donnée ne contienne pas le nom de la personne pour qu'elle soit anonyme. L'anonymat doit s'apprécier notamment au regard des autres données disponibles, qui, par croisement, permettraient une identification de la personne. Contrairement à ce que suggère Paul Ohm lorsqu'il affirme que « the failure of anonymization disrupts privacy law » (Ohm, 2010, p. 1731) il est donc faux de considérer que les juristes, au contraire des informaticiens, considèrent l'anonymat et l'identification comme un choix binaire là où les informaticiens voient un continuum entre donnée identifiante et anonyme absolu. Des entretiens menés avec différents informaticiens confirment d'ailleurs l'existence de divergence définitionnelles au sein même de la profession :

Donnée directement identifiante Entretien du 6 juin 2016 avec Mathieu S.	Donnée directement ou indirectement identifiante Entretien du 30 mai 2016 avec Pierre C.
« J'ai un fichier Excel avec des informations. Si je supprime le nom et le prénom des colonnes et que je suis plus capable de les retrouver, mon fichier il devient anonyme »	« […] on pourra toujours te dire que tous les mecs qui habitent Marly-le-Roy et qui ont quatorze ans, ils fonctionnement de la même manière. Et qu'ils sont déjà allés sur un site de jeux vidéo, et au final, y en a qu'un seul de gars, qui a quatorze ans, qui est déjà allé sur un site de jeux vidéo […] »

Figure 2 : Extraits d'entretiens 1

[12] « Data […] as relates to the private life of the individuals whom it concerns, and particularly information concerning their race, religion, political opinions, morals, health or past judicial record ». Voir : COSTA J.-P., 1972, « Convention on transnational data banks in the private sector. Preleminary draft proposed by Mr. J.P. Costa, French expert », EXP/Prot.Priv./EDB (1972) 17, Strasbourg, Conseil de l'Europe.

[13] Datalag 1973:289

[14] Ce n'est donc par exemple pas le cas des Lignes directrices de l'OCDE de 1980 sur la protection de la vie privée.

[15] Décision du Tribunal constitutionnel fédéral allemand BVerfG Urteil vom 16. Juli 1969 1 BvL 19/63 (Mikrozensus).

[16] Décision du Tribunal constitutionnel fédéral allemand BVerfG Urteil vom 15. Dezember 1983 Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83 (Volkszählungsurteil).

Par ailleurs, contrairement à ce que suggéraient Mascetti et al. (Mascetti et al., 2013), la réponse à la question de savoir si les données personnelles recouvrent uniquement les informations privées au sens où elles relèvent a priori de l'intimité de la personne, ou bien si cette catégorie rassemble toute les informations sur une personne quelle que soit la nature de cette information, ne dépend pas de la profession de la personne interrogée :

Toute information reliée à un individu est personnelle Entretien du 17 octobre 2016 avec Mathilde R.	Seules les informations relevant de la vie privée de la personne sont des données personnelles Entretien du 13 septembre 2016 avec E. Q.
« [Il] y a des informations qui sont publiques, par exemple moi genre je peux faire une demande de ton état civil. Et si je récupère toutes les informations sur plein de gens ça reste un fichier … ça reste des données personnelles […]. Et donc c'est des trucs qui sont personnels, qui sont évidemment publics »	« Donnée à caractère personnel […] je dirais que c'est des données qui touchent à la vie privée des individus, donc […] à leur identité, leur sexe, leur orientation sexuelle, leurs pensées, enfin leur liberté de pensée, leurs opinions religieuses, politiques, mais éventuellement aussi des données qui touchent des éléments médicaux, donc de santé, et de vie familale, de mode de vie familial […] »

Figure 3 : Extraits d'entretien 2

En réalité, la réponse à cette question dépend de celle à la question de savoir si une protection générale des données à caractère personnel est souhaitable, ou si la protection des données personnelles vise uniquement à protéger la vie privée des individus. Autrement dit, et pour prendre un exemple concret tiré des débats au sein du groupe de travail sur la norme Do Not Track du W3C : est-ce que le simple fait de collecter des données, potentiellement non sensibles, sur un individu, constitue une violation de ses droits ? Ou bien est-il nécessaire pour qu'un traitement de données à caractère personnel doive respecter des règles juridiques contraignantes qu'il puisse entraîner un préjudice en rapport avec son droit à la vie privée, comme la divulgation involontaire de sa vie privée ?

