Article

L'autodétermination en matière de données personnelles : un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété ?

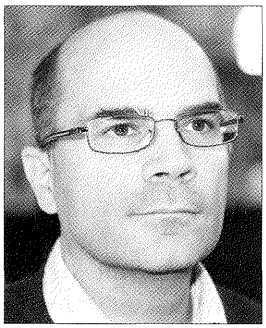
FLUECKIGER, Alexandre

Abstract

Plusieurs auteurs ont critiqué le droit fondamental à l'autodétermination en matière de données personnelles, jusqu'à remettre en cause la pertinence même de celui-ci à l'ère digitale. Certes, la multiplication, l'automatisation et la mise en réseau généralisée des capteurs de traces personnelles ont conduit aujourd'hui l'individu à souvent perdre, dans les faits, la maîtrise des données qui le concernent. Or ces dernières, caractérisant et exprimant notre personnalité, ne sauraient tomber sans autre forme de procès dans le domaine public, même pour un usage« normal». En se fondant tant sur une approche comparatiste (droit suisse, européen, états-unien et allemand) qu'historique, retraçant aussi bien les racines du droit à l'autodétermination dès le XVIII siècle que les origines de la propriété intellectuelle, l'article défend la nécessité de concevoir désormais l'autodétermination en matière de données personnelles comme un nouveau type de droit de propriété.

Reference

FLUECKIGER, Alexandre. L'autodétermination en matière de données personnelles : un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété ? *Pratique juridique actuelle*, 2013, vol. 22, no. 6, p. 837-864



L'autodétermination en matière de données personnelles : un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété ?

ALEXANDRE FLÜCKIGER

Plusieurs auteurs ont critiqué le droit fondamental à l'autodétermination en matière de données personnelles, jusqu'à remettre en cause la pertinence même de celui-ci à l'ère digitale. Certes, la multiplication, l'automatisation et la mise en réseau généralisée des capteurs de traces personnelles ont conduit aujourd'hui l'individu à souvent perdre, dans les faits, la maîtrise des données qui le concernent. Or ces dernières, caractérisant et exprimant notre personnalité, ne sauraient tomber sans autre forme de procès dans le domaine public, même pour un usage « normal ». En se fondant tant sur une approche comparatiste (droit suisse, européen, états-unien et allemand) qu'historique, retraçant aussi bien les racines du droit à l'autodétermination dès le XVIII^e siècle que les origines de la propriété intellectuelle, l'article défend la nécessité de concevoir désormais l'autodétermination en matière de données personnelles comme un nouveau type de droit de propriété.

Mehrere Autoren kritisieren das fundamentale Recht auf Selbstbestimmung bezüglich der persönlichen Daten und gehen dabei sogar so weit, dass sie ein solches Recht in der Zeit der digitalen Vernetzung überhaupt in Frage stellen. Zwar haben die Multiplizierung, die Automatisierung und die Verbreitung der erfassten Personendaten auf dem allgemeinen Netz dazu geführt, dass der Einzelne faktisch die Herrschaft über die ihn betreffenden Daten verliert. Dennoch fallen Personendaten – sie sind Ausdruck und Teil unserer Persönlichkeit – nicht ohne besonderes Verfahren in den öffentlichen Sphärenbereich («domaine public»), auch nicht bei ihrem gewöhnlichen Gebrauch. Ausgehend von der Rechtsvergleichung (Recht der Schweiz, der Europäischen Union, Deutschlands und der USA) und der bis in das 18. Jahrhundert zurückgehenden Geschichte des Rechts auf Selbstbestimmung und der Anfänge des Urheberrechts, tritt der vorliegende Aufsatz für die Notwendigkeit ein, die Selbstbestimmung über persönliche Daten als einen neuen Typus des Eigentums zu verstehen.

Plan

1. Introduction : l'érosion du droit à l'autodétermination en matière de données personnelles

Le droit à l'autodétermination en matière de données personnelles forme la clef de voûte du système juridique de protection de la sphère privée à l'ère digitale. Il garantit à chacun le droit de décider de la diffusion et de l'utilisation de ses données personnelles. Erigé au rang constitutionnel, ce droit est une construction jurisprudentielle tant en Allemagne qu'en Suisse notamment. Les développements technologiques dans le domaine des communications, qui ont justifié l'essor du droit à son origine, seraient devenus aujourd'hui si foudroyants qu'ils auraient rendu, selon certaines critiques, ce dernier aussi obsolète qu'un lecteur de cartes perforées.

Protéger la personnalité, et plus généralement la dignité de chacun, est en effet aujourd'hui une mission compliquée dans un monde aussi numérisé et interconnecté que le nôtre. L'information est devenue si fluide qu'elle nous glisse entre les doigts. A la portée de toutes et tous, elle s'échappe aussi aisément qu'elle a été facile à produire et à diffuser. Même en redoublant d'attention, il est quasiment impossible aujourd'hui d'éviter de laisser des traces

ALEXANDRE FLÜCKIGER, professeur à l'Université de Genève.
Les sites web cités ont été consultés en date du 7 mars 2013 ; à défaut de précision, les citations traduites l'ont été par l'auteur. Que

M^me^ FRANCESCA MAGISTRO, assistante auprès du Département de droit public de la Faculté de droit de l'Université de Genève, soit remerciée pour la mise au point du manuscrit.

de sa personne, instantanément communicables et infiniment consultables depuis partout[1].

Si l'observation a été évidente dès l'essor des réseaux numériques, le constat ne se limite plus à l'ordinateur de bureau ou de salon. Les capteurs de traces personnelles sont devenus bien plus mobiles et diversifiés au point de nous accompagner à tout instant dans tous les endroits de notre vie. Ils collectent non seulement notre image mais aussi nos localisations, nos lectures, nos consommations, nos préférences (appareils miniaturisés de prise de vue et de son en ultra-haute définition, téléphones multi-fonctions, web interactif [web 2.0], informatique ubiquitaire *[cloud computing],* distributeurs d'argent, lecteurs de cartes de crédit, de santé, de vote, d'étudiant, d'employé, de « fidélité » ou d'identité, désormais biométrique, GPS, puces électroniques RFID implantables tant sur des objets, des animaux et même des êtres humains). Ces senseurs, capteurs, caméras, microphones, smartphones, ordinateurs et autres tablettes produisent automatiquement une masse d'information qui peut circuler, être multipliée et compilée à toutes sortes de fins, possiblement étrangères au but initialement prévu, et sans véritable contrôle effectif par les personnes concernées. Ces données peuvent être triées pour profiler la personnalité de quiconque en établissant de véritables biographies numériques détaillées et être commercialisées à profit. Elles permettent à tout un chacun – et non seulement aux autorités – d'exercer potentiellement une surveillance sur n'importe qui dans des contextes aussi divers que les loisirs, les voyages, les rapports de travail, le milieu scolaire, les relations familiales et affectives (couples, enfants, personnes âgées) ou les relations commerciales et financières. Les motifs peuvent être aussi vertueux – tels que la sécurité, la santé, les bonnes relations d'affaire ou de voisinage, le renforcement des liens sociaux, ou, même, du sens de l'orientation – qu'hostiles, à l'exemple de la publicité intrusive, de la curiosité malsaine, du voyeurisme, de l'intimidation, de l'espionnage, du « vol » d'identité ou de données ou de l'utilisation de celles-ci pour faciliter un cambriolage.

Ces données massives produites (sous l'étiquette de *big data,* en référence – peu rassurante – au *Big Brother* orwellien) sont désormais régulièrement utilisées, croisées et agrégées dans différents contextes *(predictive analytics, data mining)* pour prédire de futurs risques, pour deviner les préférences des individus sur la base de corrélations statistiques (avancée d'une épidémie fondée sur les mots-clés utilisés dans les moteurs de recherche ou les localisations issues de téléphones portables, détection de fraudes dans l'utilisation de cartes de crédit[2], ciblage des clientes enceintes d'une chaîne de magasins sur la base de leurs profils d'achat[3], découverte d'effets secondaires de médicaments, conseils de lecture[4]) ou pour générer des décisions automatisées (analyse de solvabilité d'un client, détermination de profils suspects, éligibilité à une compagnie d'assurances, adaptation à un emploi)[5].

S'il est, en pratique, presque utopique dans cet univers technologique d'imaginer que chacun d'entre nous puisse véritablement décider si et dans quelle mesure une information relative à sa personne peut être diffusée à autrui, doit être détruite ou oubliée, faut-il en tirer la conclusion que, juridiquement, chacun d'entre nous ne puisse désormais plus revendiquer un *droit* fondamental à déterminer soi-même le sort des données qui nous concernent personnellement ? Dépassés par le développement d'un monde dont la maîtrise semble nous échapper, sommes-nous condamnés à abdiquer ?

La tentation est grande, car les atteintes résultant de la multiplication et de la diffusion généralisée des données personnelles ne sont pas encore perçues par une grande partie de nos concitoyens comme étant si importantes qu'elles justifieraient de prendre des mesures de protection particulières : « J'ai la conscience tranquille, je n'ai rien à cacher, peu m'importe l'utilisation par autrui de mes données personnelles » est un argument fréquent pour justifier son désintérêt pour une protection des données personnelles[6]. La désinvolture avec laquelle, encore, de multiples utilisateurs des réseaux sociaux informent

---

1 Sur ce constat, cf. par exemple FF 2012 255, p. 260 ss.

2 Le Forum économique mondial de Davos s'est penché en 2013 sur ces questions (sur ces exemples, et d'autres, cf. World Economic Forum, *Unlocking the Value of Personal Data : From Collection to Usage,* p. 25 ss.).

3 Charles Duhigg, « How Companies Learn your Secrets », *New York Times,* publié le 16 février 2012.

4 Sur ces exemples, cf. Omer Tene/Jules Polonetsky, « Privacy in the Age of Big Data : A Time for Big Decisions », *Stanford Law Review. Online, février 2012,* p. 63 ss (64 s).

5 Sur les problèmes posés par ces techniques sur le libre-arbitre et les droits fondamentaux plus généralement, cf. Tene/Polonetsky (n. 4) p. 65 ss ; Viktor Mayer-Schönberger/Cukier Kenneth, *Big Data : A Revolution that Will Transform How We Live, Work, and Think,* New York 2013, p. 175 ss. Ces techniques permettent même de réidentifier des données personnelles précédemment anonymisées (Tene/Polonetsky [n. 4], p. 65, avec réf. cit.).

6 Sur l'utilisation de cet argument durant les débats parlementaires relatifs à la protection des données, cf. Beat Rudin, « Die Erosion der informationellen Privatheit – oder : Rechtsetzung als Risiko ? », *in :* Thomas Sutter-Somm/Felix Hafner/Gerhard Schmid/Kurt Seelmann (éd.), *Risiko und Recht : Festgabe zum Schweizerischen Juristentag 2004,* Bâle/Genève/Berne 2004, p. 415–440, p. 429, note 74 (réf. cit.). En droit américain, pour justifier la surveillance sécuritaire, cf. Daniel J. Solove, *Nothing to Hide : The False Tradeoff between Privacy and Security,* New Haven 2011.

leurs « amis », et les « amis » de ces derniers, de leurs actions et pensées quotidiennes est un indice de cette absence de conscience des dangers potentiels.

En approfondissant la réflexion, l'argument est-il convaincant ? N'avons-nous vraiment rien à cacher, y compris le plus honnête, le plus prude, le plus intègre et le plus fidèle d'entre nous ? Notre comportement est pourtant influencé selon que nous nous savons observés ou non[7]. Plus généralement, il faut admettre que les interactions sociales sont pétries de micro-mensonges, de non-dits stratégiques, de données tronquées, d'informations adaptées au contexte ou au cercle de ses destinataires, de confidences et autres cachotteries nécessaires à notre bien-être psychique et social[8]. Quel invité dira en effet toute la vérité sur un mets au goût « spécial » confectionné par un hôte intentionné ou sur la décoration « intéressante » de son salon ? Quel assistant exprimera tout ce qu'il pense vraiment de la qualité de son article au professeur dont il est dépendant hiérarchiquement ? Qui ne compte pas sur un ami sincère pour limiter la diffusion de confidences ?

Le fait que nous laissions suinter constamment une grande quantité d'informations sur notre personne sans en être toujours véritablement conscients montre que nous avons abandonné la volonté de les contrôler nous-mêmes dans un certain nombre de cas, en espérant que cela ne portera pas à conséquence dans le futur. Il ne signifie pas encore que nous acceptions de manière libre et éclairée tous les traitements qui pourraient en être ultérieurement faits. La conscience de la gravité de l'atteinte ne se fait, souvent, sentir que plus tard – et trop tard[9].

Tout comme en matière de santé et d'écologie, les meilleures mesures restent préventives. Une fois divulguée, l'information qui a circulé sur les réseaux numériques devient encore plus difficile à oublier. Ne faudrait-il dès lors pas aller plus loin et étendre le principe de prévention, voire de précaution[10] ? La proposition d'introduire le principe d'utilisation économe des données[11] va dans ce sens.

Pour d'autres auteurs cependant, il faut se résigner ; il serait trop tard. Les progrès technologiques seraient trop avancés pour que la société soit en mesure d'en influencer le cours. L'individu n'étant plus en mesure de maîtriser lui-même le devenir des données relatives à sa personne, il faudrait dorénavant se limiter à censurer les seuls abus[12].

Dans cet article, je défendrai au contraire la nécessité de réaffirmer, et même de renforcer, le droit à l'autodétermination en matière de données personnelles. Les difficultés de mise en œuvre d'un droit fondamental ne sauraient en justifier le déclassement sans autre forme de procès.

2. De la protection de fait des données personnelles à la nécessité d'une protection par le droit

L'histoire de la protection des données personnelles est étroitement liée au développement technologique. Warren et Brandeis, dans leur article fondateur en 1890 sur le droit à la sphère privée *(right to privacy)* en *common law,* mettaient déjà clairement en exergue le rôle joué par les nouvelles inventions et *business methods* jusqu'alors inconnues. Ils visaient la photographie instantanée, la presse à sensation et de nombreux autres appareils mécaniques en prédisant que ces inventions permettraient de « crier sur les toits ce qui est chuchoté en cabinet » :

> « Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life, and numerous mechanical devices threaten to make good the prediction that ‹ what is whispered in the closet shall be proclaimed from the housetops › »[13].

Ils redoutaient que de telles invasions de la sphère privée conduisent à une douleur et une détresse psychologiques plus intenses que les simples blessures corporelles :

> « solitude and privacy have become more essential to the individual ; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury. »[14]

L'évolution a dépassé depuis longtemps les craintes des deux auteurs. Cela s'explique. Les « capteurs » de don-

---

7 Voir l'exemple de Beate Rössler, « Den Wert des Privaten ergründen – Philosophische Überlegungen zum Verhältnis zwischen Autonomie und Privatheit », *Digma* 2002, p. 106–113 rapporté par Rudin (n. 6), p. 422 ss, du sage intellectuel qui se prend à jouer au soldat d'opérette dans sa chambre, se croyant non observé ; Regina E. Aebi-Müller, Personenbezogene Informationen im System des zivilrechtlichen Persönlichkeitsschutzes, Berne 2005, p. 320.

8 « On ment tout le temps », cf. Daniel J. Solove, « The Virtues of Knowing Less : justifying Privacy Protections against Disclosure », *Duke Law Journal* 2003, vol. 53, p. 967–1066, p. 1052 : *« People lie about themselves all the time. ».*

9 Cf. Rudin (n. 6), p. 429 ss.

10 Sur cette application à la protection des données, cf. par exemple Stephan Brunner, « Mit rostiger Flinte unterwegs in virtuellen Welten », *Jusletter* 4 avril 2011, N. 45.

11 FF 2012 255, p. 265.

12 Cf. ci-dessous ch. 4.2.

13 Samuel D. Warren/Louis D. Brandeis, « The Right to Privacy », *Harvard Law Review* 1890, vol 4, p. 193–220, p. 195.

14 Warren/Brandeis (n. 13), p. 196.

nées personnelles étaient limités à la vue, l'ouïe et la mémoire des gens et à la consignation des informations dans différents registres, journaux ou autres carnets de note ou de croquis. Le développement technologique a progressivement supprimé les protections de fait de la sphère privée : les murs d'une chambre protégeaient les conversations privées, les étagères les plus hautes d'une armoire ou les fonds de tiroir les documents personnels, les limites de la mémoire humaine les informations et vues compromettantes, une futaie les galipettes crapuleuses et les documents sous forme imprimée stockés aux archives les recherches automatisées ou les profils de personnalité.

L'utilisation systématique à des fins raciales des machines à cartes perforées dès 1933 par les nazis illustre parfaitement ce dernier point[15]. De nombreux juifs allemands pensaient être protégés de fait contre la dictature hitlérienne en raison de la difficulté pratique de procéder à des recherches généalogiques aussi longues que laborieuses dans les registres imprimés classiques de l'état-civil et des précédents recensements de la population :

> « Since the advent of the Third Reich, thousands of Jews nervously assumed they could hide from the Aryan clause. »[16] With the denouement of September 15 approaching, Germany's own sense of Jewish numbers was changing dynamically. As Security Police Chief, Heydrich had concluded « it has become apparent that a great number of Jews in Germany have become baptized in the Evangelical and Catholic faiths with the idea that once they changed their residence, they would no longer appear as Jews in the registries. »[17]

C'était cependant méconnaître l'efficacité des nouvelles techniques de traitement automatisé des données personnelles qui permettaient désormais de procéder facilement à des recoupements en comparant les noms de famille et en suivant les changements de domicile afin d'établir des arbres généalogiques sur plusieurs générations de citoyens :

> « But Jews could not hide from millions of punch cards thudding through Hollerith machines, comparing names across generations, address changes across regions, families' trees and personal data across unending registries. It did not matter that the required forms or questionnaires were filled in by leaking pens or barely sharpened pencils, only that they were later tabulated and sorted by IBM's precision technology. »[18]
>
> « Laborious and protracted paper searches of individual genealogical records were possible. But each case could take months of intensive research. That wasn't fast enough for the Nazis. Hitler wanted the Jews identified en masse. Once drafted, the Nuremberg regulations would be completely dependent upon Hollerith technology for the fast, wholesale tracing of Jewish family trees that the Reich demanded. Hollerith systems offered the Reich the speed and scope that only an automated system could to identify not only half and quarter Jews, but even eighth and sixteenth Jews. »[19]

Le Tribunal fédéral, lui-même, a reconnu le rôle joué par les machines à cartes perforées dans l'extermination des juifs et des tsiganes :

> « IBM aurait fourni aux nazis une vaste assistance technologique, lors de la procédure de recensement de population, jusqu'aux décomptes des victimes dans l'enceinte des camps de concentration. La demande de Girca se fonde principalement sur un ouvrage écrit par Edwin Black, intitulé, dans sa version française, ‹ IBM et l'Holocauste ›. L'auteur [...] soutient la thèse selon laquelle, si les nazis sont parvenus à exterminer six millions de juifs durant la seconde Guerre mondiale, c'est en raison d'une organisation remarquable, qui a été rendue possible grâce à des machines à cartes perforées, propriété de l'entreprise américaine IBM, qui gérait ses filiales européennes par l'intermédiaire de son bureau de Genève[20].[...] Dans ces circonstances, la cour cantonale n'a pas violé le droit fédéral en considérant, sous l'angle de la vraisemblance et sans préjuger du bien-fondé de l'action en responsabilité, que la défenderesse, par l'entremise de son établissement genevois, pourrait avoir commis des actes de complicité de génocide au sens de l'art. 264 CP »[21].

