# Protection des données personnelles, objets connectés et chiffrement des données

par Maximilien Lanna
*Doctorant à l'Université Paris-II Panthéon-Assas (CERSA-CNRS)*
*Chercheur-Assistant à la Chaire MADP de Sciences Po Paris*

Le droit à la protection des données personnelles tend simplement à « établir les règles du jeu, à établir des équilibres entre des aspirations et des intérêts différents, concurrents, parfois contradictoires, dans une société ouverte, démocratique et libre »[1]. Alors que le FBI et l'entreprise américaine Apple se sont livrés cette année un combat judiciaire médiatisé autour de la question de savoir si il peut être demandé au constructeur de smartphones d'extraire des données chiffrées d'un de ses téléphones dans le cadre d'une enquête[2], une communication de la CNIL paru le 8 avril 2016 est venue réaffirmer la nécessité de protéger les données personnelles des individus, notamment par la technique du chiffrement[3].

Celui-ci, défini comme « un élément de la sécurité du patrimoine informationnel » par l'autorité administrative en charge de l'informatique et des libertés, pose la question épineuse de l'équilibre à trouver entre d'une part, le besoin de chiffrement des communications et données pour respecter la vie privée des individus et les libertés fondamentales (tout particulièrement, le droit au respect de la vie privée tel que défini par l'article 9 du Code civil), et les besoins en matière de surveillance. Cet équilibre, au centre des préoccupations depuis les révélations opérées par Edward Snowden[4], ancien consultant de la NSA, est

1. Émilie Debaets, *Le droit à la protection des données personnelles. Recherche sur un droit fondamental*. Thèse de doctorat en droit sous la direction de Bertrand Matthieu, soutenue à Paris-I le 12 décembre 2014.
2. Le Monde, « Reprise des hostilités entre Apple et le FBI », 11 mars 2016
3. Communication CNIL, *Quelle position de la CNIL en matière de chiffrement ?*, 8 avril 2016
4. David Lyon, *Surveillance after Snowden*, Polity Press, Octobre 2015, 120 p.

aujourd'hui à nouveau remis en question par la prolifération d'objets connectés, s'inscrivant ainsi dans le mouvement d'inversion des hiérarchies traditionnelles entre sécurité et liberté[5].

Le droit à la protection des données personnelles tel qu'on le connaît aujourd'hui s'apparente, du moins au niveau européen, à un droit fondamental[6]. Son acte de naissance, première pierre de l'édifice législatif et réglementaire que nous connaissons aujourd'hui, remonte au Data Protection Act entré en vigueur en 1970 au sein du länder d'Hesse en Allemagne[7]. Ce dispositif protecteur, suivi en 1978 par l'adoption de la loi Informatique et Libertés en France, a permis la construction progressive d'un système de protection reposant sur des instruments supranationaux et visant à se distinguer progressivement de la réglementation en matière de protection de la vie privée[8].

Protégé au titre de la vie privée par l'article 8 de la CEDH garantissant le droit au respect de la vie privée et familiale[9], l'adoption en 1981 d'une Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel – dite Convention 108 – a permis de faire la distinction entre protection de la vie privée et protection des données personnelles[10]. En matière de droit de l'Union européenne, la protection des données personnelles est régie par la directive 95/46/CE du 24 octobre 1995. Cette directive, inspirée par la Convention 108, sera remplacée en 2018 par l'entrée en vigueur du nouveau règlement européen sur le sujet[11].

Alors qu'on estime qu'ils seront 50 milliards à l'horizon 2020[12], les objets connectés, de par l'interconnexion permanente qu'ils permettent entre eux-mêmes ou entre eux et l'utilisateur, posent de nouveaux défis en matière de

5. Isabelle Boucobza et Charlotte Girard, « "Constitutionnaliser" l'état d'urgence ou comment soigner l'obsession d'inconstitutionnalité ? », La Revue des droits de l'homme, Actualités Droits-Libertés, 5 février 2016

6. Agence des droits fondamentaux de l'Union européenne, *Manuel de Droit européen en matière de protection des données*, juin 2014

7. Gloria Gonzalez, *The Emergence of Personal Data Protection as a fundamental right of the EU*, p. 57, Springer, 2014

8. Bénédicte Rey, *La vie privée à l'ère du numérique*, Lavoisier, coll. « Traitement de l'information », 2012, 297 p., ISBN : 9782746231207

9. Conseil de l'Europe, Convention Européenne des Droits de l'Homme, STCE n° 005, 1950.

10. Ainsi, selon l'article 1er de cette Convention, « Le but de la présente Convention est de garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant ("protection des données") ».