Le droit à l'auto-détermination informationnelle suppose que chacun est libre, en principe[17], de définir le régime de publicité applicable à ses données personnelles. Et donc de définir les frontières de sa privée, et de renégocier la frontière public-privé socialement tracée, sacralisée dans la conception classique de la vie privée

Il n'est pas possible, en vertu du droit des données personnelles, de recueillir et de traiter des données personnelles d'individus sans respecter un certain nombre de principes. Même lorsque, *a priori*, ces données peuvent s'avérer hors du champ de la vie privée, comme un CV ou des données publiées par les personnes elles-mêmes dans des arènes publiques comme Twitter.

[17] Des exceptions peuvent être envisagées (voir par exemple : art. 6 du RGPD).

La CJUE elle-même l'a rappelé dans son arrêt ClientEarth :

> […] les notions de «données à caractère personnel», au sens de l'article 2, sous a), du règlement n° 45/2001, et de «données relatives à la vie privée» ne se confondent pas.[18]

Mais alors, si le droit à la protection des données personnelles ne sert pas toujours à protéger la vie privée, à quoi sert-il ?

Il existe, tant dans la littérature, que dans les discours d'acteurs, diverses justifications à ce droit garanti à l'article 8 de la Charte des droits fondamentaux de l'Union européenne.

Un élément ressortant régulièrement est la perception d'un risque émanant de l'informatisation de la société. Nous utiliserons ici le terme de « risque » et non d'« incertitude », car même si le danger posé par l'informatisation n'est pas quantifié ou quantifiable[19], il s'agit du vocabulaire utilisé par les acteurs eux-mêmes. Indépendamment, donc, de la capacité ou non à déterminer et à quantifier le risque engendré par l'informatique, c'est la façon dont l'incertitude est vécue par les acteurs agissant dans le champ de la protection des données qui compte pour comprendre ce qui les a motivés à inventer un droit nouveau.

La protection des données et le risque

L'histoire de la protection des données montre que son invention est très liée à la perception de l'informatique dans les années 1960 comme quelque chose de dangereux. Ainsi, dans les premiers débats organisés sur le rapport entre l'informatique et la vie privée à la Chambre des représentants des Etats-Unis en 1966 (US House of Representatives, 1966), l'ordinateur est comparé à l'arme nucléaire par le député américain Franck Horton :

> I have become convinced that the magnitude of the problem we now confront is akin to the changes wrought in our national life with the dawning of the nuclear age (U.S. House of Representatives, 1966, p. 5).[20]

Et cet ordinateur, incapable d'oublier, rendrait notre société incapable de pardon selon Cornelius E. Gallagher :

> The possible future storage and regrouping of [...] personal information also strikes at the core of our Judeo-Christian concept of "forgive and forget," because the computer neither forgives nor forgets. (U.S. House of Representatives, 1966, p.4).

Par ailleurs, le paradigme libéral de la vie privée qui sous-tend le droit de la protection des données (Bennett et Raab, 2003) s'est inspiré notamment de l'image du panoptique de Bentham retravaillé par Michel Foucault (Simon, 2002). Dans un système panoptique, chacun peut être surveillé à n'importe quel moment, et la conscience de ce phénomène

---

[18] CJUE 16 juillet 2015 « ClientEarth contre EFSA » Aff. C-615/13 P, pt. 32.

[19] Voir, sur la distinction entre risque et incertitude, les travaux de David Le Breton (Le Breton, 2017).