L'action en responsabilité a en revanche été rejetée, ayant été jugée prescrite par le Tribunal fédéral[22].

La Cour suprême des Etats-Unis a eu l'occasion de mettre en évidence en 1989 ce type de protection des données personnelles *par le fait* en considérant que la publication de données personnelles dans des registres imprimés ne justifiait pas nécessairement la publicité des mêmes informations dans les bases de données électroniques. Comme il est très lent et laborieux de constituer des profils de personnalité en compulsant des fichiers classiques archivés et disséminés dans tout le pays, la Cour suprême a jugé que les documents imprimés, bien que publiquement consultables, protégeaient suffisamment la sphère

---

15 On trouvera une autre illustration durant la seconde guerre mondiale : celle des nazis voulant enrôler tous les hommes norvégiens en âge de combattre et dont les efforts ont été contrecarrés par la destruction, par la résistance, des machines servant à trier les fichiers (Francesca Bignami, « European Versus American Liberty : A Comparative Privacy Analysis of Anti-Terrorism Data-Mining », *Boston College Law Review* 2007, vol. 48, p. 609–698, p. 609 s.).

16 Edwin Black, *IBM and the Holocaust : The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation*, New York 2001, p. 107.

17 Black (n. 16), p. 109.

18 Black (n. 16), p. 107.

19 Black (n. 16), p. 108.

20 ATF 131 III 153, 154 s.

21 ATF 131 III 153, 163.

22 ATF 132 III 661.

privée des individus par l'« obscurité pratique » résultant de la difficulté de leur accès, contrairement aux bases de données informatiques. Il existe en effet une « vaste différence entre des dossiers publics qui peuvent être retrouvés à la suite d'une recherche diligente dans les fichiers des tribunaux, des archives municipales et des postes de police locaux à travers le pays et un relevé informatique situé dans un bureau centralisé » :

> « [It] requires us to balance the privacy interest in maintaining, as the Government puts it, the ‹ practical obscurity › of the rap sheets against the public interest in their release. [...] Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information. »[23]

Etre public pour un document, ou être dans l'espace public pour une personne, ne revêt plus la même signification dès lors que les protections de fait disparaissent. Une place publique durant la nuit (avant l'éclairage public) ou par temps de brume, un bosquet, une forêt ou un Paris médiéval tortueux avant les interventions urbanistiques d'Haussman offraient des barrières de fait à la diffusion des « données » relatives à sa personnes. Le « public » était en outre bien moins nombreux, souvent limité aux voisins ou aux passants ; les observateurs ne pouvaient compter que sur leur mémoire pour diffuser, par témoignage, des « données » qui concernaient votre personne ; les destinataires devaient se reposer sur la bonne foi de ces derniers.

Apparaître aujourd'hui sur la *Fifth Ave* et dans ses échoppes à New York, c'est être filmé mille fois, non seulement par des caméras de vidéo-surveillance, mais également apparaître sur les prises de vue de passants, et ensuite, peut-être, avoir son visage reconnu sur un réseau social. Si vous possédez un téléphone portable, votre déplacement sera connu de votre opérateur téléphonique, et même de vos amis si vous avez activé l'option localisation dans votre réseau social préféré. Vos dépenses seront tracées au centime dans les différents magasins visités. Vos impressions immortalisées en direct si vous les « gazouillez » *(tweeter)* au fur et à mesure. Le problème est patent : si le mot « public » n'a pas varié depuis un siècle, la technologie a fondamentalement modifié les implications qui en découlent. Warren et Brandeis posaient d'ailleurs exactement le même constat en 1890 : ils relataient un procès intenté par une actrice contre un photographe l'ayant saisie depuis le public dans un théâtre de Broadway avec un flash dans un rôle où elle apparaissait en collants[24]. Le lieu était public, et l'invention nouvelle.

La pratique est claire depuis lors, en Europe du moins[25] : en raison du développement des technologies de l'information, on peut porter atteinte à la sphère privée même dans un lieu public. Le sens de ce mot a changé ; le « public » se décline désormais en de multiples nuances, contribuant à rendre la distinction entre sphère publique et privée encore plus confuse[26] :

> « Da mit Hilfe elektronischer Datenverarbeitung personenbezogene Informationen in beliebigem Umfang gespeichert, verknüpft und reproduziert werden können, lassen sich auch an sich harmlose Informationen, die ohne Weiteres der Öffentlichkeitssphäre zuzurechnen wären, zu eigentlich schützenswerten Persönlichkeitsprofilen verdichten. »[27]

L'abattement progressif des protections de fait des données personnelles est un processus qui n'a cessé de prendre de l'ampleur depuis l'époque de Warren et Brandeis. Il s'est accéléré depuis la fin des années 1960, justifiant une intervention politique et juridique pour tenter de reconstruire ces protections par le droit. Si les premières législations sur la protection des données avaient dans le collimateur les grands ordinateurs centralisés, propriétés des Etats et des grandes firmes, elles ont dû par la suite affronter l'extension de l'informatique domestique où quelques ménages disposaient d'un micro-ordinateur – d'abord fixe et isolé, puis ensuite mobile et interconnecté dans un réseau mondial de communication – renversant toutes les barrières physiques qui ralentissaient ou empêchaient auparavant une diffusion facilitée des données personnelles. Aujourd'hui les capteurs de données personnelles ne sont plus limités à l'ordinateur de salon. Ils se sont tous multipliés, automatisés, digitalisés et interconnectés. Les ordinateurs investissent désormais les objets (réfrigérateurs, montres[28], lunettes[29]...) et même le corps humain (implantation de puces RFID, identifications biométriques informatisées).

---

23 U.S. Dept. of Justice v. Reporters Committee, 489 U.S. 749 (1989).

24 Dorothy Glancy, « Privacy and the Other Miss M », *Northern Illinois University Law Review* 1990, vol. 10, p. 401–440, p. 195.

25 Aux USA, cf. Solove (n. 6), p. 99 ss critiquant la conception extrêmement étroite de la *privacy* dans le contexte du 4ème amendement. Cf. ég. Bignami (n. 15), p. 624 ss.

26 Lawrence Lessig, *Code : Version 2.0,* New York 2006, p. 202 : « privacy in public ».

27 ATF 138 II 346, 359. Cf. ég. Message relatif à une nouvelle constitution fédérale du 20 novembre 1996, FF 1997 I 154 : « Une personne qui se montre en public, s'il est vrai qu'elle s'offre au regard et à l'écoute d'autrui, ne consent pas pour autant à ce que des organes de l'Etat consignent, par l'écrit, l'image ou le son, son comportement ou ses déclarations. ».

28 Cf. le projet d'« iWatch », une « smartwatch » d'Apple.

29 Cf. www.google.com/glass.

Dans le futur, l'ampleur du phénomène est difficile à prévoir. Prenons l'exemple de la vidéo-surveillance. Alors que les cassettes VHS enregistrant une image toutes les deux secondes et ré-effacée chaque jour pour stocker de nouvelles images conféraient une certaine obscurité pratique voici une décennie[30], l'informatisation, l'extension des capacités de stockage, la finesse des images offrent un potentiel de transparence inégalé. A parier, le futur sera encore plus orwellien[31]. On peut en pressentir les prémisses avec la reconnaissance faciale sur le web, la vidéo-téléphonie disponible désormais dans n'importe quel téléphone portable, la miniaturisation extrême des capteurs vidéo, l'agrégation de données massives *(big data)* et la démocratisation des drones civils pilotables par *iPad*[32]. Les prises de vue statiques de *Google Street View* apparaîtront bien vite désuètes le jour où le monde pourra être suivi en direct de partout. Même le directeur de l'une des plus puissantes agences de renseignements du monde a été incapable en 2012 de cacher sa correspondance électronique extra-maritale avec sa biographe[33] !

Il faudrait être aveugle pour ne pas admettre dans ce nouveau contexte que l'individu est en train de perdre, ou a déjà perdu, la maîtrise de ses données personnelles.

Mais tel était le cas en 1988 lorsque le Conseil fédéral a proposé une loi fédérale sur la protection des données :

> « En particulier l'individu n'est souvent plus en mesure de déterminer, même de manière approximative, quelles données le concernant sont traitées, par qui, où et quand. La maîtrise de ses propres données, il l'a perdue, et, avec elle, la faculté de choisir les personnes avec lesquelles il souhaite entrer en communication et ce qu'il entend leur faire savoir à son sujet. »[34]

Et tel était déjà aussi le cas en 1890 lorsque WARREN et BRANDEIS se plaignaient de l'invention de la photographie instantanée et des journaux à sensation qui diffusaient largement en les immortalisant des données auparavant éphémèrement accessibles ou limitées à un cercle restreint de personnes. Ils ne pouvaient plus déterminer librement quelles informations émanaient d'eux.

Ces juristes ont réagi en proposant de créer un droit à la protection de la sphère privée avec à la clef de nouvelles actions civiles ou de nouvelles dispositions pénales. De telles mesures réparatrices ou punitives ne suffisent évidemment plus depuis longtemps. Les Etats ont adopté un véritable arsenal d'instruments de politique publique, au sein desquels les instruments juridiques ne forment d'ailleurs qu'une partie, et qui ne permettent aujourd'hui plus à chacun – l'histoire se répète – de déterminer librement le sort des informations qui proviennent de notre personne.

Du constat de la perte de maîtrise de l'individu sur ses propres données consécutive à la disparition progressive de leurs protections de fait, le droit a toujours été mis au défi de redonner un contrôle aux citoyens. Au lieu de capituler devant la difficulté de la tâche, l'histoire nous montre qu'il faut simplement sans cesse remettre l'ouvrage sur le métier. La technologie modifie inexorablement les habitudes sociologiques communicationnelles. Le droit de la protection des données ne peut pas être un droit conservateur d'un passé nostalgique ; c'est un droit dynamique condamné à évoluer avec son temps. Facebook redéfinira aussi sûrement le standard de la sphère privée pour le XXI^e^ siècle que Kodak l'a fait, à la fin du XIX^e^, pour tout le XX^e^ siècle qui aura suivi.

Je conclurai de cette évolution la nécessité de reconstruire des barrières et des niches afin de recréer cette « obscurité pratique ». Le droit peut l'exiger. Une illustration : en Suisse, l'autorité n'est autorisée à publier les données personnelles que dans la version imprimée des publications officielles (recueils du droit fédéral et Feuille fédérale[35]). Une autre proposition en débat est d'introduire un droit d'exiger que les sites web ou autres applications mobiles soient « architecturalement » conçus de sorte à permettre à chacun de retrouver un contrôle effectif sur la diffusion de ses données personnelles[36]. Pour cela, l'utilisateur devrait être en mesure de créer facilement des barrières à la diffusion de ses données entre différentes catégories de personnes, comme la différenciation des « amis » en plusieurs catégories dans Facebook ou en « cercles » dans Google+ le permet, ou d'envoyer des textes et des images s'auto-détruisant après lecture[37]. Le Forum économique mondial vient de préconiser une approche technologique

---

30 JEAN RUEGG/ALEXANDRE FLÜCKIGER/VALÉRIE NOVEMBER/FRANCISCO KLAUSER, *Vidéosurveillance et risques dans l'espace à usage public : représentations des risques, régulation sociale et liberté de mouvement,* Genève 2006, p. 54.

31 On notera qu'ORWELL est, technologiquement parlant, aujourd'hui déjà dépassé ! Cf. LAWRENCE LESSIG, « On the Internet and the Benign Invasions of Nineteen Eighty-Four », *in :* Abbott Gleason/Jack Goldsmith/Martha C. Nussbaum (éd.), On « Nineteen Eighty-Four » : Orwell and Our Future, Princeton 2005, p. 212–221, cit. ci-dessous ch. 3.2.

32 TIME MAGAZINE, *Rise of the Drones,* édition du 11 février 2013.

33 THE NEW YORK TIMES, *Online Privacy Issue Is Also in Play in Petraeus Scandal,* 13 novembre 2012.

34 Message concernant la loi fédérale sur la protection des données (LPD) du 23 mars 1988, FF 1988 II 421, p. 425.

35 Art. 16 al. 3 LPubl, RS 170.512.

36 Cf. ci-dessous ch. 5.

37 Comme l'application www.snapchat.me le permet désormais pour les photographies.

et organisationnelle digne d'intérêt au problème : renforcer le pouvoir des individus en leur proposant de réunir et de stocker toutes les données qui les concernent dans des « dépôts de données personnelles » *(personal data stores)* afin que chacun puisse exercer un contrôle effectif sur ses données, associé à un système de couplage des données à des informations sur leur origine, leur provenance ou leurs autorisations (métadonnées)[38].

On se réapproprierait ainsi l'architecture pré-technologique qui limitait de fait la communication et la mémorisation des informations : le tiroir sous clé du bureau, le cabinet du médecin pour les divulgations médicales, le jardin du grand-père pour les fêtes familiales, le café du commerce pour les propos éponymes, la salle de classe pour les cours, l'urne pour les votations, le bureau du banquier pour les finances, la place publique pour l'expression politique ou le bosquet pour les cabrioles…

3. Vers la reconnaissance internationale d'un droit à l'autodétermination en matière de données personnelles

3.1. Les premiers pas en *common law*

Pour les premiers théoriciens du droit à la protection de la sphère privée, en 1890, la réponse à la question de savoir pourquoi il faudrait conférer un droit à chacun de se déterminer sur le sort de ses données personnelles devait être recherchée dans l'adaptation aux temps modernes de deux libertés fondamentales de l'être humain : la protection de la personne et la garantie de sa propriété. La première a évolué de la protection de la vie et de l'intégrité physique à l'épanouissement psychique et l'objet de la seconde s'est étendu des choses aux biens immatériels. Le droit à la vie est devenu le droit de jouir de la vie – le droit d'être laissé tranquille *(« the right to be let alone »)* :

> « Gradually the scope of these legal rights broadened ; and now the right to life has come to mean the right to enjoy life, – the right to be let alone »[39].

Un moyen pour assurer ce droit est de garantir à chacun le droit de déterminer dans quelle mesure ses pensées, ses sentiments et ses émotions doivent être communiquées aux autres, au public ou seulement à ses amis. Les bases du droit à l'autodétermination en matière d'informations personnelles sont ainsi posées ; elles trouveraient même leurs racines dans un jugement de 1769 :

> « the common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others. »[40] [affirmation illustrée en note de bas de page par l'opinion suivante : « ‹ It is certain every man has a right to keep his own sentiments, if he pleases. He has certainly a right to judge whether he will make them public, or commit them only to the sight of his friends. › J. Yates, in *Millar v. Taylor,* […] (1769) »[41].

Etre en mesure de s'opposer à la communication de telles informations est simplement un moyen de mettre en œuvre le droit plus général d'être laissé tranquille :

> « These considerations lead to the conclusion that the protection afforded to thoughts, sentiments, and emotions […] is merely an instance of the enforcement of the more general right of the individual to be let alone »[42].

Retranscrit en vocabulaire plus moderne, le droit à l'autodétermination en matière de données personnelles doit être considéré comme un moyen de garantir le droit à la liberté individuelle et plus précisément à la protection de la sphère privée.

La doctrine majoritaire puis la jurisprudence américaines ont depuis repris l'idée, toujours en mettant le pouvoir de détermination individuel en exergue :

> « Privacy is the claim of individuals... to determine for themselves when, how, and to what extent information about them is communicated to others »[43].

Le droit à la protection de la sphère privée *(« privacy »)* a été érigé au rang constitutionnel par la Cour suprême ; il est au fondement du droit américain de la protection des données :

> « Appellees contend that the statute invades a constitutionally protected ‹ zone of privacy. › The cases sometimes […] characterized as protecting ‹ privacy › have in fact involved at least two different kinds of interests. […] One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions. »[44]

---

38 Cf. ci-dessous ch. 6.6 ; World Economic Forum (n. 2), p. 13 et 23 ; Ira Rubinstein, « Big Data : The End of Privacy or a New Beginning ? », *International Data Privacy Law,* 2013, p. 1–14. Sur les moyens techniques en général, cf. Jean-Henry Morin, « L'utilisation des moyens techniques en vue d'une amélioration de la protection des données », *in : Le développement du droit européen en matière de protection des données et ses implications pour la Suisse,* Zurich, 2012, p. 1–13.

39 Warren/Brandeis (n. 13), p. 193.

40 Warren/Brandeis (n. 13), p. 198.

41 Warren/Brandeis (n. 13), p. 198, note 2.

42 Warren/Brandeis (n. 13), p. 205.

43 A. Westin, Privacy and Freedom 7 (1967), tel que cité par la Cour Suprême dans United States Department of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989), note 16, avec encore d'autres réf.

44 *Whalen v. Roe,* 429 U.S. 589 (1977). Outre ce droit constitutionnel à la « privacy » et à l'« information privacy », la Constitution fédérale protège la « privacy » par le biais du 1er amendement (droit de

La Cour suprême a défini la notion de *« privacy »* comme le pouvoir de contrôle sur les informations concernant sa personne *(« individual's control of information concerning his or her person »)* :

> « both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person. »[45]

La doctrine majoritaire partage cette conception fondée sur le contrôle de ses informations personnelles *(« control over personal information »)*[46] :

> « the right to information privacy – my right to control your communication of personally identifiable information about me – is a right to have the government stop you from speaking about me »[47].

3.2. La consécration par la Cour constitutionnelle allemande

Sur le continent européen, la Cour constitutionnelle allemande a repris l'idée[48], il y a trente ans exactement, dans un arrêt-phare, en érigeant le droit à l'autodétermination en rang constitutionnel *(Recht auf « informationelle Selbstbestimmung »)* à propos d'une loi sur le recensement de la population. Défini comme le droit de l'individu de se déterminer en principe lui-même sur la divulgation et l'utilisation de ses données personnelles, l'autodétermination trouve son fondement dans la dignité de l'être humain (art. 1 I GG) et la liberté personnelle (art. 2 I GG) :

> « Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. »[49]

Selon la Cour, ce droit devrait en particulier empêcher l'avènement d'une société dans laquelle les citoyens ne peuvent plus savoir qui sait quoi sur eux, quand et dans quelle circonstance :

> « Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiss. »[50]

Une telle société « compromettrait non seulement les possibilités d'épanouissement personnel de chacun, mais aussi le bien commun dans la mesure où l'autodétermination est une condition essentielle à la garantie d'une société libre et démocratique fondée sur les capacités et la solidarité de ses citoyens »[51]. Empreint de la volonté de prévenir à tout jamais les dérives hitlériennes, on pouvait espérer qu'un pareil droit éviterait la survenance des pires scénarios orwelliens ou kafkaïens. Trente ans plus tard, force est de constater que la mise en œuvre du principe n'a pas suivi. Dans *1984* de GEORGE ORWELL, Winston Smith pouvait au moins trouver des endroits où se cacher des « télécrans »[52] ; est-ce aujourd'hui possible sur le web, ou dans les villes anglo-saxonnes extensivement vidéo-surveillées ?

> « That's not the world we live in today. You can't know whether your search on the Internet is being monitored. You don't know whether a camera is trying to identify who you are. Your telephone doesn't make funny clicks as the NSA listens in. Your e-mail doesn't report when some bot has searched it. »[53]

En 2008, la Cour a complété le droit à l'autodétermination informationnelle, qu'elle a jugé insuffisant, en consacrant un droit fondamental à la confidentialité et à l'intégrité des systèmes techniques d'information à propos d'une surveillance informatique policière secrète[54].

