Institut Mines-Télécom

CHAIRE VALEURS ET POLITIQUES DES INFORMATIONS PERSONNELLES

DONNÉES PERSONNELLES ET OBJETS CONNECTÉS EN EUROPE

PERSPECTIVES TECHNOLOGIQUES ET ENJEUX DE RÉGULATION

RAPPORT

18 AVRIL 2017

BERNARD BENHAMOU

EXPERT ASSOCIÉ À LA CHAIRE

SOMMAIRE

Institut Mines-Télécom

DONNEES PERSONNELLES ET OBJETS CONNECTES EN EUROPE

PERSPECTIVES TECHNOLOGIQUES ET ENJEUX DE REGULATION

« Lorsqu'un objet se connecte à l'Internet, trois choses se produisent :

- *il devient intelligent,*
- *il devient piratable,*
- *et enfin il ne vous appartient plus vraiment… »*

A. C. Madrigal & R. Meyer
The Atlantic[1], 28 septembre 2014

Les terminaux mobiles ont permis à près de deux milliards et demi d'utilisateurs d'adopter une « grammaire » commune pour échanger des informations sur Internet. Désormais, la chute des prix des capteurs et la montée en puissance des outils d'analyse des informations se conjuguent pour permettre la création de nouvelles générations d'objets connectés qui viendront progressivement se fondre dans la vie quotidienne de leurs usagers au point d'en devenir indiscernables[2]. Les capacités de ces objets à recueillir des informations à chaque étape de la vie quotidienne en feront les vecteurs privilégiés de nouvelles générations de services dans les domaines de la santé, de l'énergie, de la maîtrise de l'environnement ou encore des transports…

Dans le même temps, ces capteurs constituent un levier puissant de la transformation de la notion même de « donnée personnelle ». Ils permettent en effet le recueil des informations en continu sur leurs utilisateurs et leur environnement. Ces informations qui jusqu'alors ne pouvaient être rassemblées que de manière fragmentaire, peuvent désormais être transmises et traitées à moindre coût. Qu'il s'agisse des paramètres de

---

[1] *When Everything Works Like Your Cell Phone* (The Atlantic, 28 septembre 2014)
http://www.theatlantic.com/technology/archive/2014/09/when-everything-works-like-your-cell-phone/379820/

[2] *«Les technologies les plus profondes sont celles qui disparaissent. Elles se fondent dans la trame de la vie quotidienne jusqu'à en devenir indiscernables.»* (*The Computer for the 21st Century,* Mark Weiser, Scientific American 1991)
https://www.ics.uci.edu/~corps/phaseii/Weiser-Computer21stCentury-SciAm.pdf

déplacements, des données liées à la santé, des informations sur les habitudes de vie ou de consommation, les objets connectés deviennent les témoins de chacune des actions de leurs utilisateurs. La régulation des données personnelles issues de ces objets et les mesures qui seront prises pour encadrer la conception des objets connectés constituent de nouveaux enjeux stratégiques pour les acteurs publics et pour les industriels. Les formes que prendront ces mesures d'encadrement pourraient aussi influencer l'organisation des modes de vie de nos sociétés dans les prochaines décennies.

I / LE NOUVEAU PAYSAGE TECHNOLOGIQUE DES OBJETS CONNECTES

Des données personnelles de plus en plus massives et encore plus « sensibles »

Si, isolément, les données issues des capteurs sont souvent perçues par leurs utilisateurs comme peu révélatrices de leurs actions ou de leurs comportements, leur étude et leur agrégation peuvent donner lieu à des interprétations, des déductions, voire même des anticipations sur les comportements, convictions ou état de santé notamment. Bien avant que ne soient développés des objets connectés, les sociétés émettrices de cartes de crédit développaient des algorithmes permettant, par exemple, de prévoir le divorce de leurs clients. Ce que Ian Ayres, professeur de droit à Yale, précise dans son ouvrage *Super Crunchers*[3] :

> *« Les sociétés émettrices de cartes de crédit ne se soucient pas vraiment en tant que tel du divorce de leurs clients, elles se soucient de savoir s'ils vont pouvoir payer leurs dépenses. Et, parce que les gens qui divorcent sont plus susceptibles de connaître des défauts des paiements, les ennuis « domestiques » de leurs clients sont d'un grand intérêt pour des entreprises dont le développement est basé sur la gestion des risques…*[4] *»*

La montée en puissance des objets connectés pourrait ainsi accélérer l'extension du caractère « sensible » à l'ensemble des données recueillies par les capteurs présents dans l'environnement des utilisateurs. Parmi les exemples de déduction (ou d'inférence) de données sensibles à partir d'informations collectées par des objets connectés on pourra citer 5 exemples de ces nouveaux risques.