[20] Traduction : « J'en suis venu à être convaincu que l'ampleur du problème auquel nous sommes à présent confronté est comparable aux bouleversements entraînés dans la vie de notre Nation par l'avènement de l'âge nucléaire »

produit sur les individus des effets disciplinaires. Or, la multiplication de capteurs connectés et de sources de données qu'engendre l'informatisation de la société accroît le risque de conformisme contraint à des normes sociales sur la base desquels les comportements et les performances quantifiées, par exemple par des capteurs de santé connectée reliés à une compagnie d'assurance, sont jugés. Et, comme le rappelle David Lyon (Lyon, 2015), la collecte de données sert avant tout à discriminer, et, quelque part, tout ce qui est capté ou mis en ligne par un individu peut à un moment donné se retourner contre lui.

Par ailleurs, la concentration de ces informations peut entraîner des effets de pouvoir jugés par certains acteurs des politiques publiques de protection des données comme préoccupantes pour le fonctionnement de la démocratie libérale (Sólyom, 1988) . En bref, le risque est celui d'aboutir à une société « totalitaire », selon les mots de Jan Philipp Albrecht, rapporteur du Parlement européen du Règlement général de protection des données :

> If things remain as they are, we shall be completely disenfranchised and easily fleeced in the digitised world. We shall find ourselves living in a totalitarian controlled society, which has only been able to come into existence and to hold sway thanks to the masses of information gathered about us, and which is becoming daily more entrenched by the same means (Albrecht, 2015, p. 15 -16).

Enfin, les règles relatives aux décisions automatisées et au profilage contenues aux articles 21 et 22 du RGPD visent non pas à protéger la vie privée, mais à garantir aux individus qu'ils ne seront pas soumis à l'arbitraire de la gouvernementalité algorithmique (Rouvroy et Berns, 2013). En France, la CNIL a d'ailleurs censuré le dispositif Admissions Post-Bac en 2017 en raison du fait que « les propositions d'affectation auprès de formations non sélectives dans l'enseignement supérieur s'effectuent sur la base d'un traitement entièrement automatisé permettant de déterminer les profils des candidats et n'étant assorti d'aucune intervention humaine et manuelle ».[21]

Dans ce contexte, le droit à la protection des données, assimilé à un droit à l'auto-détermination informationnelle, sert à fournir à l'individu une maîtrise des risques qu'il encourt dans l'univers numérique. D'un droit de la vie privée informationnelle, il est devenu

[21] CNIL. Décision n° MED-2017-053 du 30 août 2017 mettant en demeure le ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation.

un droit de la circulation de l'information,[22] mais il semble également être un outil de gestion de divers risques liés à l'informatisation, comme d'ailleurs semble le suggérer l'intitulé en France de la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (et non pas simplement à la vie privée).

Cette gestion est présentée par les différents acteurs, et ce depuis la fin des années 1960, pour rétablir la « confiance » du citoyen (puis du consommateur) en l'informatique[23] [24] :