11. Céline Castets-Renard, « Brève analyse du règlement général relatif à la protection des données personnelles », Dalloz IP/IT 2016, p. 331

12. Cisco France Blog, *50 milliards d'objets connectés en 2020*, accessible en ligne à : http://gblogs.cisco.com/fr-datacenter/2011/07/17/50-milliards-dobjets-connectes-en-2020/

sécurité et viennent semer le trouble dans la législation existante. L'internet des objets, défini comme « un réseau de réseaux permettant, via des systèmes d'identification électronique normalisés et unifiés […] de pouvoir récupérer, stocker, transférer et traiter, sans discontinuité entre les mondes physiques et virtuels, les données s'y rattachant »[13] a des conséquences jusque-là impensée en matière du flot de données – souvent personnelles et identifiantes – qui est établi.

La présentation envisagée aura pour but de montrer en quoi les objets connectés posent de nouvelles questions en matière de législation sécuritaire. Entre la nécessité de mettre en œuvre des mesures relatives à la cybersécurité des objets en question, besoin de garantir les droits fondamentaux des citoyens et accès administratif aux données de connexion, nous tenterons d'envisager l'équilibre à donner entre ces différents éléments ainsi que les tensions qui les animent. En effet, toute la problématique s'articule autour de la question de savoir comment concilier d'une part, protection des données et d'autre part, besoin d'accéder aux informations en vue de garantir la sécurité publique.

Cela revient en fait à se demander quelles exceptions permettent de limiter le droit fondamental qu'est celui de la protection des données personnelles. Nous verrons ainsi en quoi il apparaît nécessaire, dans certaines situations précisément définies, de pouvoir limiter cette protection. Le développement récent des objets connectés, s'il met en œuvre une évidente dispersion des données personnelles des individus (**I**) permet aussi de révéler les exigences contradictoires qui existent quant à la mise en œuvre de la protection de celles-ci (**II**).

## I. La dispersion des données personnelles des individus

Le développement en cours et à venir des objets connectés pose la question de la sécurité des données qui seront créées, transférées et stockées. Qu'il s'agisse d'un smartphone ou encore d'un bracelet connecté permettant de suivre l'activité physique, les données – souvent personnelles – des individus font l'objet d'une dispersion (**A**) que le droit a du mal à encadrer (**B**).

### A. Les objets connectés, vecteur de dispersion des données personnelles

Le modèle économique mis en place par les objets connectés – dit modèle behavioriste[14] – reprend celui initié par les réseaux sociaux et au sein duquel l'utilisateur est amené à divulguer le plus de données personnelles possible. La valeur d'usage de

13. Pierre-Jean Benghozi, Sylvain Bureau, Françoise Massi-Folléa, *L'Internet des objets, quels enjeux pour l'Europe*, Editions de la Maison des Sciences de l'Homme, Paris, 2009, 170 p.
14. Rallet, Alain, et Fabrice Rochelandet. « La régulation des données personnelles face au web relationnel : une voie sans issue ? » Réseaux 3 (2011) : 17-47.

l'offre de services en ligne dépend dès lors de la production de données par les individus eux-mêmes qui deviennent dépendant des contenus qu'ils divulguent pour pouvoir accéder à ces services[15]. Ce web symbiotique qui est mis en œuvre par les objets connectés repose dès lors sur l'échange constant de données et services entre entreprises d'une part et individus de l'autre[16]. Pourtant, cet échange n'est pas sans poser problème, notamment concernant le consentement qui est donné par les individus. Ces derniers ne sont pas forcément au courant de la diffusion massive de métadonnées que le service numérique qui est utilisé génère. Les données passives des utilisateurs ne sont dès lors pas toujours prises en compte par les conditions générales d'utilisation des applications[17] : les données sur les données échappent donc parfois au consentement des individus[18].