---

[3] *Super Crunchers: Why Thinking-By-Numbers is the New Way To Be Smart* (Ian Ayres, ed. Bantam, 2007)

[4] *How Visa Predicts Divorce* (The Daily Beast, 4 juillet 2010)
http://www.thedailybeast.com/articles/2010/04/06/how-mastercard-predicts-divorce.html

Capteurs de présence des détecteurs de fumée et troubles du comportement

Les détecteurs de fumée Nest possèdent un capteur de présence qui permet d'allumer une veilleuse lors du passage nocturne sous le détecteur. Cette fonction « annexe » pourrait avoir des conséquences importantes : l'heure et le nombre de passages sous ce capteur pourraient être révélateurs de troubles du comportement ou de pathologies. Ces données une fois soumises à des algorithmes d'analyse du risque, modifier le profil assurantiel d'un utilisateur.

Analyse de la consommation électrique et profilage ethnique ou religieux

L'analyse des schémas de consommation énergétique (avec les compteurs intelligents de type Linky) pourrait aussi être utilisée pour effectuer un profilage ethnique ou religieux des usagers. Ainsi, l'absence ou la diminution de consommation électrique à des périodes précises permettent de déduire si l'utilisateur modifie sa consommation par exemple lors du mois du ramadan ou le vendredi soir et le samedi pour les personnes qui observent le shabbat… Les initiatives européennes qui permettront de transmettre les informations issues des compteurs électriques intelligents vers des sociétés (à l'instar de l'initiative *Green Button* lancée par la Maison Blanche[5]) devront prendre en compte ces nouvelles formes d'analyses des données énergétiques.

Réfrigérateurs intelligents et risques médicaux liés aux habitudes alimentaires

Les nouvelles générations de réfrigérateurs peuvent désormais analyser les quantités de certaines denrées alimentaires ainsi que la nécessité de leur renouvellement[6]. Ces informations permettent de connaître les évolutions du régime alimentaire de leurs usagers et ainsi en déduire certains risques vis-à-vis de pathologies (diabète ou pathologies cardio-vasculaires) ou des modifications du régime alimentaire compatibles avec l'entrée dans la maladie d'Alzheimer…

[5] http://energy.gov/data/green-button

[6] *Behold: Fridge Cam lets you spy on your food while you're not home* (Mashable, 5 janvier 2016) http://mashable.com/2016/01/05/fridge-cam/#iwirTMw5bZq1

Géolocalisation et analyse des déplacements

Si la géolocalisation n'est pas encore considérée en tant que telle comme une donnée « sensible », depuis plusieurs années des juristes envisagent de la faire rentrer dans cette classification pour mieux protéger les utilisateurs[7]. L'un des programmes de la NSA révélés par Edward Snowden porte sur les données de géolocalisations des mobiles au Pakistan. Ce programme baptisé Skynet[8] est basé sur l'utilisation d'algorithmes qui analysent les déplacements des usagers et leur proximité géographique avec des personnes fichées comme terroristes. Ces algorithmes établissent alors un score qui détermine si les drones qui survolent le Pakistan peuvent lancer des missiles vers les personnes considérées comme terroristes. Ces algorithmes sont considérés par la NSA comme efficaces avec un taux de faux positifs estimé à 0,008 %, soit 15 000 personnes pouvant être considérées à tort comme terroristes… Dans un registre moins « extrême » l'analyse des déplacements d'une personne permet d'analyser ses comportements, et les évolutions de ses déplacements peuvent aussi être révélatrices dans les modes de vie, de leur état psychologique ou de leur santé.

Véhicules connectés, capteurs de vigilance et paramètres de conduite9

Les automobiles figurent désormais parmi les objets connectés les plus riches en capteurs (radar, sonar, caméras, accéléromètres, thermomètres, détecteurs d'humidité, etc.) coordonnés par une informatique embarquée de plus en plus puissante. Ce qui faisait dire à Dieter Zetsche, le P.-D.G. de Mercedes-Benz, qu'une voiture était désormais « *un smartphone avec quatre roues autour…* »[10]. À titre d'exemple, le volume d'information généré par les capteurs embarqués dans la voiture connectée Ford Fusion représentait déjà en 2012, 25 Gigaoctets de données par heure de conduite[11]. Désormais, avec la montée en puissance des voitures sans pilotes, ce sont des Téraoctects de données qui sont traitées

---

[7] *Géolocalisation : déclarer les données sensibles pour améliorer leur usage ?* (L'Atelier, 5 avril 2011) http://www.atelier.net/trends/articles/geolocalisation-declarer-donnees-sensibles-ameliorer-usage

[8] *Skynet, le programme ultra-secret de la NSA créé pour tuer* (Le Monde, 20 octobre 2015) http://www.lemonde.fr/pixels/article/2015/10/20/cree-pour-tuer_4792765_4408996.html

[9] *La voiture, cette espionne* (Le Monde, 2 octobre 2015) http://www.lemonde.fr/m-actu/article/2015/10/02/la-voiture-cette-espionne_4781511_4497186.html