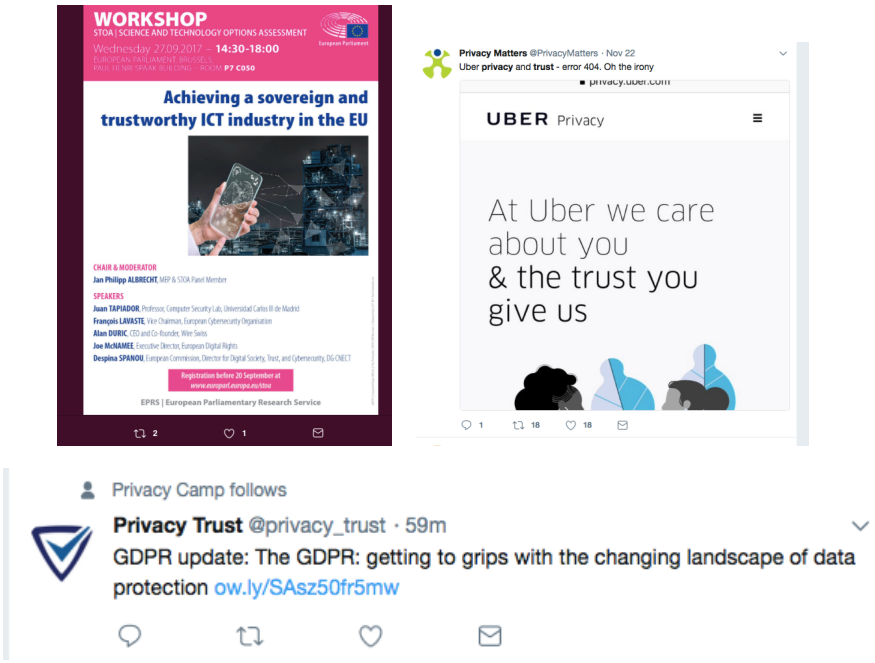

Figure 4 : Captures d'écran de tweets illustrant le lien entre la thématique de la protection des données et la thématique de la confiance

---

[22] Jan Pieter Hustinx, membre du premier groupe d'experts du Conseil de l'Europe sur la protection des données dans les années 1970 puis Contrôleur européen de la protection des données de 2004 à 2014, a évoqué dans un entretien réalisé en juin 2016 le fait que, pour lui, le droit de la protection des données est un droit à cheval entre l'article 8 CEDH protégeant la vie privée, et l'article 10 CEDH protégeant la liberté d'expression.
László Sólyom, ancien président de la République de Hongrie et ancien président de sa Cour constitutionnelle, théorisa quant à lui dans les années 1980 un droit de l'information dont une face serait le droit à la protection des données, et l'autre la liberté de l'information (Sólyom, 1988) (entretien réalisé le 21 novembre 2017). Elle se concrétisa dès 1992 en Hongrie par l'adoption d'une loi sur la protection des données instituant un Commissaire à la protection des données également en charge du libre accès aux documents administratifs, et inspire en France le rapprochement entre la CNIL et la Commission d'accès aux documents administratifs (CADA) introduit par la loi pour une République numérique du 7 octobre 2016.

[23] Entretien avec Spiros Simitis du 27 septembre 2016. Entretien avec Anna W. du 8 décembre 2016.

[24] L'argument de la confiance revient régulièrement dans les interventions des participants à une conférence organisée sur le thème de la protection des libertés fondamentales face à l'informatisation des sociétés par l'OCDE en 1974 (OCDE, 1974).

Nous n'entrerons cependant pas plus amplement dans la thématique de la confiance et de son rôle dans la légitimation des politiques publiques de protection des données, car il sera l'objet d'une autre intervention.

Conclusion

Ainsi, le droit à la protection des données à caractère personnel fondé en l'article 8 de la Charte des droits fondamentaux de l'Union européenne ne doit pas être confondu avec son article 7, protégeant la vie privée. Car si la protection des données contribue bel et bien à protéger une vie privée dont le sens a évolué dans un sens affaiblissant la frontière public-privé en offrant aux individus un droit à l'auto-détermination informationnelle, elle sert également à fournir à ce même individu des outils pour l'aider à gérer les risques de l'informatisation tels qu'ils ont à tout le moins été perçus par les concepteurs des lois de protection des données à partir des années 1960 et 1970.

Pour finir, nous ne devons pas oublier de mentionner une autre originalité de la protection des données. Si nous avons brièvement évoqué qu'en réalité, tant la littérature en droit qu'en informatique ont pris conscience depuis plusieurs décennies du fait que l'anonymat d'une donnée doit être estimée en fonction des capacités, notamment de croisement avec d'autres données, d'un adversaire souhaitant briser cet anonymat, nous n'avons pas développer sur ce qu'une telle approche suppose en termes pratiques lorsqu'il s'agit de déterminer les modalités avec lesquelles les données personnelles doivent être protégées. En effet, une telle approche suppose d'apprécier les risques de ré-identification en fonction de la situation, laquelle doit prendre en compte les risques encourus par la personne concernée en cas de ré-identification. Cette démarche, qui est celle des analyses d'impact, a été consacrée à l'article 35 du RGPD, et fera l'objet de présentations distinctes.