Outre le changement radical de modèle économique mis en œuvre par les objets connectés, ceux-ci, de par leur structure, présentent des garanties de sécurité moins efficaces que celles, par exemple, des ordinateurs. Basés sur une technologie RFID de capture automatique et d'échange de données, ils permettent ainsi de collecter ces dernières dans ce qu'elles ont de plus personnelles[19], d'où leur caractère hautement invasif[20].

Si l'on prend l'exemple d'un simple tracker d'activité, celui-ci permet de géolocaliser son utilisateur, de déterminer par extension son adresse, son lieu de travail et ses déplacements au sens large[21]. Couplé à une application permettant d'analyser les données recueillies, celui-ci permet également de déterminer des éléments relatifs à la santé de l'utilisateur (rythme cardiaque, taille, poids, distance parcourue chaque jour…)[22]. À titre d'exemple, n'importe quel *smartphone* de

15. Grazia Cecere et al., « Les modèles d'affaires numériques sont-ils trop indiscrets ? Une analyse empirique », Réseaux 2015/1 (n° 189), p. 77-101.
DOI 10.3917/res.189.0077.
16. Paul Bernal, *Internet Privacy Rights, Rights to Protect Autonomy*, Cambridge Intellectual Property and Information Law, 2014.
17. Juliette Sénéchal, « La fourniture de données personnelles par le client via Internet, un objet contractuel ? » La preuve dans le contentieux commercial, AJ Contrats d'affaires – Concurrence – Distribution. 2015, n° 5. p. 212.
18. Manuel Munier, Vincent Lalanne, Pierre-Yves Ardoy, Magali Ricarde, « Métadonnées et Aspects Juridiques : Vie Privée vs Sécurité de l'Information », 9e Conférence sur la Sécurité des Architectures Réseaux et des Systèmes d'Information (SARSSI'2014), Mai 2014, Saint-Germain-Au-Mont-d'Or, France, p. 65-76, 2014.
19. Demetrius Klitou, *Privacy Invading Technologies and Privacy by Design, Safeguarding Privacy, Liberty and security in the 21st century, Information Technology and Law Series*, Springer, 2014, p. 173.
20. Maras, Marie-Helen. "Internet of Things : security and privacy implications." International Data Privacy Law 5.2 (2015) : 99.
21. Paul Bernal, *Internet Privacy Rights, Rights to Protect Autonomy*, Cambridge Intellectual Property and Information Law, march 2014, p. 65.
22. Santé Connectée, *De la e-santé à la santé connectée*, Le livre blanc du Conseil national de l'Ordre des médecins, janvier 2015.

dernière génération embarque des paramètres relatifs à la santé et qui sont activés par défaut lors de l'achat de l'appareil.

Ce recueil de données hautement personnelles est à mettre en relation avec les failles de sécurité auxquelles les objets connectés sont soumis[23]. Trois cycles concernant les données sont identifiés : création – transmission et analyse – stockage. La donnée, qui n'est pas toujours chiffrée, est vulnérable à chacun de ces stades. En effet, les objets connectés, plus petits et compacts, n'embarquent pas le même type de protection que des systèmes plus grands et complexes peuvent mettre en œuvre.

La FTC met l'accent, Outre-Atlantique, sur trois types de risques qui sont inhérents aux objets connectés[24]. Ceux-ci permettraient en effet d'accéder plus facilement aux données personnelles, de rendre les autres systèmes encore plus vulnérables ou bien de présenter en eux-mêmes des failles de sécurité. Si ces risques ne sont pas propres aux objets connectés, la nature de ceux-ci, telle qu'évoquée précédemment, permettrait d'accentuer ces risques. Plusieurs raisons sont avancées. Par exemple, les entreprises commercialisant des objets connectés n'ont pas forcément la même expertise dans le domaine de la sécurité que les entreprises proposant des systèmes d'exploitation plus traditionnels[25]. De même, les objets connectés, notamment ceux entrant dans la catégorie des trackers d'activité physique, sont parfois le fruit du travail de jeunes startups ne possédant pas toujours les compétences propres à sécuriser l'objet qu'elle propose.