---

s'exprimer anonymement not.), du 3e, du 4e et du 5e également (cf. un résumé *in :* DANIEL J. SOLOVE/PAUL M. SCHWARTZ, Privacy Law : Fundamentals, Portsmouth 2011, p. 3).

45 *United States Department of Justice v. Reporters Comm. for Freedom of the Press,* 489 U.S. 749,763 (1989).

46 « One of the most predominant theories of privacy » selon DANIEL J. SOLOVE, « Conceptualizing Privacy », *California Law Review* 2002, vol. 90, p. 1087–1156, p. 1109 ss, qui cite de nombreuses références.

47 EUGENE VOLOKH, « Freedom of Speech and Information Privacy : The Troubling Implications of a Right to Stop People from Speaking About You », *Stanford Law Review* 2000, vol. 52, n. 5, p. 1049–1124, p. 1050 s., cit. *in :* SOLOVE (n. 8), p. 976.

48 Sur les différences entre le droit américain et allemand à ce propos, cf. PAUL SCHWARTZ, « The Computer in German and American Constitutional Law : Towards an American Right of Informational Self-Determination », *The American Journal of Comparative Law* 1989, vol. 37, p. 675–702, p. 675 ss, qui estime pourtant que l'on ne peut pas lire dans l'arrêt allemand un véritable pouvoir de contrôle sur ses données personnelles en raison du caractère non absolu du droit à l'autodétermination, reconnu d'ailleurs par la Cour elle-même (p. 690).

49 BVerfG 65, 1 C.II.1a ; BVerfG, 1 BvR 370/07 du 27.2.2008, N. 198.

50 BVerfG 65, 1 C.II.1a.

51 « Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist. » (BVerfG 65, 1 C.II.1a).

52 LESSIG (n. 31), p. 212, repris *in :* LESSIG (n. 26), p. 208.

53 LESSIG (n. 26), p. 208 s.

54 « Dieses Recht [Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme] fusst gleich dem Recht auf informationelle Selbstbestimmung auf Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG ; es bewahrt den persönlichen und privaten Lebensbereich der Grundrechtsträger vor staatlichem

3.3. Une approche européenne en évolution

En droit de l'Union européenne, « toute personne a droit à la protection des données à caractère personnel la concernant » (art. 16 I TFUE). Cette disposition a été reprise et complétée dans la Charte des droits fondamentaux (art. 8) par des exigences matérielles :

> « Toute personne a droit à la protection des données à caractère personnel la concernant.
>
> Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.
>
> Le respect de ces règles est soumis au contrôle d'une autorité indépendante. »

Le droit à l'autodétermination en matière de données personnelles n'est pas explicitement mentionné dans le texte. Le consentement, au fondement du droit à l'autodétermination, est cependant explicitement mentionné dans la Charte. La notion de « traitement » devrait être interprétée largement selon la doctrine[55]. Par ailleurs, l'esprit du projet de la révision en cours de la législation sur la protection des données est celui de renforcer le contrôle sur ses données, comme le slogan de la Commission européenne le montre : « *Take control of your personal data* »[56].

La Cour européenne des droits de l'homme a déduit pour sa part le droit à la protection des données personnelles de celui du respect de la vie privée et familiale (art. 8 I CEDH)[57]. Contrairement à la Cour allemande, elle n'a à ce jour pas explicitement reconnu un droit indépendant à l'autodétermination informationnelle. Elle n'en serait toutefois plus très éloignée, comme le soutient avec raison une partie de la doctrine[58]. L'autodétermination est en effet un principe qui sous-tend implicitement l'ensemble de la jurisprudence relative à la protection des données. Le Tribunal fédéral en fait la même lecture puisqu'il se réfère également à l'article 8 CEDH pour fonder le droit à l'autodétermination dans sa jurisprudence récente[59]. Pareille interprétation est de plus en totale cohérence avec la volonté de l'Assemblée parlementaire du Conseil de l'Europe qui a adopté, en 1998 déjà, une résolution demandant d'ajouter à la définition du droit au respect la vie privée le « droit de contrôler ses propres données », soit l'essence même de l'autodétermination en matière de données personnelles :

> « 4. Le droit au respect de la vie privée, garanti par l'article 8 de la Convention européenne des Droits de l'Homme, a déjà été défini par l'Assemblée dans la déclaration sur les moyens de communication de masse et les droits de l'homme contenue dans la Résolution 428 (1970) comme ‹ le droit de mener sa vie comme on l'entend avec un minimum d'ingérence ›.
>
> 5. Pour tenir compte de l'apparition des nouvelles technologies de la communication permettant de stocker et d'utiliser des données personnelles, il convient d'ajouter à cette définition le droit de contrôler ses propres données. »[60]

En 2012, le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[61], a renouvelé l'idée en proposant de compléter le préambule de la convention par le droit de contrôler ses propres données :

Zugriff im Bereich der Informationstechnik auch insoweit, als auf das informationstechnische System insgesamt zugegriffen wird und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten. » (BVerfG, 1 BvR 370/07 du 27.2.2008, N. 201). Sur la (non-)réception de celui-ci en droit suisse, cf. PHILIPPE MEIER, Protection des données : Fondements, principes généraux et droit privé, Berne 2011, p. 74, et réf. cit.

55 ASTRID EPINEY/YVONNE SCHLEISS, « Völker- und europarechtlicher Rahmen », *in :* Eva Maria Belser/Astrid Epiney/Bernhard Waldmann (éd.), Berne 2011, p. 53–296, p. 127, note 30.

56 EUROPEAN COMMISSION – DIRECTORATE-GENERAL FOR JUSTICE, *Take control of your personal data,* Luxembourg 2012.

57 Pour une liste recensant les multiples références doctrinales et jurisprudentielles, cf. EPINEY/SCHLEISS (n. 55), p. 60 ss. On évoquera également l'article 16 de la Convention de l'ONU relative aux droits de l'enfant (RS 0.107) qui contient une disposition analogue à l'article 8 CEDH. Sur le droit des enfants à la protection de leur vie privée dans le monde numérique en rapport avec l'art. 16 de cette convention, cf. DÉFENSEUR DES DROITS, *Enfants et écrans : grandir dans le monde numérique,* rapport 2012 consacré aux droits de l'enfant, Paris 2012, p. 85 et 91 ; sur les insuffisances du dispositif de protection des données personnelles de l'adolescent en droit du Conseil de l'Europe, de l'Union européenne et français, cf. LE MÊME, p. 92 ss.

58 EPINEY/SCHLEISS (n. 55), p. 64 ; MARKUS SCHEFER/SANDRA STÄMPFLI, « Die Grundlagen des Datenschutzes im Rahmen von Schengen », *in :* Stephan Breitenmoser/Sabine Gless/Otto Lagodny (éd.), Zurich 2009, p. 135–157, p. 139. Plus généralement on peut à raison considérer, sur le fondement de la protection de la sphère privée en droit international public, que la protection des données personnelles signifie en définitive un droit à l'autodétermination informationnelle : « Datenschutz ist aus dem Recht auf Achtung der Privatsphäre in seiner Ausprägung als persönliche Autonomie und der damit zusammenhängenden Selbstbestimmung hervorgegangen und bedeutet damit – auch im Rahmen des Schutzes der Privatsphäre – letztlich ein Recht auf ‹ informationelle Selbstbestimmung › » (EPINEY/SCHLEISS [n. 55], p. 56). *Contra :* THOMAS GÄCHTER/PHILIPP EGLI, « Informationsaustausch im Umfeld der Sozialhilfe », *Jusletter* 6 septembre 2010, p. 11, se référant à MARION ALBERS, *Informationelle Selbstbestimmung,* Baden-Baden 2005, p. 297.

59 Cf. ci-dessous ch. 4.3 *i.f.*

60 Résolution 1165 (1998) *Droit au respect de la vie privée,* citée *in :* CourEDH, *Von Hannover c. Allemagne (II),* 40660/08 et 60641/08, du 7 février 2012, N. 71.

61 STE N° 108 ; RS 0.235.1.

« Considérant qu'il est nécessaire, eu égard à la diversification, l'intensification et à l'internationalisation des échanges et des traitements de données à caractère personnel, de garantir la dignité humaine ainsi que la protection des droits de l'homme et des libertés fondamentales de chacun, notamment au moyen du droit de contrôler ses propres données et les traitements qui en sont faits. »[62]

La présence de ce droit en préambule témoigne qu'il ne s'agit pas d'un droit nouveau. Le projet de révision reconnaît plutôt de cette façon l'existence du droit de contrôle tel que défini en 1998 par l'Assemblée parlementaire du Conseil de l'Europe. Il permet également d'expliquer l'esprit sous-jacent aux différents droits contenus dans la convention – en particulier ceux de l'article 8 (notamment celui de connaître l'existence des données et les finalités de leur récolte, exiger leur rectification ou leur effacement, disposer d'une voie de droit) – qui consiste à conférer à l'individu un pouvoir de contrôle, donc à lui permettre de se déterminer sur ses données personnelles[63].

4. La reconnaissance en droit suisse d'un droit à l'autodétermination en matière de données personnelles

4.1. La place de la protection des données personnelles au sein des droits fondamentaux

Le droit à la protection des données personnelles est un aspect du droit au respect de la sphère privée selon la nouvelle Constitution fédérale de 1999[64]. Pour mettre en évidence cette caractéristique, il a été intégré dans un intitulé commun :

« Art. 13 Protection de la sphère privée

[1] Toute personne a droit au respect de sa vie privée et familiale, de son domicile, de sa correspondance et des relations qu'elle établit par la poste et les télécommunications.

[2] Toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent. »

Ce rattachement a parfois été critiqué[65]. Historiquement d'ailleurs, il trouve son origine dans la liberté personnelle[66]. Doctrine et jurisprudence sont unanimes à reconnaître que l'emploi des données personnelles met en cause d'autres droits fondamentaux également, même si les distinctions sont difficiles à opérer, car les recoupements sont inévitables[67]. En droit conventionnel, la protection des données relève également du respect de la vie privée (art. 8 CEDH)[68].

Il ne faut pas déduire de cette systématique, en particulier de l'intitulé de la disposition, que seul entrerait dans le champ du droit protégé l'emploi des données personnelles portant concrètement atteinte à la sphère privée[69]. En réalité, tout comme en droit conventionnel, on peut affirmer que le rapport à la sphère privée est présumé en présence de données personnelles[70] ; l'article 13 II Cst. ne doit ainsi pas uniquement être interprété dans le cadre exclusif de la théorie des sphères[71] ; il doit être compris

---

62 Comité consultatif, version du 10 décembre 2012 [T-PD (2012) RAP 29 Abr_fr].

63 Cette proposition n'a pas été acceptée dans le projet sans discussion : « Des opinions divergentes sont par ailleurs exprimées au sujet de l'introduction du droit de contrôler ses propres données dans le Préambule, telle que figurant dans les propositions de modernisation. Tandis que les partisans de cette proposition estiment que la maîtrise de l'information est un aspect important de la protection des données, que ce droit découle de plus du droit à la vie privée et que, par conséquent, le lien avec la Convention européenne des droits de l'homme se justifie pleinement, d'autres, en revanche, estiment que cette insertion peut ajouter de la confusion en donnant le sentiment que l'on consacrerait un nouveau droit. » (Comité consultatif, séance du 24 septembre 2012, ch. 23 [T-PD (2012) RAP 28]).

64 ATF 138 I 331, 337 ; Message relatif à une nouvelle constitution fédérale du 20 novembre 1996, FF 1997 1, p. 155 ; Meier (n. 54), p. 66 ; Jörg Paul Müller/Markus Schefer, Grundrechte in der Schweiz, Im Rahmen der Bundesverfassung, der EMRK und der UNO-Pakte, 4ème éd., Berne 2008, p. 164 s.

65 Cf. par exemple Gächter/Egli (n. 58), N. 36 ss ; Rudin (n. 6), p. 421. Pour un résumé des critiques, cf. ATF 138 I 331, 337, qui a refusé d'entrer en matière sur celles-ci.

66 Cf. ci-dessous ch. 3.1 et 3.2.

67 ATF 138 I 331, 337 ; Eva Maria Belser, « Der grundrechtliche Rahmen des Datenschutz », *in :* Eva Maria Belser/Astrid Epiney/Bernhard Waldmann (éd.), Datenschutzrecht : Grundlagen und öffentliches Recht, Berne 2011, p. 319–410, p. 332 et p. 394 ss ; Rudin (n. 6), p. 419.

68 ATF 138 I 331, 338 ; Epiney/Schleiss (n. 55), p. 60 – les deux avec réf. cit.

69 Cf. par exemple Pascal Mahon, « Les enjeux du droit à l'information », *in :* Thierry Tanquerel/François Bellanger (éd.), L'administration transparente : actes de la IVe Journée de droit administratif, organisée à Genève le 7 mars 2001, Genève/Bâle/Munich 2002, p. 9–41, p. 36. La Cour constitutionnelle allemande l'a précisé clairement : « Der Schutzumfang des Rechts auf informationelle Selbstbestimmung beschränkt sich dabei nicht auf Informationen, die bereits ihrer Art nach sensibel sind und schon deshalb grundrechtlich geschützt werden. Auch der Umgang mit personenbezogenen Daten, die für sich genommen nur geringen Informationsgehalt haben, kann, je nach dem Ziel des Zugriffs und den bestehenden Verarbeitungs- und Verknüpfungsmöglichkeiten, grundrechtserhebliche Auswirkungen auf die Privatheit und Verhaltensfreiheit des Betroffenen haben » (BVerfG, 1 BvR 370/07 du 27.2.2008, N. 198).

70 Epiney/Schleiss (n. 55), p. 63.

71 Rudin (n. 6), p. 421 ; Gächter/Egli (n. 58), N. 38 ; Brunner (n. 10), N. 6. Sur la critique de la théorie des sphères dans le monde digital, cf. par exemple Rolf H. Weber, « Neue Grundrechtskonzeptionen zum Schutz der Privatheit », *in :* Rolf H. Weber/Florent

comme une expression de l'autonomie de l'individu[72]. Disposer de la maîtrise de ses propres données a certes pour effet d'améliorer la protection de sa sphère privée. L'objet de l'atteinte au droit à l'autodétermination en matière de données personnelles est cependant différent ; la seule violation de la volonté de la personne relative à la manière de traiter ses données personnelles suffit[73].

Fondamentalement pourtant, le rattachement me paraît pertinent. L'esprit de la protection des données réside bien, en fin de compte, dans la protection de la sphère privée. Dans le monde télécommunicationnel d'aujourd'hui, puis-je encore trouver un endroit où je puisse « être laissé tranquille » *(« be let alone »),* seul, avec ma famille, mes amis, mes collègues, mon banquier ou mon médecin, sélectionnant moi-même les informations que je veux bien partager, mais avec eux seulement, sans être épié ou surveillé par mes voisins, mon employeur, mon propriétaire, mon assureur, mon vendeur, mes parents, les services administratifs, les Etats étrangers ou par les curieux de la planète entière ?

4.2. Une disposition constitutionnelle mal rédigée

Ni le texte constitutionnel ni le Message qui l'accompagne n'évoquent explicitement un droit à l'autodétermination en matière de données personnelles. Le second, précisant que le droit de consultation et de rectification de ses propres données permet aux personnes concernées de se protéger des abus[74], se réfère cependant, en note de bas de page, à l'arrêt de la Cour constitutionnelle allemande sur le recensement de la population :

> « A moins que l'ordre juridique n'en dispose autrement, chacun doit pourvoir déterminer la valeur qu'il attache à ses propres données et l'utilisation qu'il souhaite qu'on en fasse. Chaque individu doit pouvoir déterminer librement le cercle des personnes avec qui il souhaite entrer en communication et sous quelle forme. »[75]

Selon le Conseil fédéral et la doctrine majoritaire, le contenu de la disposition constitutionnelle va plus loin que sa lettre ne laisserait l'entendre ; l'article 13 II Cst. protège aussi l'utilisation « ordinaire » des données personnelles, et non seulement abusive, en conférant à chacun le droit, constitutionnel, de déterminer soi-même dans quelle mesure des données relatives à sa personne peuvent être traitées par les autorités et/ou les particuliers[76]. La rédaction de la disposition constitutionnelle « prête à confusion »[77] ; elle est « malheureuse »[78], pour les tenants

Thouvenin (éd.), Neuer Regulierungsschub im Datenschutzrecht ?, Zurich 2012, p. 7–29, p. 13 et 16 ; Brunner (n. 10), N. 6 ; Aebi-Müller (n. 7), p. 303.

72 Rudin (n. 6), p. 421.

73 Aebi-Müller (n. 7), p. 284.

74 Message relatif à une nouvelle constitution fédérale du 20 novembre 1996, FF 1997 I, p. 155.

75 Message concernant la loi fédérale sur la protection des données (LPD) du 23 mars 1988, FF 1988 II, p. 426.

76 FF 2012 255, p. 270 s. ; Ulrich Häfelin/Walter Haller/Helen Keller, Schweizerisches Bundesstaatsrecht, 8ème éd., Zurich 2012, N. 389 ; Meier (n. 54), p. 65 et 74 ; Pierre Moor/Alexandre Flückiger/Vincent Martenet, Droit administratif : Les fondements, vol. I, 3ème éd., Berne 2012, p. 949 ; René Rhinow/Markus Schefer, Schweizerisches Verfassungsrecht, Bâle 2009, N. 1376 ; Giovanni Biaggini, BV : Bundesverfassung der Schweizerischen Eidgenossenschaft und Auszüge aus der EMRK, den UNO-Pakten sowie dem BGG, Zurich 2007, Art. 13, N. 11 et 13 ; Regina Kiener/Walter Kälin, Grundrechte, Berne 2007, p. 158 ; Müller/Schefer (n. 64), p. 168 ; Céline Gutzwiller, Droit de la nationalité et fédéralisme en Suisse, Genève 2008, p. 423 ; Andreas Auer/Alexandre Flückiger, « La vidéosurveillance dans l'œil de la Constitution », *PJA/AJP* 2006, p. 924–942, p. 933 s ; Sandrine Rohmer, Spécificité des données génétiques et protection de la sphère privée : les exemples des profils d'ADN dans la procédure pénale et du diagnostic génétique, Zurich/Genève 2006, p. 55 ss ; Rudin (n. 6), p. 419 s. ; Jörg Paul Müller/Martin Looser, « Les problèmes principaux de la protection des données en Suisse », *in :* Pierre Tabatoni (coor.), La protection de la vie privée dans la société d'information, vol. 3, Paris 2002, p. 67–90, p. 80 ; Jörg Paul Müller, Grundrechte in der Schweiz : im Rahmen der Bundesverfassung von 1999, der UNO-Pakte und der EMRK, 3ème éd., Berne 1999, p. 45. Gächter/Egli (n. 58), N. 19 et 38, reconnaissent que la disposition est rédigée trop étroitement et que la notion d'abus doit être interprétée plus largement, sans admettre cependant l'existence d'un droit à l'autodétermination informationnelle. Belser (n. 67), p. 121 et 399 ss, critique les deux aspects : interprétation littérale limitant l'étendue du droit à l'emploi abusif et non-reconnaissance d'un droit à l'autodétermination (cf. ég. Eva Maria Belser/Bernhard Waldmann, Grundrechte II : Die einzelnen Grundrechte, Zurich 2012, p. 79). Pascal Mahon, « Art. 13 », *in :* Jean-François Aubert/Pascal Mahon, Petit commentaire de la Constitution fédérale de la Confédération suisse du 18 avril 1999, Zurich/Bâle/Genève 2003, p. 123–131, Art. 13, N. 16, et Andreas Auer/Giorgio Malinverni/Michel Hottelier, Droit constitutionnel suisse : Les droits fondamentaux, vol. II, 2ème éd., Berne 2006, N. 386 s. déduisent de la disposition constitutionnelle le droit de consulter ses données, de les faire rectifier et d'éliminer les « inutiles », sans évoquer ni discuter le droit à l'autodétermination, si bien que l'on ne saurait en inférer qu'ils en critiquent le principe, du moins explicitement.