Bibliography

Acquisti, Alessandro, et Ralph Gross. 2006. « Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook ». *Proc. 6th Int. Conf. Priv. Enhancing Technol.* p. 36–58.

Albrecht, Jan Philipp. 2015. *Hands off our data!* Bruxelles : Jan Philipp Albrecht,

Allen, Anita L. 1988. *Uneasy Access: Privacy for Women in a Free Society*. Rowman & Littlefield, 244 p. ISBN : 978-0-8476-7328-5.

Ariès, Philippe, et Georges Duby, éd. 1985. *Histoire de la vie privée*. Paris : Seuil,

Bennett, Colin J., et Charles D. Raab. 2003. The Governance of Privacy. Policy Instruments in Global Perspective. Aldershot : Ashgate,

Collomb, Cléo. 2016. « Pour un concept technologique de trace numérique ». Disponible sur:<http://www.academia.edu/29393685/_2016_Pour_un_concept_technologique_de_trace_num%C3%A9rique (Consulté le 17 janvier 2017).

Decew, Judith Wagner. 2015. « The feminist critique of privacy: past arguments and new social understandings ». Dans : Roessler B, Mokrosinska D (éd.). *Soc. Dimens. Priv.* [En ligne]. Cambridge : Cambridge University Press, p. 85–103. Disponible sur : < http://ebooks.cambridge.org/ref/id/CBO9781107280557A018 > (Consulté le 22 juillet 2017). ISBN : 978-1-107-28055-7.

Fraser, Nancy. 1990. « Rethinking the Public Sphere: A Contribution to the Critique of Actually Existing Democracy ». *Soc. Text*. n°25/26, p. 56–80.

Gellert, Raphael. 2016. « We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-Based and the Risk-Based Approaches to Data Protection ». *Eur. Data Prot. Law Rev. EDPL*. Vol. 2, p. 481.

Gonzalez Fuster, Gloria. 2014a. « Fighting For Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection ». *Birkbeck Law Rev.* Vol. 2, n°2, p. 263–278.

---. 2014b. *The Emergence of Personal Data Protection as a Fundamental Right of the EU* [En ligne]. Dordrecht : Springer, Disponible sur : < //www.springer.com/gp/book/9783319050225 > (Consulté le 22 novembre 2017).

Guerrand, Roger-Henri. 1987. « Espaces privés ». Dans : Ariès P, Duby G (éd.). *Hist. Vie Privée Tome 4 Révolution À Gd. Guerre*. Paris : Seuil, p. 325–411.

Finocchario, Giusella et Vishik, Claire. 2010. « Law and Technology: Anonymity and Right to Anonymity in a Connected World » in Monica Wachowicz (dir.) *Movement-Aware Applications for Sustainable Mobility: Technologies and Approaches*, IGI Global, pp. 140-156

Habermas, Jürgen. 1988. L'espace public: archéologie de la publicité comme dimension constitutive de la société bourgeoise. Paris : Payot, 324 p.(Critique de la politique Payot). ISBN : 978-2-228-88013-8.

Jeanneret, Yves. 2011. « Complexité de la notion de trace ». Dans : Galinon-Mélénec B (éd.). *Homme-Trace Perspect. Anthropol. Traces Contemp.* Paris : CNRS-éditions, p. 59–86.

Knight, Frank H. 1921. *Risk, Uncertainty and Profit* [En ligne]. Boston, MA : Hart, Schaffner & Marx; Houghton Mifflin Co., Disponible sur : < http://www.econlib.org/library/Knight/knRUP2.html#Pt.II,Ch.III >

Le Breton, David. 2017. « Introduction ». *Que Sais-Je*. Vol. 2e éd., p. 3–10.