Ces objets connectés ont ensuite la particularité d'être relativement peu coûteux et donc de ne pas embarquer des solutions de sécurité satisfaisantes. Le groupe de travail de l'article 29 a eu l'occasion d'insister sur ce point dans un avis en date de 2014 et dans lequel il constate que la plupart des capteurs présents sur le marché ne mettent pas en œuvre d'échanges de données sécurisés. En effet, la dernière menace mise en avant repose sur le fait que des correctifs de sécurité ne sont quasiment jamais proposés aux utilisateurs une fois qu'ils ont fait l'acquisition de l'objet et que des failles de sécurité apparaissent. Deux options sont dès lors avancées afin de pouvoir faire face à ces menaces. D'une part, mettre en place une obsolescence programmée de ces dispositifs et d'autre part, instaurer un droit au silence des puces permettant de faire taire celles-ci à distance[26]. Si ces mesures semblent représenter une bonne amorce de solution, elles n'empêchent pour autant pas une certaine confusion au niveau juridique.

---

23. Mario Ballano Barcena et al., Security Response, *How safe is your quantified self ?*, SYMANTEC (Version 1.1 – Aug. 11, 2014), www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/how-safe-is-your-quantifiedself.pdf
24. FTC, *Internet of Things : Privacy & Security in a Connected World*, 9 janvier 2015.
25. Privacy Rights Clearinghouse, *Mobile Health and Fitness apps : what are the Privacy Risks ?*, posted July 2013, Revised December 2014.
26. Bernard Benhamou, « La gouvernance de l'internet après Snowden », Politique étrangère 2014/4 (Hiver), p. 15-27, DOI 10.3917/pe.144.0015.

### B. Les objets connectés, objets juridiques insaisissables

Partant du constat que les objets connectés permettent de recueillir un nombre encore plus grand de données, la question s'est posée de savoir comment la loi devait venir encadrer ces pratiques. En effet, au vu des risques de sécurité en cause, la question a pu se poser de savoir si la loi « Informatique et libertés » n'était pas dépassée[27]. Le Conseil d'État, dans son rapport annuel en date de 2014, est venu trancher la question en indiquant que la réglementation « Informatique et libertés » était toujours d'actualité, mais que les modalités de mise en œuvre de cette protection devaient évoluer[28].

De manière plus générale, on peut opposer ici un certain principe de précaution à un principe d'innovation libre[29]. Selon une thèse développée par un chercheur américain, le droit peut soit chercher à réglementer en amont les innovations technologiques, en cherchant à tout prix à les encadrer – c'est ce que l'on désigne ici par principe de précaution –, soit le droit peut faire place au principe d'innovation libre, venant simplement accompagner l'innovation par l'instauration de grands principes.

Il semble incontestable que nous nous situons actuellement dans la deuxième hypothèse. À titre d'exemple, l'article 6 de la loi « Informatique et libertés » met en œuvre des principes permettant d'encadrer les modalités de collecte des données personnelles : entre finalité déterminée, proportionnalité et principe d'exactitude des données récoltées, ces principes – bien que difficiles à faire respecter en pratique – constituent le socle de règles à respecter dans la mise en œuvre d'un traitement de données, bien que la récolte continue de données regroupées sous la notion de big data mette à mal ces principes[30]. Ces derniers semblent en effet difficilement conciliables avec l'idée d'une collecte permanente de données pour des finalités qui ne sont toujours pas connues à l'avance[31].

Cependant, si l'on peut penser dans un cas qu'il est du rôle des pouvoirs publics de réguler au mieux ces innovations, force est de constater qu'une réglementation trop poussée finirait par limiter les innovations en la matière. Dès lors, c'est sur le terrain de la coopération – notamment internationale – qu'il faut se placer.