77 « L'expression ‹ emploi abusif › ne doit pas être comprise dans le sens que seule l'utilisation illicite de données relatives à un tiers tomberait dans le champ d'application de cette disposition. Contrairement à la lettre de l'art. 13, al. 2, la Constitution fédérale garantit de manière générale au particulier le droit de pouvoir décider lui-même à qui et quand il veut dévoiler ses données personnelles. » (Müller/Looser [n. 76], p. 80).

78 Meier (n. 54), p. 65 ; Rainer J. Schweizer, « Art. 13 Abs. 2 », *in :* Bernhard Ehrenzeller/Philippe Mastronardi/Rainer J. Schweizer/Klaus A. Vallender (éd.), Die schweizerische Bundesverfassung : Kommentar, 2ème éd., Zurich 2008, p. 324–334, N. 39 (« missglückt ») ; Rudin (n. 6), p. 419 et 425.

de la doctrine majoritaire du moins. En d'autres termes, pour cette dernière, le terme d'« emploi abusif » doit être compris comme un emploi contraire à la détermination de la personne sur le traitement de ses données.

La lecture littéraliste par la doctrine minoritaire[79] conduit à sortir l'emploi courant (non « abusif ») des données personnelles de la protection de l'article 13 II Cst. Le simple traitement « normal » effectué sans consentement ne serait à lui seul plus protégé constitutionnellement[80]. On ouvrirait à mon avis là une boîte de Pandore susceptible de remettre en cause un certain nombre d'acquis législatifs et jurisprudentiels, tant fédéraux qu'internationaux[81] : la simple conservation de données serait-elle toujours « abusive » ? L'utilisation à des fins publicitaires ou de marketing ordinaire le serait-elle ? Qu'en serait-il du renseignement sur la solvabilité d'autrui ? Il reviendrait dans toutes ces hypothèses à la personne concernée d'apporter la preuve d'un « abus », notion extrême aux contours flous qui conduirait dans le futur à limiter la protection à des cas exceptionnels. L'usage normal ne serait plus protégé. L'individu perdrait en fin de compte la maîtrise juridique de ses données personnelles, après en avoir déjà perdu la maîtrise de fait. Tombant en quelque sorte dans le « domaine public », les données personnelles seraient ainsi, par exemple, mises à la libre disposition des grandes entreprises de réseaux sociaux, sites de ventes à distance et autres sites de partage d'images pour leur usage « normal », se réfugiant dans le caractère vague et discutable de la notion d'« abus » pour exercer à notre place la maîtrise effective sur nos propres données.

L'interprétation littérale de l'article 13 II Cst. serait en outre difficilement compatible avec le droit international (CEDH, Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[82], dispositions de l'Union européenne pertinentes pour la Suisse[83]). Ces textes n'imposent certes pas explicitement le droit à l'autodétermination mais celui-ci peut être déduit de leur pratique[84]. Ils fixent en tous les cas un standard de protection plus élevé que la seule limitation à l'utilisation abusive[85]. Pour que la Suisse soit en mesure de respecter ses engagements internationaux (art. 5 Cst.), les autorités devraient recourir à la méthode de l'interprétation conforme et considérer que les traitements de données personnelles contraires au droit international seraient « abusifs ». La solution est pragmatique mais dogmatiquement insatisfaisante, comme c'est souvent le cas avec ce type d'interprétation[86]. Le Tribunal devrait par ailleurs refuser d'appliquer une loi fédérale contraire à l'autodétermination en matière de données personnelles telle que découlant implicitement de la jurisprudence de la Cour européenne relative à l'article 8 CEDH[87]. Le constituant lui-même n'aurait en outre plus le droit de modifier l'article 13 II Cst. dans un sens contraire à l'interprétation donnée à l'article 8 CEDH par la Cour de Strasbourg comme le Tribunal fédéral vient de le reconnaître[88]. De plus, indépendamment d'une procédure judiciaire, la Suisse risquerait de perdre le niveau de protection « adéquat » exigé par le Conseil de l'Europe[89] et l'Union européenne[90], rendant problématique l'échange transfrontière de données dans le futur[91].

On notera enfin que l'imprécision rédactionnelle a été reprise en droit cantonal. En effet, les constitutions cantonales qui garantissent un droit à la protection des données personnelles prémunissent en général contre un usage abusif[92]. Ce n'est que plus rarement qu'elles ne se limitent pas à l'emploi abusif[93]. En outre, si aucun canton ne mentionne explicitement un droit à l'autodétermination, plusieurs d'entre eux en reconnaissent des composantes spécifiques, à l'exemple du droit de consultation de ses propres données[94], de celui de rectification des données

79 Belser (n. 67), p. 378 et 400. Cf. n. 76 *i.f.*

80 A déduire de Belser (n. 67), N. 115.

81 Dans ce sens, cf. Schweizer (n. 78), N. 39. Plus optimiste en revanche : Belser (n. 67), p. 399 ss.

82 RS 0.235.1.

83 Pour un exposé du droit de l'Union et de sa pertinence pour la Suisse, cf. Epiney/Schleiss (n. 55), p. 119 ss et 283 ss.

84 Cf. ci-dessus ch. 3.3.

85 Sur cet argument, cf. Rudin (n. 6), p. 420.

86 Moor/Flückiger/Martenet (n. 76), p. 305 s et 349 ss.

87 Cf. art. 190 Cst., Moor/Flückiger/Martenet (n. 76), p. 373. A la différence de la convention du Conseil de l'Europe, non directement applicable, même si certaines dispositions, à l'exemple des art. 5 et 8, pourraient l'être selon une partie de la doctrine (cf. Epiney/Schleiss [n. 55], p. 80).

88 Dans une affaire relative à l'art. 8 CEDH précisément, cf. TF, arrêt 2C_828/2011 du 12.10.2012, c. 5.2 et 5.3 (destiné à publication).

89 Art. 2 I du Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données (RS 0.235.11).

90 Art. 25 I de la Directive 95/46/CE 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.

91 Dans ce sens, cf. Rudin (n. 6), p. 420.

92 Art. 18 al. 3 Cst. BE ; art. 5 al. 1er Cst. GL ; art. 12 al. 2 Cst. FR ; art. 8 al. 2 Cst. SO ; art. 6 al. 2 let. g Cst. BL ; art. art. 2 let. g Cst. SG ; art. 15 al. 2 Cst. AG ; art. 8 al. 2 let. d Cst. TI ; art. 15 al. 2 Cst. VD ; art. 11 al. 2 et 3 Cst. NE ; art. 21 al. 2 Cst. GE.

93 Art. 11 al. 1er let. j Cst. BS : « droit à la protection des données personnelles » ; art. 15 al. 1er Cst. AR : « droit à ce que ses données personnelles soient protégées ».

94 Art. 18 al. 1er Cst. BE ; art. 11 al. 1er let. j Cst. BS ; art. 15 al. 2 Cst. AR ; art. 8 al. 2 let. d Cst. TI ; art. 15 al. 2 Cst. VD ; art. 11 al. 2 Cst. NE.

inexactes[95] et de la destruction des données inadéquates ou inutiles[96].

4.3. Une consécration jurisprudentielle progressive

Le cheminement du Tribunal fédéral vers la reconnaissance de ce droit a été progressif. Les deux premiers arrêts que la doctrine a coutume de citer pour fonder la création jurisprudentielle datent de 1987[97], sans mention explicite pourtant. Dans la première affaire, le Tribunal fédéral a reconnu l'intérêt d'une personne, soumise à un contrôle d'identité alors qu'elle se trouvait sur un lieu connu pour être un point de rencontre homosexuel, à pouvoir consulter dans les dossiers de police les inscriptions qui la concernaient en dehors d'une procédure pendante. La cour a déduit cet intérêt « du rapport étroit existant entre les inscriptions opérées et l'exercice de la liberté personnelle, ainsi que de la nécessité de pouvoir demander, au besoin, la rectification de ces inscriptions. »[98] Pour étayer son argumentation, elle évoque à la fin de son raisonnement, brièvement et sans développement, l'arrêt de la Cour constitutionnelle allemande sur le recensement de la population, sans toutefois nommer le droit déduit par le juge germanique :

> « Diesen Gedanken hat denn auch das Bundesverfassungsgericht in seinem sog. Zensus-Urteil angesichts der modernen Datenbearbeitungsmöglichkeiten unterstrichen (BVerfGE 65 Nr. 1 S. 41 ff. E. 1a [...]). »[99]

Dans le second arrêt de 1987, le Tribunal fédéral a jugé inconstitutionnelle une disposition législative genevoise qui interdisait à quiconque de prendre connaissance d'un dossier de police le concernant. Il ne mentionne pas non plus explicitement le droit à l'autodétermination, mais se limite à évoquer la reconnaissance du principe d'accès à ses données dans « la plupart des législations des pays occidentaux » et à énoncer la prédiction – prémonitoire – de la croissance de son rôle dans le futur en raison de l'informatisation qui permet la diffusion immédiate des informations :

> « Indépendamment des règles régissant le droit de consulter un dossier formellement constitué, le droit constitutionnel confère donc à la personne concernée le droit d'être renseignée, d'une part, sur les données qui ont été enregistrées à son sujet par une autorité publique et, d'autre part, sur l'usage qui en a été fait. Ce droit aux renseignements est du reste reconnu, dans son principe, par la plupart des législations des pays occidentaux [...]. Il est appelé à jouer un rôle de plus en plus important pour la protection de l'individu, car le traitement informatique des données en permet la diffusion et le traitement immédiats à tous les échelons de l'administration publique »[100].

En 1990, le Tribunal fédéral, dans une formule définissant l'essence même du droit l'autodétermination en matière de données personnelles – mais qu'il abandonnera dans les années suivantes en ne la reprenant que dans la jurisprudence récente – est devenu plus explicite. Il a reconnu un droit à toute personne de « pouvoir garder la maîtrise des informations qui la concernent » en se fondant sur une opinion doctrinale en droit privé. A défaut, la conservation de données personnelles, même conforme à la Constitution, porterait atteinte à la liberté personnelle :

> « Jusqu'à présent, le Tribunal fédéral n'a pas eu à examiner si la conservation de renseignements personnels, même recueillis d'une façon conforme à la constitution, peut porter atteinte à la liberté personnelle [...]. Cette question doit être tranchée par l'affirmative car toute personne doit pouvoir garder la maîtrise des informations qui la concernent (PIERRE TERCIER, Le nouveau droit de la personnalité, p. 67 ch. 460). »[101]

L'expression *« informationelles Selbstbestimmungsrecht »* n'apparaît expressément dans la jurisprudence du Tribunal fédéral publiée qu'en 1994 dans une affaire établissant le droit du travailleur de consulter son dossier personnel. Le droit privé ne garantissant pas explicitement ce droit, la Cour s'est référée à la doctrine pour établir que le droit de consultation découlait de la disposition du Code des obligations sur la protection de la personnalité du travailleur (art. 328 CO). Le juge a précisé ensuite, en complément, qu'un tel droit devait être compris comme faisant partie du droit à l'autodétermination en matière de données personnelles, au fondement également de la législation fédérale sur la protection des données :

---

95 Art. 18 al. 1er Cst. BE ; art. 11 al. 1er let. j Cst. BS ; art. 15 al. 2 Cst. AR ; art. 8 al. 2 let. d Cst. TI ; art. 15 al. 2 Cst. VD ; art. 11 al. 2 Cst. NE.

96 Art. 18 al. 1er Cst. BE ; art. 15 al. 2 Cst. VD ; seulement « inutiles » : art. 11 al. 2 Cst. NE.

97 Selon SCHWEIZER (n. 78), N. 39, le droit a été reconnu dès 1987 comme droit constitutionnel non écrit. Il se réfère aux ATF 113 Ia 5 ; Ia 262 ; ATF 120 II 121 ; ATF 122 I 162 ; ATF 128 II 268 ; ATF 133 I 77.

98 ATF 113 Ia 1, 5 (citation extraite du chapeau).

99 ATF 113 Ia 1, 6. L'arrêt est également utilisé une seconde fois plus loin (p. 11).

100 ATF 113 Ia 257, 264 s.

101 SJ 1990 561, 563, TF. Le principe a été repris par l'Office fédéral de la justice dans un avis de droit fixant les conditions de licéité de la vidéosurveillance dans un garage souterrain sous l'angle du droit privé : « Le fait de photographier un conducteur à l'entrée d'un parking et de filmer le numéro de la plaque d'immatriculation et la marque de la voiture, ainsi que de conserver ces informations un certain temps constitue une atteinte à la personnalité du conducteur, voire du détenteur du véhicule : ‹ Toute personne doit pouvoir garder la maîtrise des informations qui la concernent › » (JAAC 1992 N° 20 164, 167).

« Das Einsichtsrecht ist als Teil des informationellen Selbstbestimmungsrechtes zu verstehen [...], das auch der Datenschutzgesetzgebung des Bundes zugrundeliegt »[102].

Le Tribunal fédéral a repris en 1996 la même formule, mais dans le cadre d'un rapport de droit public[103].

En 1998, il a fait une allusion indirecte au droit à l'autodétermination pour y poser des limites. Il a recouru à une expression utilisée par la Cour constitutionnelle allemande dans son arrêt sur le recensement de la population, sans toutefois s'y référer explicitement. On se rappelle que celle-ci avait souligné dans son raisonnement qu'un droit à l'autodétermination permettrait de prévenir l'avènement d'une société dans laquelle les citoyens ne pourraient plus savoir qui connaît quoi sur eux, à quel moment et dans quelle circonstance[104]. Dans cette nouvelle affaire où un contribuable critiquait le fait qu'on lui refusait le droit de connaître l'identité des personnes qui demandaient la délivrance d'une attestation fiscale le concernant, le Tribunal fédéral a jugé que nul ne disposait d'un droit constitutionnel à être informé lorsqu'un tiers consulte ses données personnelles contenues dans des registres et déclarées publiques par la loi (qu'il s'agisse d'un registre fiscal cantonal, du registre foncier ou du registre du commerce). Une telle prétention conduirait sinon à accorder un « droit général de connaître en tout temps qui sait quoi sur soi ». Un tel droit, poursuivait-il, serait « difficilement applicable – du moins exprimé de manière si générale – et conduirait en fin de compte à bloquer toute communication » :

« Ein solcher Anspruch würde auf ein generelles Recht eines jeden hinauslaufen, jederzeit zu wissen, wer was über ihn weiss. Ein solches ‹ Recht › wäre jedenfalls in dieser allgemeinen Form kaum praktikabel und könnte im Ergebnis jegliche Kommunikation zum Erliegen bringen »[105].

Dans cet arrêt, le Tribunal signifie simplement qu'il fixe des limites au droit à l'autodétermination afin de prévenir des conséquences indésirables. La précision du Tribunal fédéral est d'autant plus légitime que la Cour de Karlsruhe a elle-même précisé dans son arrêt fondateur que ce droit ne conférait pas une maîtrise absolue et illimitée sur ses données, précisément pour tenir compte des nécessités de communiquer[106]. L'arrêt lausannois ne saurait donc être compris comme le refus de reconnaître un tel droit, et encore moins comme une incohérence jurisprudentielle[107].

En 2001, il a évoqué ce droit sans se prononcer sur la nature constitutionnelle de celui-ci. Il a simplement relevé qu'il s'agissait d'« un droit, privé, à l'autodétermination en matière de données personnelles concrétisé dans la loi fédérale sur la protection des données »[108].

Sous l'empire de la nouvelle Constitution fédérale, le Tribunal fédéral a énoncé en 2002 la nature et la source du principe en droit constitutionnel. Le droit à l'autodétermination en matière de données personnelles se déduira dorénavant de l'article 13 II Cst., en tant que partie du droit à la protection de la sphère privée, et non plus de la liberté personnelle (art. 10 II Cst.) :

« Während Art. 10 Abs. 2 BV die verfassungsrechtliche Grundgarantie zum Schutz der Persönlichkeit darstellt [...], schützt Art. 13 Abs. 2 BV den Einzelnen vor Beeinträchtigungen, die durch die staatliche Bearbeitung seiner persönlichen Daten entstehen (Recht auf informationelle Selbstbestimmung). Der verfassungsrechtliche Datenschutz ist Teil des Rechts auf eine Privat- und persönliche Geheimsphäre (Art. 13 Abs. 1 BV). »[109]

Le chapeau de cet arrêt qualifie par ailleurs entre parenthèse le droit à la protection contre l'emploi abusif de données personnelles de « informationelles Selbstbestimmungsrecht », y compris d'ailleurs dans la version française : « Atteinte [...] au droit à la protection contre l'emploi abusif de données personnelles (‹ informationelles Selbstbestimmungsrecht › ; art. 13 al. 2 Cst.) par un frottis de la muqueuse jugale, respectivement par l'établissement et le traitement d'un profil d'ADN ».

En 2003, il a clairement précisé la source et le contenu de l'article 13 II Cst. Ce dernier garantit un droit à l'autodétermination, conférant à chacun le droit de « pouvoir déterminer lui-même si et dans quel but les informations à son sujet sont traitées » :

« Art. 13 BV [...] Abs. 2 schützt den Einzelnen vor Beeinträchtigungen, die durch die staatliche Bearbeitung seiner persönlichen Daten entstehen (Recht auf informationelle Selbstbestimmung ; [...]). Die einzelne Person soll selbst bestimmen können, ob und zu welchem Zwecke Informationen über sie bearbeitet werden »[110].

---

102 ATF 120 II 118, 121.

103 « Das Einsichtsrecht ist Teil des sog. informationellen Selbstbestimmungsrechts, wie es in der Lehre und der Rechtsprechung anerkannt wird (vgl. BGE 120 II 118 E. 3a S. 121 ; Botschaft zum DSG, BBl 1988 II 417f. ; BVerfGE 65 Nr. 1 S. 41 E. 1a = EuGRZ 1993 S. 577 [588]) » (ATF 122 I 153, 162).

104 Cf. ci-dessus ch. 3.2.

105 ATF 124 I 176, 183.

106 Cf. ci-dessous ch. 6.1.

107 Dans ce sens pourtant, cf. GÄCHTER/EGLI (n. 58), N. 29.

108 « Die gegen seinen Willen veröffentlichte Fotografie stellt deshalb eine Verletzung seines im allgemeinen Persönlichkeitsrecht (Art. 28 Abs. 1 ZGB) gründenden Rechtes am eigenen Bild sowie seines privatrechtlichen, im DSG konkretisierten Rechts auf informationelle Selbstbestimmung dar » (ATF 127 III 481, 494).

109 ATF 128 II 259, 268.

110 ATF 129 I 232, 245. La formulation est reprise, en français, deux ans plus tard dans un arrêt non publié (TF, 2P.165/2004 du 31 mars 2005, c. 7.1) et, cinq ans plus tard, en allemand (TF, arrêt 1D_17/2007 du 2 juillet 2008, c. 4.1).