Lyon, David. 2015. *Surveillance After Snowden*. Cambridge, Mass. : Polity Press,

MacKinnon, Catharine A. 1989. *Toward a Feminist Theory of the State*. Harvard University Press, 360 p. ISBN : 978-0-674-89645-1.

Mascetti, Sergio, Anna Monreale, Annarita Ricci, et Andrea Gerino. 2013. « Anonimity: A Comparison Between the Legal and Computer Science Perspectives ». Dans : *Eur. Data Prot. Coming Age*. Dordrecht : Springer, p. 85–115.

Merzeau, Louise. 2013. « L'intelligence des traces ». *Intellectica*. Vol. 1, n°59, p. p.115–135.

Newman, Abraham. 2008. Protectors of Privacy. Regulating Personal Data in the Global Economy. Ithaca : Cornell University Press,

Norberg, Patricia A., Daniel R. Home, et David A. Home. 2007. « The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors ». *J. Consum. Aff.* n°41, p. 100–126.

OCDE. 1974. Questions d'ordre politique soulevées par la protection des données et des libertés individuelles, principes et perspectives. Compte-rendu du séminaire 24-26 juin 1974. Paris : OCDE, (Etudes d'informatique, 10)

Ohm, Paul. 2010. « Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization ». *UCLA Law Rev.* n°57, p. 1701–1777.

Packard, Vance. 1965. *The Naked Society*. New York : Pocket Books Inc.,

Posner, Richard A. 1981. « The Economics of Privacy ». *Am. Econ. Rev.* Vol. 71, n°2, p. 405–409.

Prost, Antoine. 1987. « Frontières et espaces du privé ». Dans : Ariès P, Duby G (éd.). *Hist. Vie Privée Tome 5 Prem. Guerre Mond. À Nos Jours*. Paris : Seuil, p. 13–154.

Quelle, Claudia. 2017. *The 'Risk Revolution' in EU Data Protection Law: We Can't Have Our Cake and Eat It, Too* [En ligne]. Rochester, NY : Social Science Research Network, Disponible sur : < https://papers.ssrn.com/abstract=3000382 > (Consulté le 12 septembre 2017).

Riehl, Wilhelm Heinrich. 1889. *Die Familie* [En ligne]. Stuttgart : Cotta'sche Buchhandlung, Disponible sur : < https://www.booklooker.de/B%C3%BCcher/Riehl-W-H+Die-Familie/id/A021xGu901ZZ8 > (Consulté le 29 juillet 2017).

Rochelandet, Fabrice. 2010. Économie des données personnelles et de la vie privée. Paris : Découverte, ISBN : 978-2-7071-5765-2.

Rouvroy, Antoinette, et Thomas Berns. 2013. « Gouvernementalité algorithmique et perspectives d'émancipation: Le disparate comme condition d'individuation par la relation? » *Réseaux*. Vol. 177, n°1, p. 163.

Simon, Bart. 2002. « The Return of Panopticism: Supervision, Subjection and the New Surveillance ». *Surveill. Soc.* [En ligne]. Vol. 3, n°1,. Disponible sur : < http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3317 > (Consulté le 15 mars 2017).

Sólyom, László. 1988. « Egy új szabadságjog: az információszabadság ». *Valóság*. n°31, p. 14–34.

US House of Representatives. 1966. Hearings before a Subcommittee of the Committee on Government Operations. House of Representatives, 89th Congress, Second Session.

Warren, Samuel D., et Louis D. Brandeis. 1890. « The Right to Privacy ». *Harv. Law Rev.* Vol. 4, n°5, p. 193–220.

Contact

Julien Rossi
COSTECH
Université de technologie de Compiègne
julien.rossi@utc.fr
Twitter : @julienrossi