---

27. Laurent Cytermann, « La loi Informatique et libertés est-elle dépassée ? », RFDA 2015, p. 99.
28. Les Rapports du Conseil d'État, « Le Numérique et les Droits fondamentaux », 2014.
29. Adam Thierer, « The Internet of Things and Wearable Technology : Addressing Privacy and Security Concerns without Derailing Innovation », 21 RICH. J.L. & TECH. 6 (2015), http://jolt.richmond.edu/v21i2/article6.pdf
30. Isabelle Beyneix, « Le traitement des données personnelles par les entreprises : big data et vie privée, état des lieux », La semaine Juridique, Edition Générale, n° 46-47, 9 novembre 2015.
31. Viktor Mayer-Shönberger and Kenneth Cukier, *Big Data, A Revolution That Will Transform How We Live, Work and Think*, John Murray Publishers, 2013.

Pourtant, l'exemple récent de l'invalidation du *Safe Harbor* montre que des progrès sont encore à établir. Alors que la directive relative au traitement des données à caractère personnel dispose que le transfert de telles données vers un pays tiers ne peut, en principe, avoir lieu « que si le pays-tiers en question assure un niveau de protection adéquat à ces données », la Cour de justice de l'Union européenne a invalidé la décision de la Commission constatant que les États-Unis n'assurent pas un niveau de protection adéquat aux données à caractère personnel transférées.

Si la Cour de justice a autorisé de manière provisoire que ce flux de données entre les continents puisse perdurer, elle a, avec cet arrêt, marqué le coup d'envoi de nouvelles négociations visant à la conclusion d'un nouvel accord. Intitulé *Privacy Shield* et entré en vigueur le 1er août 2016, celui-ci a pour but de renforcer les garanties apportées aux citoyens européens quant à la protection de leurs données, notamment vis-à-vis des problématiques de surveillance de masse ou d'absence de recours efficaces. Ces difficultés que le droit a à se saisir de ces problématiques révèlent l'existence d'exigences contradictoires en matière de protection des données.

## II. Des exigences contradictoires en matière de protection des données

Comme le révèle la CNIL dans son rapport d'activité pour l'année 2015, trois tendances se dessinent concernant la collecte et le traitement des données personnelles. D'abord, la création de nouveaux fichiers visant à la lutte anti-terroriste, ensuite, une recrudescence de la surveillance et du contrôle des communications électroniques et enfin, l'évolution du renseignement avec la « possibilité de collecter un volume important de données »[32]. Si l'exigence de sécurité publique permet de limiter la portée de la protection des données (**A**), il ne faut pourtant pas négliger le mouvement de renforcement de la protection qui est à l'œuvre (**B**).

### A. La sécurité publique, limite légitime à la protection des données

La protection des données personnelles, bien qu'élevée au rang de droit fondamental, peut faire l'objet de certaines restrictions. En effet, si l'enjeu pour l'État est de promouvoir la protection de la vie privée, notamment en passant par la protection des données personnelles, il apparaît nécessaire, dans certaines situations précisément définies, de pouvoir limiter cette protection et ce afin de garantir la sûreté. La jurisprudence de la CEDH a déjà eu l'occasion de démontrer qu'il existe des exceptions légitimes à la protection des données personnelles des individus.

32. CNIL, *rapport d'activité annuel*, 2015.

Dans un arrêt rendu par la Cour le 6 septembre 1978[33] et concernant une affaire d'interception de communications, d'écoutes téléphoniques et d'opérations de surveillance, celle-ci a conclu à la non-violation de l'article 8 de la Convention en considérant que le législateur – allemand en l'espèce – pouvait permettre aux autorités de surveiller des correspondances. Si la Cour n'a pas conclu à la violation de l'article 8 de la Convention Européenne des Droits de l'homme, elle n'a pourtant pas manqué de rappeler que « l'existence de dispositions législatives accordant des pouvoirs de surveillance secrète » devait se cantonner à une situation exceptionnelle[34]. Cette interprétation est toujours la sienne aujourd'hui, comme en témoignent les arrêts Zakharov et Szabo, les juges considérant dans la seconde espèce que les mesures de surveillance ne peuvent être utilisées que si strictement nécessaires à la sauvegarde des institutions[35].