Le Tribunal fédéral l'a rappelé en 2007 à propos de la durée de conservation de données de vidéosurveillance. Une plus longue durée porte une grande atteinte au droit à l'autodétermination en matière de données personnelles protégé par l'article 13 II Cst. et augmente ainsi le risque d'une utilisation abusive :

> « Vor diesem Hintergrund fällt die Dauer der Aufbewahrung der Aufzeichnungen ins Gewicht : Eine längere Aufbewahrungsdauer stellt bereits per se einen schwerer wiegenden Eingriff in das von Art. 13 Abs. 2 BV geschützte informationelle Selbstbestimmungsrecht dar und erhöht die Gefahr einer missbräuchlichen Verwendung der Videoaufzeichnungen »[111].

En 2012, le Tribunal fédéral a eu l'occasion de préciser le contenu de ce droit, qu'il a qualifié de constitutionnel *(verfassungsmässig geschütztes Recht),* en reprenant l'excellente formulation qu'il avait utilisée en 1990 (maîtrise/*Herrschaft* des données). Dans le domaine de la protection des données, a–t–il jugé, « le droit constitutionnel à l'autodétermination en matière de données personnelles (art. 13 II Cst. et art. 8 I CEDH) garantit à chacun la maîtrise de ses données personnelles, quel que soit en principe le degré de sensibilité effectif des informations concernées » :

> « Im Bereich des Datenschutzes garantiert das verfassungsmässig geschützte Recht auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV und Art. 8 Ziff. 1 der Konvention vom 4. November 1950 zum Schutze der Menschenrechte und Grundfreiheiten [...]), dass grundsätzlich ohne Rücksicht darauf, wie sensibel die fraglichen Informationen tatsächlich sind, dem Einzelnen die Herrschaft über seine personenbezogenen Daten zusteht »[112].

Le Tribunal administratif fédéral a défendu le même avis, dans le sillage de la pratique de la défunte Commission fédérale de la protection des données (et de la transparence)[113].

Les juges fédéraux ont désormais rajouté, avec raison, un fondement au droit à l'autodétermination : celui du droit au respect de la vie privée et familiale tel qu'il découle de l'article 8 I CEDH[114].

5. Les contours du droit à l'autodétermination en matière de données personnelles

Le droit à l'autodétermination en matière de données personnelles est un droit constitutionnel qui garantit à chacun la maîtrise de ses données personnelles[115]. Il trouve son fondement tant à l'article 13 II Cst. qu'à l'article 8 I CEDH[116] et se justifie par le fait que de telles données caractérisent et expriment la personnalité de l'individu[117]. Concrètement, il autorise toute personne à déterminer elle-même si et dans quels buts des informations à son sujet peuvent être traitées[118]. Il permet à celle-ci d'exprimer sa volonté et de consentir ou non à l'emploi de ses données personnelles[119]. A l'exemple des autres droits fonda-

---

111 ATF 133 I 77, 85.

112 ATF 138 II 346, 359 s. Le TF ne discute pourtant pas dans cet arrêt les critiques de la doctrine. Il se réfère aux pages 361 ss de l'ouvrage de BELSER (n. 67), lesquelles évoquent la doctrine dominante, et non l'opinion personnelle, critique, de cet auteur (aux p. 375 ss et 399 ss notamment). L'autre arrêt concernait la sauvegarde de données personnelles dans le système d'information de la police zurichoise et l'opposition d'une personne à une trop longue conservation de ses données : « Gestützt auf das informationelle Selbstbestimmungsrecht (Art. 13 Abs. 2 BV, Art. 8 Ziff. 1 EMRK) kann sich die betroffene Person zur Wehr setzen, dass ihre Personendaten ohne ersichtlichen Grund auf lange Zeit in einem öffentlichen Register gespeichert werden. » (ATF 138 I 256, 262). Dans un troisième arrêt, il décrit l'art. 13 II Cst. sans référence à l'autodétermination (« verfassungsrechtliche Datenschutz »), mais sans discuter ce point non plus (ATF 138 I 331, 337).

113 « Dieses verfassungsmässige Recht auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV und Art. 8 Ziff. 1 EMRK) lässt grundsätzlich ohne Rücksicht darauf, wie sensibel die fraglichen Informationen tatsächlich sind, dem Einzelnen die Herrschaft über seine personenbezogenen Daten zukommen und schützt ihn vor Beeinträchtigungen, die durch die staatliche Bearbeitung seiner persönlichen Daten entstehen. » (ATAF 2012/14, du 10 avril 2012, c. 4.1). Sur un exemple de la pratique de la commission, cf. JAAC 69.106 du 15 avril 2005, c. 2.3.

114 Cf. ci-dessus ch. 3.3. Dans un arrêt non publié récent, le TF ne s'est pourtant référé qu'à l'article 13 II Cst. pour fonder le principe dans une affaire relative à un prélèvement génétique : « Im vorliegenden Fall war die Beschaffung der DNA-Daten an sich nicht rechtswidrig. Namentlich haben die Strafbehörden weder in strafbarer Weise noch unter Verletzung von Gültigkeitsvorschriften gehandelt. Allerdings hätten die DNA-Daten überhaupt nicht mehr existieren dürfen. Der Zugriff darauf verletzte das Recht der Beschwerdeführerin auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV [...]). » (TF, arrêt 6B_299/2012 du 20 septembre 2012).

115 Cette définition est celle donnée par le TF (réf. cit. ci-dessus ch. 4.3 *i.f.*).

116 Réf. cit. ci-dessus ch. 4.3 *i.f.*

117 « Chacun doit pouvoir inconditionnellement maîtriser les données qui le concernent, parce que ces données caractérisent et expriment sa personnalité. » (PAUL-HENRI STEINAUER, « Le droit privé matériel », *in :* Nicolas Gillard [éd.], La nouvelle loi fédérale sur la protection des données, Lausanne 1994, p. 85–112, p. 97).

118 TF, arrêt 2P.165/2004 du 31 mars 2005, c. 7.1. cité ci-dessus ch. 4.3. Cf. ég. les définitions de MEIER (n. 54) et de MÜLLER/SCHEFER (n. 64) qui sont des allusions directes à celle donnée en 1890 déjà en *common law :* « Le droit à l'autodétermination comme le droit pour chaque personne de pouvoir déterminer elle-même si et dans quels buts des informations à son sujet (en particulier sur son comportement, ses opinions, ses sentiments, ses émotions, sa santé et ses habitudes) peuvent être traitées. » (MEIER [n. 54], p. 70 ; cf. ég. MÜLLER/SCHEFER [n. 64], p. 167).

119 Le droit à l'autodétermination informationnelle est « le droit de ne pas accepter un traitement qui ne correspond pas à la volonté exprimée » (MEIER [n. 54], p. 65). Dans le même sens : AEBI-MÜLLER (n. 7), p. 284.

mentaux, il peut être restreint aux conditions classiques de la base légale, de l'intérêt public et de la proportionnalité (art. 36 Cst.). Il ne déploie qu'indirectement des effets entre particuliers (art. 35 III Cst.)[120].

Ce droit fondamental se décline en différents droits spécifiques qui le concrétisent[121] : le droit de connaître l'existence de données personnelles, de les consulter, de faire rectifier des données inexactes ou de faire radier ses propres données[122], le droit de spécifier le but de l'utilisation des données récoltées[123], le droit de s'opposer à leur traitement[124], le droit à la transparence de la collecte (caractère reconnaissable de celle-ci et devoir d'information), le droit de ne pas exporter ses données vers des pays moins protecteurs, le droit à la sécurité des données (protection en cas d'atteinte à l'intégrité des données suite à un traitement illicite ou contraire à sa volonté ainsi qu'en cas de brèche de sécurité [vol ou perte des données], comprenant en plus le droit d'être avisé en pareil cas)[125], le droit à l'anonymat[126], en particulier celui d'aller et venir anonymement[127], le droit à l'oubli[128], le droit d'exiger un cadre et des moyens techniques permettant à chacun d'exercer effectivement des choix éclairés : architecture informatique conçue pour améliorer le pouvoir de contrôle *(privacy enhancing technologies)*, protection intégrée de la vie privée *(privacy by design)*, dépôts de données personnelles *(personal data store)*[129], de même que le droit de disposer librement de ses données à sa mort (droit successoral numérique)[130]. En tant qu'expressions concrètes du droit à l'autodétermination, ces droits revêtent, à mon avis, tous une nature constitutionnelle[131].

Le droit à l'autodétermination ne comprend en revanche pas celui de connaître l'identité des personnes tierces qui consultent les données personnelles de quelqu'un[132]. Il ne saurait non plus conférer de manière générale le droit « d'empêcher les gens de parler de vous »[133].

Enfin, il faut relever que tous les droits et principes applicables à la protection des données personnelles ne découlent pas forcément du droit à l'autodétermination. Les exigences de traitement licite, effectué de bonne foi et proportionné précisées dans la loi ou en droit international

---

120 Cf. ci-dessous ch. 6.5.

121 Cf. par exemple BIAGGINI (n. 76), Art. 13, N. 14, qui qualifie ces droits spécifiques d'« Instrumente zur Wahrung des Datenschutzes ».

122 MEIER (n. 54), p. 71 s. ; BIAGGINI (n. 76), Art. 13, N. 14 ; MAHON (n. 76), N. 16 ; AUER/FLÜCKIGER (n. 76), p. 934 ; MÜLLER/SCHEFER (n. 64), 168 s.

123 SCHWEIZER (n. 78), N. 39.

124 JEAN-PHILIPPE WALTER, « Le droit de l'individu à l'autoprotection lors du traitement de données personnelles dans le domaine des télécommunications », *in :* Bertil Cottier (dir.), Le droit des télécommunications en mutation, Fribourg 2001, p. 459–482, p. 465.

125 MEIER (n. 54), p. 72. Avant de proposer par voie législative un mécanisme obligatoire de signalement des atteintes portées à la protection des données personnelles, le Conseil fédéral a préféré temporiser, se fiant aux travaux en cours au sein du Conseil de l'Europe et de l'UE (Avis du 9.12.2011 sur la motion *Reimann, Renforcer le droit de regard sur ses propres données personnelles,* déposée au Conseil national le 30.9.2011 [11.3990]). Le droit des Etats aux USA comprend déjà une obligation d'annonce (« Data security breach notification statutes » : SOLOVE/SCHWARTZ [n. 44], p. 135 ss). Une partie de la doctrine estime que le TF devrait compléter le principe de l'autodétermination par un nouveau droit constitutionnel non écrit à l'intégrité des systèmes digitaux sur le modèle du droit allemand (« Integritât digitaler Systeme, d.h. ein [...] Schutz [...] der digitalen Kognition ») (WEBER [n. 71], p. 27).

126 MEIER (n. 54), p. 72 ; BEAT RUDIN, « Das Recht auf Anonymität, Anonymität als Teil der informationellen Selbstbestimmung : wenig geregelte Anwendungsfälle und viel Handlungsbedarf », *Digma* 2008, p. 6–13.

127 Sur ce droit en rapport à la vidéosurveillance, cf. AUER/FLÜCKIGER (n. 76), p. 932.

128 Cf. DIRK LANGER, « Le droit à l'oubli à l'épreuve d'Internet », *Jusletter* 12 mars 2012, pour une comparaison entre les droits suisses, allemand, français, américain et européen ; FRANZ WERRO, « The Right to Inform v. the Right to be Forgotten : A Transatlantic Clash », *in :* Aurelia Colombi Ciacchi/Christine Godt/Peter Rott/Leslie Jane Smith (éd.), Haftungsrecht im Dritten Millennium = Liability in the Third Millennium : Liber amicorum Gert Brüggemeier, Baden-Baden 2009, p. 285–300, pour une comparaison entre le droit suisse et américain. Cf. ég. ROBERT KIRK WALKER, « The Right to Be Forgotten », *Hastings Law Journal* 2012, vol. 64, p. 257–286, p. 257 ss ; ROLF H. WEBER, « Der Ruf nach einem Recht auf Vergessen : ein neues datenschutzbezogenes Verfassungsrecht im Spannungsfeld zwischen Privatheit und Transparenz ? », *Digma* 2011, p. 102–105, p. 102 ss.

129 LAWRENCE LESSIG, L'inspirateur de ces outils, définit ceux-ci en rapport précisément avec le pouvoir de contrôle qu'ils sont censés conférer : « Architecture/Code : Technology could be used to protect privacy. Such technologies are often referred to as ‹ Privacy Enhancing Technologies. › These are technologies designed to give the user more technical control over data associated with him or her. » (LESSIG [n. 26], p. 223 ; cf. ég. p. 38 ss et p. 226 s.). Cf. ég. BRUNNER (n. 10), N. 41 ss. Sur la protection intégrée de la vie privée *(privacy by design)*, cf. COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ONTARIO, Protection intégrée de la vie privée : les sept principes fondamentaux, Toronto 2009. Sur les dépôts de données personnelles, cf. ci-dessous ch. 6.6.

130 Sur cette question, cf. ci-dessous ch. 6.6 note 213.

131 La doctrine et la jurisprudence s'accordent à considérer que tel est au minimum le cas pour les droits de consultation, de rectification et de radiation (BIAGGINI [n. 76], Art. 13, N. 13). Ces droits sont parfois explicitement constitutionnels en droit cantonal, cf. ci-dessus ch. 4.2 *i.f.* Ils ont en outre été déduits de l'article 8 CEDH (cf. par exemple MEIER [n. 54], p. 72).

132 ATF 124 I 176, 183 cit. ci-dessus ch. 4.3 note 106.

133 Pour une telle lecture du *right to information privacy* états-unien, dans le cadre d'une critique du point de vue de la liberté d'expression, cf. VOLOKH (n. 47), p. 1049 : a « Right to Stop People From Speaking About You ».

(art. 4 I et II LPD ; art. 5 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[134]), découlent des principes constitutionnels généraux correspondants (art. 5 Cst. notamment).

6. Les critiques

Le droit à l'autodétermination en matière de données personnelles a été critiqué pour diverses raisons que j'ai regroupées en six catégories, et auxquelles je tenterai de répondre. Si ces critiques ont motivé certains auteurs à suggérer des adaptations ou des mesures pour pallier les défauts du droit à l'autodétermination[135], elles ont conduit d'autres à plaider carrément pour son abandon[136].

6.1. Une mise en danger des libertés de communication

L'échange social implique d'échanger constamment des informations sur autrui, que ce dernier le veuille ou non. Il paraît légitime dans une démocratie de maintenir un flux d'information équilibré entre les individus. Dès lors, selon certains, « prise à la lettre, [une conception purement subjective du ‹ droit à l'autodétermination en matière de données personnelles ›] conduirait à bloquer tout processus de communication »[137]. Elle conduirait également à un « égoïsme des données personnelles » *(« Datenegoismus »)*[138]. Cette absence de partage, cette communication à sens unique, conduirait à privilégier indûment ceux qui savent sur ceux qui ignorent :

> « Das Recht auf informationelle Selbstbestimmung führt deshalb, pointiert formuliert, zu einer ‹ rein faktisch begründete[n] Privilegierung des Wissenden vor dem Nichtwissenden im Entscheid über die Informationsverteilung. › »[139].

Ni en Europe, ni en Suisse en particulier, il n'a jamais été question de concevoir ce droit de manière absolue, encore moins de le « prendre à la lettre » puisque, à l'instar de tout autre droit fondamental, il est susceptibles d'être restreint ou mis en balance avec d'autres. Les libertés de communication, en particulier le droit de recevoir librement des informations, de se les procurer et de les diffuser (art. 16 Cst.) et la liberté des médias (art. 17 Cst.) forment les contrepoids principaux. Le droit à l'autodétermination n'a pas pour vocation d'empêcher l'échange communicationnel. La Cour constitutionnelle allemande l'a d'ailleurs reconnu elle-même dans son arrêt fondateur :

> « Dieses Recht auf ‹ informationelle Selbstbestimmung › ist nicht schrankenlos gewährleistet. Der Einzelne hat nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über ‹ seine › Daten ; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Information, auch soweit sie personenbezogen ist, stellt ein Abbild sozialer Realität dar, das nicht ausschliesslich dem Betroffenen allein zugeordnet werden kann. »[140]

On retrouve dans cette critique un parallèle frappant avec l'ancestral débat sur la garantie de la propriété : faut-il mettre en commun et partager de manière égalitaire les ressources (ici informationnelles) comme le proposent les théories sociales de la propriété privée ? Faut-il permettre à autrui de savoir tout sur soi, avec pour corollaire de s'autoriser à savoir tout sur autrui ? Les données personnelles constituent-elles un bien commun à libre disposition de tout un chacun ?

Il est indubitable que nombre de personnes veulent être en mesure d'épier leurs voisins, de suivre le parcours de leurs amis et connaissances, de consulter leur déclaration d'impôt, de comparer leur salaire, de suivre leur vie amoureuse, de vérifier la solvabilité de leurs co-contractants, de surveiller leur propriété, de connaître la réputation d'un commerçant, d'un professeur ou d'un médecin, de surveiller leurs enfants ou de connaître le profil de personnalité de leurs locataires ou de leurs employés. La demande sociale en ce sens est forte, et parfois même contradictoire si celui qui veut s'informer sur son voisin désire simultanément protéger ses propres données personnelles.

Tirant un parallèle avec le vendeur qui veut cacher les défauts de son produit, les défenseurs d'une société hyper-transparente estiment que la protection de la vie privée reviendrait à conférer aux individus « plus de pouvoirs pour cacher des informations sur eux-mêmes que d'autres pourraient utiliser à leur détriment », empêchant fâcheusement les gens de se faire une opinion éclairée sur leurs congénères :

---

134 RS 0.235.1.

135 Brunner (n. 10), N. 36, 51 et ch. VI ; Aebi-Müller (n. 7), p. 286 ; Beat Rudin, « Kollektives Gedächtnis und informationelle Integrität : Zum Datenschutz im öffentlichen Archivwesen », *PJA/AJP* 1998, p. 247–260, p. 248 s.

136 Belser (n. 67), p. 399 ss ; Gächter/Egli (n. 58), N. 24 ss et 36 ss.

137 Mahon (n. 69), p. 36. Dans le même sens, Rudin (n. 135), p. 248 ; Aebi-Müller (n. 7), p. 290. Sur cet argument en cas d'extension trop grande du droit à l'autodétermination, cf. ATF 124 I 176, 183 ci-dessus note 133.

138 Aebi-Müller (n. 7), p. 287, note 1564 (réf. cit.).

139 Aebi-Müller (n. 7), p. 289.

140 BVerfG 65, 1.

> « when people today decry lack of privacy, what they want, I think, is mainly something quite different from seclusion : they want more power to conceal information about themselves that others might use to their disadvantage. »[141] « We would think it wrong (and inefficient) if the law permitted a seller in hawking his wares to make false or incomplete representations of their quality. But people ‹ sell › themselves as well as their goods by professing high standards of behavior to induce others to engage in advantageous social or business dealings with them, while concealing facts that these acquaintances need in order to evaluate their character. »[142]

Ces derniers recourraient égoïstement à la protection de la vie privée « pour effectuer des transactions avantageuses tant sur le marché de l'emploi que celui du mariage et, plus généralement, sur le marché des relations humaines, qu'il s'agisse du plan personnel ou commercial. »[143]

Il est vrai que la disparition progressive des barrières de fait protégeant les données relatives aux personnes depuis un siècle a coïncidé avec une extension généralisée de la transparence, non seulement dans les Etats de droit moderne[144] mais aussi dans les pratiques individuelles, recomposant la notion même de vie privée.