La situation exceptionnelle soulevée à l'époque par la Cour Européenne des Droits de l'Homme nous permet d'envisager l'hypothèse d'interceptions de communications réalisées par le biais d'objets connectés. L'actualité récente a permis d'illustrer les conflits qui existent à l'heure actuelle sur ces questions. Récemment, ce sont Apple et le FBI qui se sont opposés aux États-Unis, l'agence fédérale américaine ayant demandé au constructeur de pouvoir contourner le système de sécurité d'un de ses smartphones afin d'accéder à son contenu[36]. De manière plus large, c'est la question du chiffrement des données qui est abordée, celui-ci permettant aux données et aux conversations des utilisateurs de rester secrètes.

Les principes relatifs à la surveillance des communications par les pouvoirs publics ont été à l'origine fixés par la loi du 10 juillet 1991. Cette loi est venue réaffirmer le secret des communications et seuls deux cas permettant d'y déroger ont été mentionnés : sur décision de l'autorité judiciaire ou, à titre exceptionnel et pour des finalités définies par la loi, sur décision du premier ministre et sous le contrôle de la commission nationale de contrôle des interceptions de sécurité (CNCIS). Comme le souligne le rapport du Conseil d'État consacré au numérique et aux droits fondamentaux, la surveillance des communications par les pouvoirs publics est l'un des instruments de la responsabilité de l'État visant à assurer la protection de la sécurité de la population et la défense des intérêts fondamentaux de la Nation.

---

33. Cour Européenne des Droits de l'Homme, Klass et autres c Allemagne, n° 5029/71, 6 septembre 1978.
34. Cour Européenne des Droits de l'Homme, Fiche thématique, Protection des données personnelles, juin 2016.
35. Cour. EDH, Gr. Ch., 4 décembre 2015, Zakharov c. Russie, Req. n° 47143/06 et Cour EDH, 5e sect., 12 janvier 2016, Szabo c. Hongrie, Req. n° 37138/14.
36. http://www.lefigaro.fr/secteur/high-tech/2016/03/29/32001-20160329ARTFIG00023-le-fbi-abandonne-ses-poursuites-contre-apple.php

Dès lors, les « interceptions administratives relèvent d'une démarche de prévention de la criminalité organisée, du terrorisme et des autres menaces contre la sécurité nationale ». À ce titre, bien que la directive n° 2002/58/CE (dite vie privée et communications électroniques) énonce un principe de confidentialité interdisant « à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférents » (article 5.1), l'article 15.1 de la directive permet aux États membres d'adopter des dispositions limitant la portée de ce principe dans la mesure où une limitation « constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques »[37].

Ces exceptions, légitimées par la sauvegarde de la sécurité nationale, se trouvent renforcées par les dispositions concernant la cryptographie. En effet, il est admis que l'État puisse se doter de capacités permettant de lever la confidentialité des messages chiffrés. L'article 230-1 du Code de procédure pénale dispose que, dans le cadre d'une enquête, il est possible de faire appel à toute personne qualifiée « en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair de ces informations ». L'usage de procédés de déchiffrement est ainsi explicitement admis.

Depuis la mise en place d'une réglementation propre à la protection du secret des communications, les techniques et procédés de transmission, de stockage et d'analyse des données ont évolué[38]. Deux textes sont récemment venus compléter le dispositif afin de répondre à l'évolution des techniques ainsi qu'aux nouvelles menaces pour la sécurité. Il s'agit d'une part de la loi de programmation militaire, ayant permis de modifier le régime juridique applicable aux accès administratifs aux données de connexion et de la loi relative au renseignement dont le principal objet a été d'autoriser ou de légaliser de nouvelles modalités de collecte. Ce dispositif s'est trouvé renforcé avec l'état d'urgence, la loi du 21 juillet 2016 prévoyant ainsi que les juges des référés des tribunaux administratifs puissent autoriser l'exploitation des éléments informatiques saisis lors des perquisitions effectuées dans le cadre de l'état d'urgence. Cependant, ce mouvement permettant d'avoir accès aux données ne doit pas éclipser le mouvement contradictoire consistant en un renforcement concomitant des dispositifs protecteurs des données personnelles.

---

37. Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).

38. Institut Montaigne, *Big Data et Objets connectés, Faire de la France un champion de la Révolution Numérique, rapport*, avril 2015.

### B. Le renforcement de la protection des données

Alors que les critères relatifs à la sécurité permettent un accès amplifié aux données personnelles, on constate, parallèlement à ce mouvement, la mise en place de nouvelles solutions visant à renforcer les droits des individus sur leurs données personnelles. Dès lors, on ne peut que constater les tensions existant entre d'une part, la volonté de pouvoir donner aux autorités un moyen d'accéder plus facilement aux données personnelles des individus et d'autre part, le mouvement – majoritairement européen – visant à la mise en place d'une législation respectueuse des données des individus.

Sécuriser les flux de données personnelles provenant des objets connectés est apparu comme une amorce de solutions permettant de protéger efficacement la vie privée des individus. Cependant, le chiffrement des données n'apparaît pas comme une solution infaillible permettant de garantir la confidentialité des données. Encore plus menacée eu égard au caractère ubiquitaire des objets connectés[39], des amorces de solutions tentant de protéger au mieux les données ont été avancées, parfois en vain. En effet, si l'on prend l'exemple de la pseudonymisation, celle-ci ne vient pas changer la nature des données : elles restent des données personnelles dont la réidentification par le responsable de traitement ou une tierce partie est possible[40]. Il en va de même pour l'anonymisation qui ne permet pas la mise en œuvre de mesures de sécurité infaillibles[41]. Il a dès lors été prévu de renouveler la protection d'ordre juridique, notamment par l'adoption d'un règlement européen. Celui-ci, en projet depuis 2012, vise à remplacer la directive de 1995 sur le sujet du traitement des données. L'emploi d'un instrument juridique différent permettra, à terme, une unification des règles en la matière, tout en permettant de réduire l'autonomie de chaque État. Autonomie qui s'exprime en France avec l'adoption de la loi pour une République numérique mettant en œuvre des mesures telles que le droit à l'oubli numérique pour les mineurs ou encore le principe de portabilité des données.

Le règlement européen est surtout l'occasion de mettre en œuvre de nouveaux principes de protection, directement inspirés du concept d'autodétermination informationnelle. Ce dernier, issu d'une décision de la Cour constitutionnelle fédérale allemande de décembre 1983 s'entend du « pouvoir de l'individu à décider lui-même, sur base du concept d'autodétermination, quand et dans quelle

39. Lu Xiaofeng, Qu Zhaowei, Li Qi, Hui Pan, « Privacy Information Security Classification for Internet of Things based on Internet Data », International Journal of Distributed Sensor Networks 2015, article ID 932941.
40. Florence Raynal et al., « De nouvelles dispositions pour protéger les données personnelles », Documentaliste-Sciences de l'Information 2014/3 (Vol. 51), p. 23-25, DOI 10.3917/docsi.513.0023.
41. Narayanan Arvind, Edward W. Felten, « No silver bullet : De-identification still doesn't work », White Paper, 2014.

mesure une information relevant de sa vie privée peut être communiquée à autrui »[42]. Ce concept d'autodétermination informationnelle inspire directement le projet de règlement européen avec l'instauration de principes tels que ceux de l'*accountability* (conformité aux règles en vigueur), des *privacy impact assessments* (études d'impact) et du *privacy by design*. Ce dernier, qui n'est pourtant pas nouveau, permet d'incorporer directement des règles de protection des données personnelles et de la vie privée dans les dispositifs informatiques utilisées par les individus, et ce dès leur conception[43]. Bien que le manque de définition concrète d'un tel principe puisse poser problème, celui-ci permet de démontrer la volonté d'une protection en amont des données personnelles[44].