Une importance plus grande donnée par l'ordre juridique à l'un de ces pôles aura pour conséquence de réduire proportionnellement celle de l'autre, puisque le conflit entre droits fondamentaux se résout par des pesées d'intérêt[145]. Cette caractéristique explique pourquoi les pratiques en matière de protection des données et de transparence peuvent être si différentes d'un endroit à l'autre, malgré des principes fondamentaux relativement semblables. Les Etats-Unis par exemple attachent depuis le 11 septembre 2001 une importance à la sécurité publique telle qu'elle justifie une surveillance généralisée de la population au détriment de la protection de la *privacy* de chacun[146]. Dans le registre des relations entre particuliers, le même phénomène peut être observé en relation avec la liberté d'expression (garantie du *free speech)* découlant du premier amendement de la Constitution[147], ouvrant le débat entre ceux qui estiment que les règles en matière de protection de la sphère privée ne sont pas vraiment défendables par rapport à la liberté d'expression[148] et ceux qui pensent que la protection des données est une partie intégrante de la liberté d'expression, et non pas l'ennemi de cette dernière[149].

La question revient à savoir si la liberté d'information confère un droit à s'informer *sur autrui*. La problématique est évidemment centrale : si j'ai un droit d'être informé sur les données personnelles d'autrui, je porte atteinte au droit d'autrui à déterminer librement la diffusion de ses propres données si ce dernier refuse de me les communiquer. La pratique ne va pas si loin en Europe et en Suisse en particulier. Le droit d'accéder aux documents officiels est par exemple limité en droit fédéral s'il porte atteinte à la sphère privée de tiers, à moins qu'un intérêt public à la transparence ne soit exceptionnellement jugé prépondérant (art. 7 II LTrans). Le principe de transparence vise en Suisse à éclairer les activités administratives et non pas à dévêtir le citoyen, alors qu'aux Etats-Unis, la loi sur la liberté de l'information *(Freedom of Information Act)* semble être mieux conçue pour divulguer des informations sur les personnes communiquant avec le gouvernement que pour révéler la conduite de ce dernier[150]. Un autre exemple d'information sur autrui est celui des plateformes d'évaluation en ligne des médecins ou des enseignants, populaires aux USA, mais très limitées en Suisse[151].

---

141 RICHARD A. POSNER, The Economics of Justice, Cambridge Mass. 1981, p. 271, tel que cité par SOLOVE (n. 8), p. 1032.

142 POSNER (n. 141), p. 233, tel que cité par SOLOVE (n. 8), p. 1033.

143 « A person constructs a public self to display to the world, and then sells this self by ‹ using it to make advantageous transactions in employment and marriage markets and, more generally, in the market for human relationships whether of a personal or of a commercial character. › » (RICHARD A. POSNER, Overcoming Law, Cambridge Mass. 1995, p. 532, tel que cité par SOLOVE [n. 8], p. 1032).

144 Sur l'extension de ce principe en droit suisse, cf. MOOR/FLÜCKIGER/MARTENET (n. 76), p. 942 ss.

145 Sur l'équilibre à trouver entre la protection des données et le principe de transparence, cf. STEPHAN BRUNNER/ALEXANDRE FLÜCKIGER, « Nochmals : der Zugang zu amtlichen Dokumenten, die Personendaten enthalten », *Jusletter* 4 octobre 2010 ; ALEXANDRE FLÜCKIGER, « Le conflit entre le principe de transparence et la protection de la sphère privée », *Medialex* 2003, p. 225–233, p. 225 ; ALEXANDRE FLÜCKIGER, « Quand la transparence de l'administration conduit à celle des citoyens : la divulgation de données personnelles dans les informations étatiques en droit américain et suisse », à paraître).

146 Critique sur l'importance trop grande conférée aux arguments sécuritaires qui limitent la *privacy* en droit états-unien, cf. SOLOVE (n. 6).

147 VOLOKH (n. 47).

148 « Information privacy rules are not easily defensible under existing free speech law. » (VOLOKH [n. 47], abstract).

149 Pour PAUL M. SCHWARTZ, « Free Speech vs. Information Privacy : Eugene Volokh's First Amendment Jurisprudence », *Stanford Law Review* 2000, vol. 52, p. 1559–1572, p. 1572, au contraire l'« information privacy law is an integral element of the mission of free speech and not its enemy. ».

150 CHARLES H. KOCH, Administrative Law and Practice, 3ème éd., Eagan, Minn. 2010, p. 501 ; pour des exemples très illustratifs, cf. FLÜCKIGER (n. 145) (à paraître).

151 Cf. PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE, Les plateformes d'évaluation en ligne, Berne 18 mars 2009 (www.edoeb.admin.ch – rubrique Thèmes> Protection des données> Internet).

6.2. Une importation décontextualisée d'une institution étrangère en droit suisse

Certains critiquent le droit à l'autodétermination informationnelle au motif que celui-ci aurait été importé d'Allemagne par la doctrine et la jurisprudence helvétiques sans prise en compte des spécificités juridiques nationales. La liberté personnelle en droit allemand garantirait une liberté d'action générale (« allgemeine Handlungsfreiheit ») alors qu'elle se limiterait aux « manifestations élémentaires de la personne humaine nécessaire à son épanouissement »[152] en droit suisse[153].

A cela on peut répondre, d'une part, que le droit étranger reste une simple source d'inspiration tant pour le juge que pour le législateur ; libre à ces derniers de conférer un sens spécifique. D'autre part, certes, la protection des données personnelles relève en fin de compte de la liberté personnelle reposant elle-même sur la dignité humaine ; le constituant l'a cependant érigée en une disposition spécifique pour tenir compte des particularités du contexte technologique modifiant fondamentalement l'étendue et l'intensité de l'atteinte à la liberté personnelle. Que le Tribunal fédéral et la doctrine majoritaire veuillent accorder plus d'autonomie à l'individu dans ce domaine précisément, plutôt que dans celui de la liberté personnelle en général, ne fait qu'exprimer des besoins différents résultant d'un contexte spécifique.

6.3. L'absence de contenu substantiel du droit à l'autodétermination

Le droit à l'autodétermination informationnelle est également critiqué au motif qu'il serait sans contour et qu'il n'offrirait dès lors aucune limite intrinsèque[154]. Il serait substantiellement neutre :

> « The privacy self-management model attempts to be neutral about substance – whether certain forms of collecting, using, or disclosing of personal data are good or bad – and instead focuses on whether people consent to the collection, use, or disclosure of their data. Consent legitimizes nearly any form of collection, use, and disclosure of personal data. »[155]

Le constat est pertinent. La liberté octroyée à la personne par le droit à l'autodétermination a pour effet d'atomiser les contours de ce que chacun considère comme sa sphère privée, et de ce qu'il juge conforme à sa propre intégrité personnelle ou à sa dignité. L'autodétermination n'offre en effet aucun standard pour juger des informations qui devraient ou non transparaître d'une personne. De telles règles devraient être trouvées ailleurs, en particulier dans une nouvelle composante de la liberté personnelle – l'intégrité informationnelle *(« informationelle Integrität »)*[156] – qui viendrait compléter l'intégrité physique et psychique dans la protection de la sphère privée ou, plus généralement, dans la garantie de la dignité humaine[157].

Est-ce un motif suffisant pour déconstitutionnaliser le droit à l'autodétermination ? Certainement pas à mon avis dans la mesure où, d'une part, ériger en droit fondamental la liberté de décider du sort de ses données personnelles demeure une prérogative essentielle de l'expression de sa liberté personnelle dans le monde numérique moderne. D'autre part, l'absence de limites intrinsèques au droit à l'autodétermination ne signifie pas l'absence de limites extrinsèques (en particulier celles découlant de l'article 36 Cst.), diminuant l'enjeu pratique de la controverse.

6.4. L'appellation trompeuse du droit à l'autodétermination

L'appellation du droit à l'autodétermination en matière de données personnelles serait trompeuse, car elle évoquerait la fausse impression que son détenteur disposerait d'un véritable monopole sur ses données *(« ein eigentliches Verfügungsmonopol über seine eigenen Daten »*[158] ; *« ein umfassendes Verfügungsrecht »*[159]) et qu'il serait absolu[160]. L'expression pourrait induire le « citoyen-consommateur en erreur sur l'étendue de sa protection (qui n'est pas absolue et qui ne dépend pas uniquement de sa volonté) »[161]. Or le droit à l'autodétermination peut être restreint à l'instar des autres droits fondamentaux aux conditions classiques de la base légale, de l'intérêt public et de la proportionnalité en vertu de l'article 36 Cst[162]. La Cour allemande l'a elle-même expliqué[163].

---

152 ATF 133 I 110 (120).

153 Cf. Aebi-Müller (n. 7), p. 287 et réf. cit. ; Gächter/Egli (n. 58), N. 24 ; Belser (n. 67), p. 377.

154 Aebi-Müller (n. 7), p. 288 ; Rudin (n. 135), p. 249 qui préfère pour cette raison une autre appellation : intégrité informationnelle ; Gächter/Egli (n. 58), N. 28.

155 Daniel J. Solove, « Privacy Self-Management and the Consent Paradox », à paraître, *in : Harvard Law Review* 2013, vol. 126, p. 2.

156 Rudin (n. 135), p. 248 s. ; Meier (n. 54), p. 67. Critique sur la formulation proposée par Rudin : Aebi-Müller (n. 7), p. 288.

157 Cf. Rudin (n. 135).

158 Belser (n. 67), p. 377. Cf. ég. Rudin (n. 135).

159 Belser (n. 67), p. 400.

160 Rudin (n. 135), p. 248 s.

161 Meier (n. 54), p. 67.

162 Kiener/Kälin (n. 76), p. 159 ; Biaggini (n. 76), Art. 13, N. 15 ; Müller/Schefer (n. 64), p. 170 ss ; Meier (n. 54), p. 67.

163 « Der Einzelne hat nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über ‹ seine › Daten » (cité ci-dessus ch. 6.1).

La formule allemande *(« Recht auf ‹ informationelle Selbstbestimmung › »)* est frappante en effet. Elle possède la force de la clarté conceptuelle ; celle qui permet d'amorcer un débat franc. Elle n'est pas trompeuse à mon sens puisque le droit à l'autodétermination s'inscrit dans la logique classique des droits fondamentaux susceptibles de restriction. Changer de formule uniquement parce qu'elle « laisserait croire » que le droit ne peut être restreint n'est à mon avis pas suffisamment convaincant. D'autres droits fondamentaux pourraient aussi être débaptisés si l'on suivait le raisonnement, puisque l'intitulé libertaire de ceux-ci, clair et concis, est tout autant susceptible de porter à confusion pour un lecteur ingénu.

La notion suggérée de protection de l'intégrité informationnelle, que j'ai exposée dans la section précédente, est en soi excellente et, même, probablement plus précise que celle de protection des données ou de la sphère privée. Elle élude pourtant la question, centrale, de la maîtrise des données. L'intégrité des données personnelle peut en effet, conceptuellement, être assurée par d'autres moyens que par l'octroi d'un droit de contrôle sur ses données. En érigeant le droit à l'autodétermination sur le plan constitutionnel, le constituant veut signifier l'importance symbolique et juridique de la liberté de choisir, qu'il faut comprendre comme moyen essentiel de garantir l'intégrité informationnelle de la personne.

La formule allemande reste toutefois critiquable sous certains aspects. Peut-être un peu pédante, elle se réfère à la notion plus volatile d'information. L'expression d'autodétermination « en matière de données personnelles » me semble à cet égard préférable.

6.5. Un utopique consentement libre et éclairé

Un nombre croissant de personnes souhaitent partager leurs données pour se dévoiler au plus grand public, d'autres veulent être profilées le plus nettement possible pour devenir la cible de marketing le plus précisément ajusté ou pour rencontrer des amis partageant les mêmes goûts, à défaut d'âme-sœur. Certains applaudissent à l'idée de voir leur visage automatiquement reconnu sur la toile, d'autres exigent de marcher ou de courir le marathon dans des rues vidéo-protégées, de passer des portiques de sécurité et même des scanners corporels afin de se sentir plus en sécurité ou de pouvoir être localisés en tout temps afin de ne pas se perdre. Plus prosaïquement, nombre d'entre nous sommes simplement heureux de nous affranchir de disques durs instables et fastidieux pour accéder en tout temps à nos diverses données depuis des terminaux de plus en plus variés, ainsi que de partager plus rapidement et simplement des informations au sein d'un groupe restreint d'amis ou pour diffuser des photos de famille dans un cercle familial toujours plus éclaté géographiquement.

On ne saurait y voir de difficulté tant que le droit à déterminer librement le sort de nos données personnelles est exercé de manière libre et éclairée[164].

Or le consentement au traitement des données, au cœur du droit à l'autodétermination, peut de moins en moins être donné dans ces conditions idéales[165]. Lorsque le consentement est demandé, il n'existe, dans les faits, pas forcément d'alternative crédible. Le choix est souvent contraint. Certains services détiennent de véritables monopoles en imposant des conditions générales ne laissant aucune marge de choix. Les moyens techniques permettant de contrôler les degrés de traitement et de diffusion des données sur les services du web sont compliqués, pas toujours compréhensibles, longs à mettre en œuvre et pas nécessairement fiables. La personne n'est souvent pas consciente des risques encourus à diffuser des informations, a priori anodines, mais qui, agrégées, permettent d'établir de véritables profils de personnalité pouvant être commercialisés et rediffusés à diverses fins ; et celle qui en est consciente est souvent tentée de tolérer des mini-violations de son droit à l'autodétermination, par lassitude, par gain de paix ou de temps, car les atteintes, prises individuellement, paraissent à court terme plus déplaisantes que réellement intolérables. Enfin, les offreurs de services n'hésitent plus à recourir à des techniques de manipulation mises au point par la psychologie sociale, auxquelles les juristes feraient d'ailleurs bien de s'intéresser de plus près[166].

Une réponse classique des législateurs a été de renforcer les exigences relatives au consentement dans le but de s'assurer que celui-ci soit donné de manière véritablement libre et en toute connaissance de cause[167]. Or même les personnes les plus informées n'ont soit plus envie, ne sont soit en pratique plus en mesure de gérer

---

164 Le consentement au traitement des données doit être fondamentalement libre et éclairé (art. 4 V LPD ; ATF 138 I 331, 339 et 343 s.).

165 Sur cette problématique, SOLOVE (n. 155), p. 4 ss ; BRUNNER (n. 10), N. 35.

166 Dans ce sens, cf. SOLOVE (n. 155). Sur l'admissibilité de l'utilisation de ces techniques en droit public en rapport avec l'usage de la *soft law,* cf. ALEXANDRE FLÜCKIGER, « Pourquoi respectons-nous la soft law ? Le rôle des émotions et des techniques de manipulation », *Revue européenne des sciences sociales* 2009, Tome XLVII, N° 144, p. 73–103, p. 76 ss.

167 Cf. par exemple la dernière révision de la LPD en Suisse (cf. FF 2012 255, p. 264). En droit américain, SOLOVE (n. 155), p. 2, dresse le même constat.

convenablement les paramètres de protection de leur vie privée dans la masse des informations personnelles générées dans l'univers numérique. Multiplier par exemple les exigences d'approbation explicite (système de l'*opt in)* – une expression typique de l'autodétermination informationnelle – serait dans ces conditions une fausse bonne idée. Les entreprises trouveront toujours des moyens pour générer des taux élevés de consentement, par exemple en conditionnant simplement l'accès à leurs produits ou leurs services à une série d'*opt in* successifs[168]. Gérer les multiples réglages des applications dans toutes leurs finesses est un exercice fastidieux décourageant les meilleures volontés. Au même titre que le conducteur d'une voiture s'attend à ce qu'il n'ait pas à régler lui-même tous les mécanismes de sécurité de son véhicule, nombre d'entre nous souhaitent que les dispositifs soient conçus et paramétrés d'office de manière à assurer un niveau minimum de protection :

> « many people do not want to micromanage their privacy. They want to know that someone is looking out for their privacy and that they will be protected from harmful uses. With the food we eat and the cars we drive, we trust that there will be a general level of safety. [...] We trust that certain basic features will be available and that these products will fall within certain reasonable parameters of safety. We do not have to become experts on cars or milk. »[169]

Poursuivre le renforcement des exigences en matière de consentement ne conduirait pas nécessairement dans ces circonstances à améliorer le pouvoir de contrôle :

> « Although the privacy self-management model is certainly a laudable and necessary component of any regulatory regime, I contend that it is being asked to do work beyond its capabilities. Despite its goal is to provide people with control over their personal data, privacy self-management does not provide meaningful control. [...] More troubling, I will argue, is that even well-informed and rational individuals cannot appropriately self-manage their privacy. »[170]

L'exemple des services de messagerie gratuits qui, pour cibler leurs publicités, scannent le contenu de l'ensemble de la correspondance, y compris celle reçue, montre la difficulté. L'internaute est libre certes de passer à un service concurrent, tant que celui-ci existe et offre une qualité de service égale[171], mais la démarche découragera ceux qui n'ont pas envie de rapatrier l'ensemble de leurs messages, de reconfigurer laborieusement un compte et d'informer tous leurs correspondants de leur changement d'adresse. Et quelle est la liberté du correspondant, même informé ? Doit-il refuser de répondre à un ami ou un client qui utilise une telle adresse de messagerie ?

La réponse résiderait-elle alors dans la suppression du droit à l'autodétermination et, partant, de la nécessité de consentir ? Une partie, minoritaire, de la doctrine le préconise. L'admissibilité du traitement des données ne serait plus jugée selon la volonté de la personne concernée mais suivant des exigences indépendantes, telles que l'exactitude ou la transparence du traitement :

> « Da wir die strukturellen Anforderungen an staatliches Handeln nicht über ein ‹ Recht auf informationelle Selbstbestimmung › konstruieren, verliert die ‹ Einwilligung › ihren zentralen Stellenwert. Die Zulässigkeit staatlicher Datenbearbeitung richtet sich grundsätzlich *nicht* nach dem Willen des Betroffenen. Massgeblich ist stets, ob der staatliche Umgang mit Personendaten sachgerecht und transparent erfolgt. »[172]

En réalité, le problème que pose la difficulté d'exprimer librement et de manière éclairée sa volonté n'est pas spécifique à la protection des données : il est sous-jacent à l'ensemble du droit privé. Une telle conception, plus paternaliste, de la protection des données ne poserait guère de difficulté en pratique dans le domaine du droit public où celui-ci a de toute manière une portée plus réduite[173]. On pourrait tout au plus disserter sur le paradoxe consistant à devoir supprimer la liberté de choix pour garantir un élément de la liberté personnelle :

> « In response to people's inability to exercise meaningful consent regarding privacy, paternalistic regulation might limit people's freedom to choose in the name of enhancing their autonomy »[174] « But privacy paternalism creates a paradox. In order to give people the ability to develop their selfhood the law must override their choices. »[175]

Mais le droit constitutionnel à l'autodétermination déploie des effets également entre les particuliers, indirectement certes, en vertu de l'article 35 III Cst., et non seulement envers les collectivités publiques[176]. L'impact d'un

---

168 SOLOVE (n. 155), ch. 6, autrefois « optimiste » sur les possibilités de ce mécanisme pour améliorer la protection des données.

169 SOLOVE (n. 155), p. 18.

170 SOLOVE (n. 155), p. 2.

171 Tel est le cas aujourd'hui comme le montre la publicité négative de Microsoft à l'encontre de Google pour promouvoir Hotmail au détriment de Gmail scannant l'ensemble de la correspondance (www.scroogled.com).

172 GÄCHTER/EGLI (n. 58), N. 55, en matière de droit public.

173 Même si l'Etat recourt fréquemment au droit privé pour réaliser un intérêt public (MOOR/FLÜCKIGER/MARTENET [n. 76], p. 112 ss ; sur les problèmes que pose l'application du principe de l'autonomie de la volonté à la collectivité publique, cf. p. 119 ss).

174 SOLOVE (n. 155), p. 14.

175 SOLOVE (n. 155), p. 15.

176 ATF 138 II 346 S. 360 ; BELSER (n. 67), p. 372 ss (p. 400 : pour cette auteure, l'effet horizontal devrait être direct si l'art. 13 II Cst. devait être interprété strictement, c'est-à-dire restreint à l'emploi abusif) ; MEIER (n. 54), p. 68 ; BIAGGINI (n. 76), Art. 13, N. 16 ; SCHWEIZER (n. 78), N. 43.

abandon de l'autodétermination serait dès lors bien plus radical en droit privé, fondé sur l'autonomie de la volonté.

Dans un souci d'harmonisation, il me semble par conséquent préférable de développer des règles tant de droit public que de droit privé limitant ponctuellement l'autodétermination de la personne afin de protéger la partie faible et garantir une concurrence efficace notamment, en s'inspirant des solutions retenues par les législateurs pour limiter le droit de propriété classique et la liberté économique. Nul besoin pour cela d'abandonner le droit à l'autodétermination. Comme celui-ci est susceptible d'être restreint aux mêmes conditions que n'importe quel autre droit fondamental, l'intérêt public ou la protection d'un droit fondamental d'autrui (art. 36 II Cst.) justifiera de protéger dans certains cas l'individu contre des traitements de données, même contre sa volonté. Le choix sera politico-juridique. Doit-on par exemple interdire toute reconnaissance faciale dans les réseaux sociaux ou les moteurs de recherche sur le web ? Doit-on empêcher les enfants et les adolescents de trop s'exposer sur les réseaux sociaux[177] ? Doit-on interdire aux enseignants de devenir « amis » avec leurs élèves sur ces réseaux pour prévenir des abus sexuels[178] ? Doit-on prévoir l'effacement automatique des données personnelles après l'écoulement d'un certain délai ou faut-il laisser à chacun le choix d'exercer ou non un droit à l'oubli[179] ?

6.6. La perte dans les faits de la maîtrise de ses données personnelles – la question de l'assimilation au droit de propriété

Il est devenu aujourd'hui presque impossible de vivre et de communiquer sans laisser de traces dans un monde rempli de capteurs de données toujours plus nombreux, automatisés, performants et discrets. Le constat ne vaut pas seulement sur le web, mais partout sur le territoire et dans les bâtiments. L'individu sait-il vraiment si, où, quand et quelles données sont exactement collectées sur lui et à quelles fins ? N'en perd-il pas le contrôle[180] ? Le droit à l'autodétermination informationnelle serait dès lors devenu une « construction irréaliste » *(« wirklichkeitsferne Konstruktion »)* dans les rapports de droit public et une fiction « audacieuse » *(« kühnste Zustimmungsfiktion »)* dans les rapports de droit privé[181].

Comme je l'ai montré en introduction, l'histoire de la protection des données se confond avec une succession de pertes de maîtrise suivies par de nouvelles régulations toujours aussi rapidement dépassées par l'évolution technologique et laborieusement mises en œuvre. Le droit de la protection des données n'est pas différent de ce point de vue des multiples politiques publiques qui peinent à être exécutées correctement. Faut-il pourtant abroger le droit de la circulation routière en raison des innombrables dépassements de vitesse et de la fréquence des accidents[182] ? Faut-il supprimer le principe cardinal de la séparation du milieu bâti de celui qui ne l'est pas en droit de l'aménagement du territoire parce que celui-ci est difficile à exécuter dans certaines parties du pays ? Que dire de la protection de l'environnement : serait-elle devenue une « construction irréaliste », une fiction « audacieuse » à l'époque des changements climatiques ? La réponse est éminemment politique. Retirer à l'individu la maîtrise de droit sur ses données personnelles parce qu'il en a perdu la maîtrise de fait est un argument défaitiste.

L'exemple du développement de l'informatique ubiquitaire *(cloud computing)*, des données massives *(big data)* conduisant à prédire des risques, des comportements et des préférences *(predictive analytics)* ainsi que celui des réseaux sociaux géants notamment montre à mon avis qu'il faut au contraire donner les moyens à chacun de se réapproprier ses propres données personnelles. Rappeler que le droit à l'autodétermination est gravé dans le bronze de la Constitution est un signal fort. Il permet d'exiger que les architectures informatiques laissent la possibilité aux utilisateurs de ne pas diffuser leurs données à certains cercles de personnes, de s'assurer que les données sont correctement conservées lorsque l'on veut les utiliser, qu'elles sont intégralement détruites lorsqu'on le désire et qu'elles sont gardées en sécurité[183]. Le plus grand danger de l'informatique ubiquitaire réside en effet dans la perte de contrôle de ses données[184].

---

177 Sur le droit des enfants en rapport avec la protection des données, cf. ci-dessus note de bas de page 57.

178 Comme l'exige une loi récente très contestée du Missouri : « Teachers cannot establish, maintain, or use a work-related website unless it is available to school administrators and the child's legal custodian, physical custodian, or legal guardian. Teachers also cannot have a non work-related website that allows exclusive access with a current or former student. » (cf. http://www.huffingtonpost.com/daniel-j-solove/missouri-ban-teachers-friending_b_915656.html).

179 Cf. ci-dessus ch. 5.

180 Dans ce sens, cf. BRUNNER (n. 10), N. 35.

181 BELSER (n. 67), p. 400 ; BRUNNER (n. 10), N. 33 : « wirklichkeitsfremd ».

182 Sur cet exemple en rapport avec la protection des données, cf. AEBI-MÜLLER (n. 7), p. 303.

183 Sur les exigences de la LPD à respecter dans la relation contractuelle unissant l'utilisateur de l'informatique ubiquitaire à l'offreur du service, cf. PHILIPPE FUCHS, « Cloud Computing – eine datenschutzrechtliche Betrachtung », *Jusletter* 6 juin 2012, N. 13 ss.

184 FUCHS (n. 183), N. 26 ss.

Une piste pour renforcer la mise en œuvre de la protection des données personnelles consisterait à s'inspirer du droit de la propriété privée[185]. L'idée selon laquelle l'individu disposerait d'un droit de propriété sur les informations qui le concernent est ancienne. Elle remonte à JOHN LOCKE et a permis de faire évoluer cette institution vers la propriété intellectuelle[186]. Elle se retrouve en arrière-plan du droit à l'autodétermination et du pouvoir de maîtrise et de contrôle qui en découle. La doctrine américaine la discute depuis 1967 au moins à la suite d'un texte fondateur d'ALAN WESTLIN :

> « personal information, thought of as the right of decision over one's private personality, should be defined as a property right. »[187]

La maîtrise dont il est question sur les données personnelles ne peut évidemment être exactement la même que sur les choses. Les règles devraient dès lors être adaptées *mutatis mutandis*[188]. Certains optent pour une voie médiane en voyant sa place entre les droits réels et ceux de la personnalité :

> « Le droit de la protection des données et la notion de maîtrise développée à cet égard trouvent effectivement très bien leur place entre les droits réels (maîtrise au sens de possession) et la protection de la personnalité (maîtrise au sens de droit de la personnalité). »[189]

La proposition d'assimiler l'autodétermination avec la propriété est critiquée, soit parce que la première n'est pas forcément rattachable à la seule personne concernée[190], soit parce que le droit de maîtrise sur les données n'est pas absolu[191], soit encore en raison du caractère plus volatile de l'information[192]. Cette dernière peut être aisément transmise et, une fois connue, ne peut plus être ôtée des esprits. C'est pourquoi, à ce propos, la propriété intellectuelle protège les créations de l'esprit, plutôt que l'esprit lui-même de celles-ci[193].

L'exemple du droit à sa propre image, tantôt protégé par le droit d'auteur[194], tantôt par le droit de la personnalité et de la protection des données[195], montre pourtant que

---

185 Dans ce sens, cf. en droit suisse BRUNNER (n. 10), N. 36 : « Die Datenschutzgesetzgebung sollte um Mechanismen ergänzt werden, die eine klare Zuordnung von ‹ Herrschaftsrechten › – dingliche Rechte wie z.B. Verfügungs- und Nutzungsrechte – an Daten ermöglichen » ; URS HESS-ODONI, « Die Herrschaftsrechte an Daten », *Jusletter* 17 mai 2004, p. 1 : « In der sozialen und ökonomischen Wirklichkeit besteht aber das Bedürfnis nach Herrschaftsrechten (dinglichen Rechten) an Daten. ». Cf. ég. RUDIN (n. 6), p. 428 ss qui se demande pourquoi la protection de la sphère privée, aussi importante pour l'avènement d'une société libérale que la garantie de la propriété privée l'est pour une économie libérale, est plus difficile à mettre en œuvre que la propriété.

186 SOLOVE (n. 46), p. 1112.

187 ALAN F. WESTIN, Privacy and Freedom, Londres/Sydney/Toronto 1967, p. 7, tel que cité *in :* SOLOVE (n. 46), p. 1112 ; LESSIG (n. 26), p. 228 ss ; LAWRENCE LESSIG, « Privacy as Property », *Social Research : An International Quarterly* 2002, 69, no 1, p. 247–269 ; PAUL M. SCHWARTZ, « Property, Privacy, and Personal Data », *Harvard Law Review* 2004, vol. 117, no 7, p. 2056–2128, p. 2055 ss défend, dans un article fouillé, un modèle de propriété adapté aux données personnelles (p. 2095 ss pour l'exposé des cinq éléments de son modèle). Pour une présentation de l'état du débat aux USA avec de nombreuses références, cf. NADEZHDA PURTOVA, « Property Rights in Personal Data : Learning from the American Discourse », *Computer Law & Security Report* 2009, vol. 25, no 6, p. 507–521, p. 507 ss.

188 Cf. dans ce sens en droit suisse la proposition de HESS-ODONI (n. 185), N. 38 : « Im Rahmen der Lückenfüllung ist [dem Datenberechtigten] daher eine eigentumsähnliche Verfügungsmacht in Analogie zu Art. 641 Abs. 1 ZGB zuzusprechen. » Cf. en droit américain, la proposition plus élaborée de SCHWARTZ (n. 187), p. 2055 ss et les réf. cit. ci-dessous note de bas de page 197. Cf. ég. THE ECONOMIST, *New rules for big data : Regulators are having to rethink their brief,* édition du 25 février 2010.

189 GILLES MONNIER « Le piratage informatique en droit pénal », *sic !* 2009, p. 141–153, p. 143.

190 « Das Recht auf informationelle Selbstbestimmung hat nach dem ‹ Volkszählungsurteil › allerdings nicht zur Folge, dass der Einzelne ein eigentumsgleiches Recht an ‹ seinen Daten › hat. Denn der Mensch ist Teil einer miteinander kommunizierenden Gemeinschaft. Eine Information, auch soweit sie personenbezogen ist, stellt ein Abbild sozialer Realität dar, das nicht ausschliesslich dem Betroffenen allein zugeordnet werden kann. » (HANS-JÜRGEN PAPIER, *Festvortrag zur Veranstaltung aus Anlass des 25. Jahrestages der Verkündung des Volkszählungsurteils des Bundesverfassungsgerichts,* Karlsruhe, 15 décembre 2008 ; www.sueddeutsche.de/digital/dokumentation-der-papier-rede-das-internet-vergisst-nicht-1.367248).

191 « Bien que l'on ait coutume de parler de maîtrise sur ou de l'information, le droit [à l'autodétermination en matière de données personnelles] ne se rattache pas à la garantie de la propriété (art. 26 Cst. féd.) ; l'individu ne dispose pas d'un droit de maîtrise absolu sur les données le concernant. » (MEIER [n. 54], p. 66) ; « Entgegen vereinzelter Aufassungen hat der Betroffene kein eigentliches ‹ Dateneigentum › und stehen keine absoluten, uneingeschränkten Verfügungsrechte über Daten in Frage » (AEBI-MÜLLER [n.7], p. 286, note 1561 et p. 294). Cf. ég. GÄCHTER/EGLI (n. 58), N. 25.

192 SOLOVE (n. 46), p. 1113. Le même débat existe pour les données de localisation (géo-données) ; DANIEL KETTIGER, « Geobasisdaten zu Rohrleitungen », *VPB* 2009, n. 20093, p. 48–56, ch. 2.3.1, estime que celles-ci ne peuvent faire l'objet ni de propriété ni de possession.

193 SOLOVE (n. 46), p. 1113.

194 Cf. par exemple en droit allemand l'article 22 I de la loi sur les droits d'auteur dans le domaine artistique *(Kunsturhebergesetz)* selon lequel les images ne peuvent être diffusées qu'avec l'autorisation expresse de la personne concernée (cité *in :* CourEDH, *Von Hannover c. Allemagne [III],* 40660/08 et 60641/08, du 7 février 2012, N. 70).

195 En droit suisse, cf. ATF 138 II 346 358 ; ATF 136 III 401 (404). C'est aussi le cas du droit conventionnel (cf. l'arrêt cité dans la note précédente, N. 96 : « Le droit de la personne à la protection de son image constitue ainsi l'une des conditions essentielles de son épanouissement personnel. Elle présuppose principalement la maîtrise par l'individu de son image, laquelle comprend notamment la possibilité pour celui-ci d'en refuser la diffusion »).

l'assimilation de cette dernière avec la propriété intellectuelle est une piste stimulante pour repenser tout le droit de la protection des données dans le monde numérique[196].

L'utilisation dans le langage courant de l'expression « vol de données personnelles », juridiquement incorrecte certes[197], montre l'extrême porosité conceptuelle entre la propriété et la protection des données. Cette intimité n'a d'ailleurs pas échappé au législateur fédéral : la protection des données personnelles est insérée, dans le Recueil systématique du droit fédéral, à la suite de la propriété intellectuelle, dans la même systématique et sous le même intitulé[198]. Le nid a déjà été préparé ; il ne resterait plus qu'à le remplir !

Raccrocher le droit à l'autodétermination à la garantie de la propriété ne poserait de plus aucune difficulté pratique, du moins pour l'ensemble des données personnelles assimilables à des créations dématérialisées[199]. Dans le monde digital, le nombre de données personnelles dématérialisées est devenu incalculable, à commencer par toutes les données relatives à des textes ou à des images postées sur un réseau social, stockées sur un serveur décentralisé *(cloud computing)* ou dans des bases de données électroniques désormais consultables sur le web[200]. Elles sont toutes aussi reproductibles, diffusables et transférables que les œuvres dématérialisées protégées par le droit d'auteur ; pratiquement, les problèmes de mise en œuvre sont identiques. L'industrie cinématographique a investi de gros moyens pour lutter contre la contrefaçon et la diffusion non autorisée. Même si les résultats ne sont pas vraiment à la hauteur des attentes espérées[201], on pourrait s'en inspirer pour renforcer le respect effectif du droit à l'autodétermination[202], encore plus déficient qu'en matière de propriété intellectuelle[203].

Enfin, certaines propositions techniques et organisationnelles émergentes pour réhabiliter l'individu dans la maîtrise de ses données, à l'instar des nouveaux dépôts de données personnelles *(personal data sores),* impliquent d'adopter un modèle, adapté, de propriété afin que l'individu puisse les faire valoir à l'encontre de tout un chacun :

> Selon le dernier Forum économique mondial de Davos, « [o]ne of the missing elements of the dialogue around personal data has been how to effectively engage the individual and give them a voice and tools to express choice and control over how data about them is used. Over the past twelve months there has been significant momentum in terms of personal data stores that provide individuals a place to store and control how a copy of their data is used and government initiatives to encourage organisations to give individuals a copy of data about them. »[204] Les principales caractéristiques des dépôts de données personnelles

196 Cf. par exemple LESSIG (n. 26), p. 200 : « the problems of privacy and copyright are exactly the same. With both, there's a bit of ‹ our › data that ‹ we've › lost control over. » ; WALKER (n. 128), p. 268 s. trouve la piste intéressante mais jonchée de difficultés sur le plan constitutionnel ; PAMELA SAMUELSON, « Privacy as Intellectual Property ? », *Stanford Law Review* 2000, p. 1125 ss ; critique en droit états-unien en rapport avec la liberté d'expression : VOLOKH (n. 47), p. 1063.

197 BERTRAND PERRIN, « La protection pénale des données informatiques de l'entreprise : un enjeu crucial », *L'expert-comptable suisse* 2011, vol. 85, no 8, p. 605–610, ch. 4.2. Cf. ég. MONNIER (n. 189), p. 141 ss, sur la protection pénale contre le piratage informatique. Sur l'acquisition par le gouvernement allemand de données volées concernant des clients allemands d'une banque suisse, et son caractère punissable en droit suisse, cf. GÜNTER HEINE, « Entwendete und staatlich angekaufte Bankdaten – viel Lärm um nichts ? », *Archives de droit fiscal suisse* 2010–2011, 79, p. 525–544, p. 525 ss.

198 RS 23.

199 Sur la situation juridique des copies d'œuvres sur les serveurs de l'informatique ubiquitaire *(cloud computing),* cf. VINCENT SALVADÉ, « Le droit d'auteur dans le nuage ou dans le brouillard ? : aspects juridiques concernant le cloud computing », *sic !* 2012, p. 161–168, p. 161 ss.

200 Sur l'applicabilité du droit de la protection des données à l'informatique ubiquitaire, cf. FUCHS (n. 183), N. 11 ss ; PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE, *Explications concernant l'informatique en nuage (cloud computing),* Berne 2011. Sur la nécessité d'étendre et d'adapter le droit de propriété aux données personnelles pour répondre aux défis posés par le *cloud computing* et autres développements informatiques actuels, cf. NADEZHDA PURTOVA, « Property in Personal Data : Second Life of an Old Idea in the Age of Cloud Computing, Chain Informatisation, and Ambient Intelligence », *TILT Law & Technology Working Paper* no 2010/017.

201 Sur les difficultés de mise en œuvre du droit d'auteur dans le monde digital, en lien avec la protection des données personnelles, cf. FLORENT THOUVENIN, « Durchsetzung von Urheberrechten und Datenschutz : Lehren aus dem Scheitern von ACTA », *in :* Rolf H. Weber/Florent Thouvenin (éd.), Neuer Regulierungsschub im Datenschutzrecht ?, Zurich 2012, p. 105–129, p. 105 ss.

202 « As with copyright, a privacy property right would create strong incentives in those who want to use that property to secure the appropriate consent. » (LESSIG [n. 26], p. 228 ss). L'auteur n'est pourtant pas dupe des difficultés : « The big difference between copyright and privacy, however, is the political economy that seeks a solution to each problem. With copyright, the interests threatened are powerful and well organized ; with privacy, the interests threatened are diffuse and disorganized. With copyright, the values on the other side of protection (the commons, or the public domain) are neither compelling nor well understood. With privacy, the values on the other side of protection (security, the war against terrorism) are compelling and well understood. » (LE MÊME, p. 200 s.).

203 Sur ce constant en droit privé de la protection des données, cf. BRUNO BAERISWYL, « Geschichten aus dem Wilden Westen – Der Datenschutz im privatrechtlichen Bereich geht seine eigenen Wege : Der Grundrechtsschutz bleibt auf der Strecke », *Digma* 2010, p. 140–145, p. 140 ss.

204 WORLD ECONOMIC FORUM (n. 2), p. 13.

sont entièrement compatibles avec un modèle de propriété des données[205].