Si le Parlement européen, *via* cette directive, souhaite intégrer à priori les standards susceptibles de permettre aux individus de garder un contrôle sur leurs données, il n'est pas la seule institution supranationale à vouloir protéger la vie privée des individus. La CJUE, dans un arrêt de grande chambre en date du 8 avril 2014, est venue indiquer que la directive 2006/24/CE relative à la conservation des données comporte « une ingérence dans les droits fondamentaux d'une vaste ampleur et d'une gravité particulière »[45]. Selon cette directive, il est fait obligation aux fournisseurs de services de communications électroniques de conserver les données en cause, afin de les rendre accessibles aux autorités nationales compétentes en matière de recherche, de détection et de poursuite d'infractions graves[46]. La Cour relève ainsi que les dispositions de cette directive relative à la conservation des données « portent atteinte à certaines dispositions de la Charte des Droits fondamentaux de l'Union Européenne »[47], notamment les articles 7 et 8 relatifs respectivement à la vie privée et à la protection des données personnelles. Ainsi, le juge de Luxembourg considère que la lutte contre la criminalité organisée et le terrorisme ne saurait autoriser des atteintes injustifiées aux droits fondamentaux en relevant particulièrement deux principes, la nécessité et la proportionnalité de l'atteinte, ces deux critères faisant défaut en l'espèce.

---

42. BVerfGE 65, 1 – Volkszählung Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. Und 19. Oktober 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden.
43. Laure Marino, « Le règlement européen sur la protection des données personnelles : une révolution ! », La Semaine Juridique, Edition Générale, 30 mai 2016, Hebdomadaire, n° 22.
44. Alain Rallet et al, « De la Privacy by Design à la Privacy by Using. Regards croisés droit/économie », Réseaux 2015/1 (n° 189), p. 15-46. DOI 10.3917/res.189.0015.
45. CJUE, grande chambre, 8 avril 2014, Digital Rights Ireland Ltd & Michael Seitlinger e.a., affaires jointes C-293/12 & C-594/12.
46. Article 1 § 1, Directive 2006/24/CE.
47. Marie-Laure Basilien-Gainche, « Une prohibition européenne claire de la surveillance électronique de masse », La Revue des droits de l'homme [En ligne], Actualités Droits-Libertés, mis en ligne le 14 mai 2014, consulté le 15 janvier 2016. URL : http://revdh.revues.org/746.

La criminalité organisée et le droit des données personnelles sont récemment l'objet de tensions qui tiennent à les opposer tout en les renforçant mutuellement. Les nouvelles menaces terroristes, généralisées ces derniers temps, rendent légitimes la mise en place de moyens de surveillance élevés nécessitant un accès plus large aux données personnelles des individus. Parallèlement à ce mouvement, la dynamique relative à la protection des données personnelles prend progressivement de l'ampleur, entre les révélations de différents lanceurs d'alertes et les pressions de la société civile, renforcées par une prise de conscience collective de l'opinion publique. Ces tensions, chacune légitime eu égard aux objectifs poursuivis, sont soumises à l'appréciation d'un principe de proportionnalité par le juge. Elargi dans le cadre du droit national et du Conseil de l'Europe, il est d'appréciation stricte pour le Parlement (cf., le règlement européen entrant en application en 2018) et la Cour de justice (cf. les arrêts Schrems et Digital Rights Ireland invalidant pour l'un le Safe-Harbor et pour l'autre, la directive 2006/24/CE). Si les tensions entre besoins sécuritaires et nécessité de protection des données s'en trouvent renforcées, ces oppositions permettent, in-fine, de déterminer les positions de chacune des institutions concernées, mais également de démontrer la bivalence de la surveillance pesant sur les individus, entre surveillance par les entreprises privées (grâce par exemple aux objets connectés) et surveillance par les gouvernements (via les modalités d'accès aux données de connexion). Il faudra, sur le long-terme, trouver une solution permettant une mise en équilibre entre ces différentes tensions, équilibre qui semble à l'heure actuelle précaire et malléable.