Alors que la propriété des choses a été codifiée depuis un passé millénaire et celle des créations intellectuelles depuis quelques siècles[206], la discussion sur la propriété des données personnelles n'en est qu'aux préliminaires avec un passé de quelques décennies seulement. Les hésitations tant de la doctrine que des codificateurs par rapport à la propriété intellectuelle me semblent à cet égard instructives. Assimiler la protection des expressions de l'intellect humain à la propriété privée classique n'a pas été aussi évident de prime abord qu'il y paraît aujourd'hui. En 1890, pour les pères de la protection de la sphère privée en *common law,* le principe qui protège les écrits personnels et toutes les autres productions de ce type, non contre le vol et l'appropriation physique, mais contre la publication, sous quelque forme que ce soit, n'est en réalité pas le principe de la propriété privée, mais celui d'une « personnalité inviolable ». La formule « droit de propriété », qui a été utilisée pour qualifier le droit de contrôler l'acte de publication (ou de non-publication), n'est peut-être pas entièrement satisfaisante, ont-ils affirmé ; elle décrit pourtant suffisamment bien, selon eux, un droit qui, bien qu'incorporel, comprend la plupart des éléments essentiels de la propriété :

> « The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality[207].
>
> The [...] right to control the act of publication, and to decide whether there shall be any publication at all [...] has been called a right of property ; an expression perhaps not quite satisfactory, but on the other hand sufficiently descriptive of a right which, however incorporeal, involves many of the essential elements of property, and is at least positive and definite[208]. »

A la même époque, on refusait de codifier la propriété intellectuelle dans le giron du Code civil suisse en raison de la nouveauté de la matière et de son caractère trop évolutif :

> « Un code civil doit, en principe, embrasser tout le droit privé. Mais il est nécessaire d'admettre des exceptions à cette règle ; le projet en connaît d'assez importantes. [...] celles qui ont trait à la propriété littéraire et artistique, aux marques de fabrique, aux brevets d'invention, au contrat d'assurance, ont été laissées en dehors du projet [...] ; il s'agit ici de matières relativement nouvelles, où des solutions d'une valeur permanente ne sont pas encore trouvées et où se produisent des changements incessants, qu'il est plus aisé d'opérer sous le régime de la législation spéciale que sous celui d'une codification intégrale ; bien plus, ces matières ne peuvent être élucidées d'après les mêmes méthodes que les parties du droit privé qui sont au bénéfice d'expériences séculaires et qui ont reçu leurs formes en quelque sorte définitives »[209].

Il ne pourrait évidemment s'agir que d'une propriété adaptée aux spécificités de la matière. Un régime de propriété des données personnelles serait cependant bien moins éloigné qu'on ne le pense des principales caractéristiques du droit d'auteur : l'objet à protéger est également immatériel ; le droit moral de l'auteur inhérent à la personne – droit de divulgation, de paternité et d'intégrité de l'œuvre est – naliénable et perpétuel[210], tout comme devrait l'être le droit moral de la personne au sujet de laquelle des données sont traitées.

Ce droit moral du « propriétaire des données » pourrait comprendre l'ensemble des droits actuellement garantis par l'autodétermination en matière de données personnelles que j'ai recensés ci-dessus (parmi d'autres[211] le droit d'accès, de rectification, d'effacement des données et le droit à l'intégrité de celles-ci). Il serait complété par une liste de droits patrimoniaux que le propriétaire des données pourrait librement céder et négocier (droit d'utilisation à des fins convenues, droit de suite en cas de cession ultérieure). Le cocontractant obtiendrait la qualité d'ayant-droit de la personne au sujet de laquelle des données sont traitées et pourrait exercer directement les droits patrimoniaux qui lui ont été cédés, à l'opposé du droit moral qui demeurerait attaché à la personne concernée. Une telle institution permettrait en outre de régler probablement plus aisément les droits successoraux lors de la mort de leur propriétaire[212] et formerait le point de départ

---

205 Voir dans ce sens l'analyse de RUBINSTEIN (n. 38) p. 11 ss qui compare les huit caractéristiques des dépôts au modèle de propriété des données tel que proposé par SCHWARTZ (n. 187).

206 Selon WARREN/BRANDEIS (n. 13), p. 195, « Copyright appears to have been first recognized as a species of private property in England in 1558. ».

207 WARREN/BRANDEIS (n. 13), p. 205.

208 WARREN/BRANDEIS (n. 13), p. 205 en note de bas de page.

209 Message à l'Assemblée fédérale concernant le projet de code civil suisse, FF 1904 1, p. 10 s. cité *in :* ALEXANDRE FLÜCKIGER/JEAN-DANIEL DELLEY, « L'élaboration rationnelle du droit privé : de la codification à la légistique », *in :* Christine Chappuis/Bénédict Foëx/Luc Thévenoz (éd.), Le législateur et le droit privé : colloque en l'honneur du professeur Gilles Petitpierre, Genève 2006, p. 123–143, p. 132.

210 Sur ces droits, cf. DENIS BARRELET/STÉPHANE WERLY, Droit de la communication, 2ème éd., Berne 2011, p. 611 ss.

211 Pour une liste de l'ensemble des droits, cf. ci-dessus ch. 5.

212 Sur la pratique actuelle des différents sites web, cf. la comparaison *in :* TIME MAGAZINE, *From Here to E-ternity : What happens to your virtual things when you're gone ?* Edition du 11 février 2013, p. 54 s. ; GERRY W. BEYER/NAOMI R. CAHN, « When You Pass on, Don't Leave the Passwords Behind : Planning for Digital Assets », *Probate & Property* 2012, vol. 26, no 1, p. 40–43, p. 40 ss.

d'une nouvelle fiscalité des données personnelles[213]. Un régime particulier devrait enfin être défini pour les personnes morales.

Alors que le droit constitutionnel à l'autodétermination informationnelle ne déploie des effets directs qu'envers les collectivités publiques (le droit positif ne lie en effet les particuliers que de manière indirecte en vertu de l'article 35 III Cst.[214]), le faire évoluer vers un droit de propriété aurait pour conséquence de le faire valoir *erga omnes* dans les relations entre individus[215]. Cet exercice de codification permettrait de reprendre la mainmise sur ses données personnelles, en particulier dans le champ du droit privé. Dans ce domaine, la mise en œuvre est encore plus déficiente[216] alors qu'un immense marché des données personnelles très lucratif s'est progressivement développé. Les sites web, les moteurs de recherche, les sites de stockage ubiquitaire, les réseaux sociaux et autres concepteurs d'applications pour appareils mobiles négocient aujourd'hui la gratuité de leurs services contre l'utilisation toujours plus intrusive de données personnelles fournies par leurs utilisateurs, qui ne sont d'ailleurs même plus forcément les données concernant leur propre personne comme l'exemple de la reconnaissance faciale sur Facebook le montre aux USA. Les compagnies établissent ensuite de véritables profils de personnalité de plus en plus détaillés dévoilant nos attitudes, nos émotions, nos intérêts, nos goûts, nos habitudes, nos forces, nos faiblesses et même nos comportements futurs probables pour les revendre à prix d'or. Le marché qui s'est créé depuis plusieurs années a conduit à concentrer les profits aux mains de quelques grands opérateurs dominants au détriment tant des individus concernés – qui ne bénéficient que très partiellement de la cession de leur droit d'usage – qu'au préjudice des Etats auxquels échappe en grande partie des ressources fiscales[217]. Si les réseaux sociaux et autres plateformes coopératives devaient devenir le modèle dominant de l'« espace public » du futur, alors la question de savoir qui contrôle cet espace et comment le pouvoir y est organisé deviendra cruciale :

> « If it is indeed true that social networks represent ‹ public space › then very careful consideration needs to be given to who controls that public space and how the power within that space is exercised. »[218]

Sur le modèle du droit d'auteur, le propriétaire des données personnelles – si l'ordre juridique devait faire le pas – disposerait d'un contre-pouvoir qu'il pourrait faire valoir comme monnaie d'échange. Il pourrait non seulement négocier comme actuellement la gratuité des services contre l'utilisation de ses données mais serait susceptible de toucher des « droits de données personnelles » lors de la revente de données, agrégées ou non, ou de profils de personnalité. La gestion de ces droits pourrait être confiée si nécessaire aux préposés à la protection des données ou à d'autres entités de confiance. Les économistes ont déjà commencé à plancher sur ce type de modèle :

> « Since there is, in principle, no reason why third parties should not pay individuals for the use of their data, we introduce a realistic market that would allow these payments to be made while taking into account the privacy attitude of the participants. »[219]

La protection de la personne dans ce nouveau contexte technico-économique exige d'ériger en droit fondamental la maîtrise sur ses données afin de créer un véritable régime de propriété des données personnelles, comme nos ancêtres ont institué autrefois en droit fondamental la maîtrise de la personne sur ses choses et ses créations intellectuelles. Le risque sinon est de mettre ses données à la libre disposition d'autrui sans que l'on soit en mesure d'exiger une prestation quelconque en contrepartie pour ceux qui le désirent :

---

213 Sur la proposition d'introduire à cet effet une taxe sur les données personnelles, « la ressource essentielle de l'économie numérique » où les « utilisateurs, bénéficiaires d'un service rendu, deviennent [...] des quasi-collaborateurs, bénévoles, des entreprises. », cf. Pierre Collin/Nicolas Colin, Mission d'expertise sur la fiscalité de l'économie numérique, Paris 2013, p. 2 et 136.

214 ATF 138 II 346 p. 360 ; Belser (n. 67), p. 372 ss ; Meier (n. 54), p. 68 ; Biaggini (n. 76), Art. 13, N. 16 ; Schweizer (n. 78), N. 43. Cf. ég. la position plus complexe de Gächter/Egli (n. 58), N. 39 s., 47 et 52, pour qui l'article 13 II Cst. ne viserait en première ligne que le seul législateur, mais conserverait un effet direct. On précisera cependant que des obligations positives sont imposées aux Etats dans le cadre de l'art. 8 CEDH (Epiney/Schleiss [n. 55], p. 66 s., avec réf. cit.). On notera par ailleurs que Belser (n. 67), p. 400, refusant de lire un droit à l'autodétermination dans l'article 13 II Cst. propose pourtant de conférer un effet horizontal direct à l'article 13 II Cst., mais seulement si les tribunaux devaient suivre sa proposition d'interpréter cette dernière disposition à la lettre, c'est-à-dire de restreindre la protection à l'emploi abusif.

215 Walker (n. 128), p. 268 ; Volokh (n. 47), p. 1063.

216 Baeryswil (n. 203), p. 140 ss. Brunner (n. 10), ch. VI, plaide à raison pour un « changement de paradigme » dans le domaine du droit privé : « Hinsichtlich der Rechtsdurchsetzung ist (namentlich im privatrechtlichen Bereich) ein klarer Paradigmenwechsel nötig ».

217 Sur la proposition d'introduire à cet effet une taxe sur les données personnelles, cf. Collin/Colin (n. 213).

218 Lorna Stefanick, Controlling Knowledge : Freedom of Information and Privacy Protection in a Networked World, Edmonton 2011, p. 186.

219 Christina Aperjis/Bernardo A. Huberman, *A Market for Unbiased Private Data : Paying Individuals According to their Privacy Attitudes,* HP Social Computing Research, 25 avril 2012, www.hpl.hp.com/research/scl/papers/datamarket/datamarket.pdf. Cf. ég. les auteurs cit. sous note 188.

« Entweder gelingt es, den grundrechtlichen Gehalt des Datenschutzes auch im privatrechtlichen Bereich zu verwirklichen, oder der Datenschutz wird zur Disponibilität der Datenbearbeiter gestellt. »[220]

La mesure n'est toutefois pas suffisante à elle seule. L'information étant devenue fluide et surabondante, le propriétaire n'est plus capable de gérer seul ses données. Si des entreprises privées sont désormais prêtes à l'assister – ouvrant un nouveau marché de la « réputation numérique »[221] , ou si des dépôts de données personnelles *(personal data stores)* lui sont proposés pour l'aider à les gérer et les contrôler[222], il est fort à parier que les forces du marché ne seront pas suffisantes pour assurer la protection effective du propriétaire des données. Des mesures d'assistance, obligations positives de l'Etat, seront indispensables en complément (protection pénale renforcée, droits de recours collectifs ou confiés aux offices de protection des données, surveillance par ces dernières pour exercer une « police » des données, garantie du respect d'éventuelles mesures techniques de protection, gestion collective des « droits de données personnelles », diverses mesures alternatives d'aide à la mise en œuvre)[223]. En effet, ni un régime de propriété des données, ni d'ailleurs le droit à l'autodétermination, ne sont forcément synonymes d'une « autoprotection » des données *(« Selbstdatenschutz »)* ou d'une « auto-gestion » des données *(« self-management »)*[224] : on peut défendre soi-même sa propriété privée, la confier à une société de surveillance ou laisser à la police le soin de patrouiller dans les rues pour la garantir ; la gestion de ses droits d'auteur est confiée à des sociétés de gestion spécialement créées à cet effet[225].

Une telle conception de la propriété des données n'est pas acquise d'avance. Il est certain qu'elle réunira une coalition d'opposants aussi divers que les tenants du partage libertaire des données, les défenseurs de l'hyper-transparence, les critiques du marché, du capitalisme et de l'institution de la propriété privée, les opposants à la marchandisation de la personne ainsi que les grands opérateurs économiquement intéressés à disposer de données librement disponibles. Les réponses à ces critiques vont varier selon les pays et dépendre des mêmes valeurs et sensibilités nationales qui gouvernent le rapport de l'individu à la propriété privée et au marché en général.

Il est pourtant tout à fait envisageable de développer une « protection sociale » des données pour prévenir un « capitalisme sauvage » de celles-ci, même si la circulation globalisée des données personnelles nécessitera d'harmoniser les standards de protection, repoussant d'autant la concrétisation d'une telle proposition. Un régime spécial de libre accès aux données pourrait aussi être adopté pour tenir compte des évolutions des pratiques sociologiques en matière de communication, sur le modèle du libre accès que le propriétaire doit garantir aux forêts et aux pâturages afin que le promeneur puisse s'approprier « baies, champignons et autres menus fruits sauvages » (art. 699 I CC)[226].

En conséquence, je défends l'idée qu'ancrer constitutionnellement la propriété des données personnelles est le pas qui devrait suivre celui qui a conduit au droit à l'autodétermination dans l'évolution des droits relatifs à la personne. Interpréter à la lettre l'article 13 II Cst. pour se limiter à règlementer l'emploi abusif des données et « déconstitutionnaliser » le droit à l'autodétermination, comme une minorité de la doctrine le propose aujourd'hui[227], rendrait la circulation des données personnelles encore plus fluide et sauvage qu'elle ne l'est aujourd'hui ; elle transférerait à la collectivité publique la détermination du sort des données personnelles, qui n'aurait compétence d'agir qu'en cas d'« abus » puisqu'il ne reviendrait plus à la personne de se déterminer elle-même quel que soit le type d'usage. Si l'autodétermination était comprise comme un droit de propriété en droit positif,

220 BAERYSWIL (n. 203), p. 145, qui ne s'exprime pas sur le modèle de propriété..

221 Cf. par exemple www.reputation.com cité dans l'article de THE ECONOMIST, *Protecting privacy online – The price of reputation : Is the market for protected personal information about to take off ?* édition du 23 février 2013.

222 Cf. ci-dessus note 38 et ci-dessus dans la présente section.

223 Cf. dans ce sens une partie des propositions résultant de l'évaluation de la LPD *in :* FF 2012 255, p. 255 ss ainsi que de BRUNNER (n. 10), N. 51 : « Angesichts der praktischen Schwierigkeiten des ‹ Selbstdatenschutzes › lassen sich die Zielsetzungen des Datenschutzes faktisch insgesamt wohl nur verwirklichen, wenn stärker auf Kontrollmechanismen gesetzt wird, die durch Dritte – bestimmte Aufsichts-, Bewilligungs-, Kontroll- oder Zertifizierungsinstanzen – gehandhabt werden ».

224 Cf. par exemple WALTER (n. 124), p. 482 (autodétermination et autoprotection). Sur les difficultés de mettre en œuvre l'autoprotection en droit suisse, cf. BRUNNER (n. 10), N. 51. Sur le *self-management* des données en droit états-unien, cf. SOLOVE (n. 155) : on trouve ici une différence de taille entre droits européens et le droit des USA puisque la mise en œuvre du second dépend essentiellement des individus forcés à agir devant les tribunaux alors que les premiers ont instauré des préposés à la protection des données, cf. BIGNAMI (n. 15), p. 684 ss.

225 Art. 40 ss LDA, RS 231.1.

226 SCHWARTZ (n. 187), p. 2084 ss, propose, dans son modèle de propriété des données personnelles, d'aborder celles-ci sous l'angle des biens communs : « A public goods perspective on information privacy thus does not preclude the propertization of personal data. » (p. 2090).

227 Cf. ci-dessus ch. 6.

la suggestion de la doctrine minoritaire équivaudrait aujourd'hui à proposer une expropriation.

On ne peut dès lors que saluer le Tribunal fédéral qui n'hésite désormais plus à utiliser l'expression « droit de maîtrise sur ses données personnelles » pour définir le droit autodétermination qu'il reconnaît constitutionnellement[228]. La direction prise par les institutions européennes en faveur d'un « droit de contrôle » sur les données devrait marquer durablement la tendance dans la décennie à venir[229].

7. Conclusion

Le droit à l'autodétermination en matière de données personnelles est une condition nécessaire pour protéger la sphère privée à l'ère digitale. Il est cependant insuffisant à lui seul pour assurer un contrôle effectif. La numérisation généralisée de notre monde a fait disparaître les barrières de fait dans la diffusion des informations. L'obscurité pratique qui en résultait autrefois s'est changée en transparence de fait, laissant hors de contrôle une masse croissante de données personnelles produites désormais automatiquement et circulant sans entrave. L'individu laisse des traces digitales de lui partout et constamment. Il revient au droit de renforcer ces barrières puisque de telles données caractérisent et expriment la personnalité de l'individu.

Pour retrouver cette maîtrise perdue, il faut renforcer le droit à l'autodétermination, en particulier dans les relations entre les particuliers où la mise en œuvre est la plus déficiente, en lui conférant un effet direct valable *erga omnes* qui le fera évoluer vers un droit de propriété *sui generis,* lui conférant un véritable pouvoir de maîtrise, et non plus de contrôle seulement.

Comme en propriété intellectuelle, la gestion et la défense de ce droit nécessitera des mesures complémentaires pour assister le propriétaire des données, car l'objet est devenu beaucoup trop fuyant pour que celui-ci soit en mesure d'en assurer seul le contrôle[230].

Enfin, le droit de propriété des données personnelles devra faire l'objet de restrictions suffisantes afin de trouver un équilibre avec les libertés de communication, en particulier avec la liberté d'information avec laquelle il sera en tension constante, toutes aussi indispensables pour l'épanouissement individuel dans un Etat de droit démocratique.

---

228 Cf. ci-dessus ch. 4.3.

229 Cf. ci-dessus ch. 3.3.

230 Telle est la volonté du Conseil fédéral : « Améliorer le contrôle et la maîtrise des données : le contrôle et la maîtrise des données après leur divulgation est un aspect primordial. Ainsi, la possibilité de renforcer les mécanismes de contrôle à disposition du PFPDT et d'adapter aux développements technologiques les droits des personnes concernées devrait être analysée. » (FF 2012 255, p. 268 s).