[10] *Detroit Motor Show: Car firms take on the tech giants* (BBC News, 13 janvier 2015) http://www.bbc.com/news/business-30786709

[11] *Ford Issues Predictions for Next Wave of Automotive Electronics Innovation* (Washington Times, 27 décembre 2012) http://www.washingtontimes.com/news/2012/dec/27/ford-predicts-next-auto-electronics-innovation/

par les capteurs des véhicules[12]. Si, dans leur majorité, ces capteurs sont dédiés à l'analyse des paramètres de fonctionnement du véhicule, d'autres sont spécifiquement destinés à analyser les paramètres physiologiques du conducteur ou son style de conduite. Ces capteurs pourraient au-delà de l'évaluation de son niveau de vigilance, devenir une source d'information précieuse, notamment sur la santé du conducteur. L'analyse de la conduite a d'ailleurs donné lieu à des expérimentations par des groupes d'assurance afin de moduler les primes (principe du « *Pay How You Drive* »). Il est à noter que jusqu'ici ces expérimentations ont souvent été jugées trop intrusives par les assurés potentiels[13].

Objets connectés et évolutions des structures de soins

Pour Eric Topol, le spécialiste américain des technologies de la santé, c'est l'ensemble des structures de soins qui pourraient bientôt être transformées par l'utilisation croissante des objets connectés :

> *« Exceptés pour certaines fonctions clés comme les soins intensifs et la chirurgie, les hôpitaux seront entièrement transformés en centre de surveillance des données. Les gens souriront en repensant aux visites chez leur médecin avec le légendaire stéthoscope ainsi que l'ensemble des pratiques qui existaient avant l'ère numérique…*[14] *»*

Au-delà des structures de santé actuelles, le parcours de soins sera alors constitué d'objets médicaux connectés qui éviteront aux patients d'avoir à se rendre à l'hôpital ou dans des laboratoires médicaux et permettront un suivi à distance des paramètres de santé ainsi qu'un développement des mesures de prévention. Les données recueillies par ces objets seront utiles aux professionnels de santé et pourraient être précieuses pour les acteurs de l'assurance. À mesure que se développeront ces objets, les conduites à risques pourraient ainsi être sanctionnées économiquement, voire même socialement. À cet égard, le traitement des données médicales pourrait devenir un enjeu politique et économique

[12] *« Les véhicules équipés de caméras 4K parcourent 50 000 kilomètres par semaine et captent 70 000 points de contrôle à la seconde (la forme de la route, les panneaux routiers…). Des teraoctets de données sont ainsi rapatriés quotidiennement pour être analysés. »* *Les nouveaux défis de la cartographie routière pour les voitures autonomes* (Le Monde, 10 mars 2017) http://www.lemonde.fr/pixels/article/2017/03/12/les-nouveaux-defis-de-la-cartographie-routiere-pour-les-voitures-autonomes_5093246_4408996.html

[13] *Assurances auto: êtes-vous prêt à tout dévoiler pour payer moins cher ?* (L'Express, 2 février 2016) http://votreargent.lexpress.fr/high-tech/assurances-auto-etes-vous-pret-a-tout-devoiler-pour-payer-moins-cher_1759408.html

[14] *Eric Topol on the Future of Medicine* (Wall Street Journal, 7 juillet 2014) http://www.wsj.com/articles/eric-topol-on-the-future-of-medicine-1404765024
voir aussi son ouvrage *The Creative Destruction of Medicine (*Eric Topol, Ed. Basic Books janvier 2012)

majeur à la fois pour les citoyens et pour l'ensemble des acteurs impliqués dans la protection sociale.

Si, dans le passé, le développement en France et en Europe d'une couverture mutualisée des risques sociaux répondait à un choix politique, il correspondait aussi à l'absence de technologies permettant la mesure individualisée des risques en particulier dans le domaine de la santé. Or les technologies de suivi et de prévention des risques (qui pourraient s'appuyer bientôt sur l'essor des objets connectés de santé et des outils de génomique de masse [15]) pourraient modifier cet équilibre au profit d'une rationalité économique très différente de celle que nous connaissons aujourd'hui. Ce que M. Demurger, le directeur général de la MAIF[16] résume ainsi :

> *« C'est un renversement complet du monde de l'assurance. Traditionnellement, les assureurs avaient très peu de données sur leurs clients mais un grand nombre de clients. Grâce au big data, nous pouvons désormais récolter un grand nombre de données comportementales sur une seule personne. »*

En plus des contraintes économiques pesant sur l'assurance maladie (en raison de la montée en puissance des coûts des examens complémentaires ou des instruments thérapeutiques), l'usage des objets de santé connectés dédiés au diagnostic mais aussi à la prévention des pathologies pourrait transformer l'économie de la santé. Les acteurs du secteur prudentiel pourraient ainsi déplacer le centre de gravité de l'économie de la santé vers la prévention[17]. De plus, la tentation pour les acteurs du secteur prudentiel d'orienter la société vers une couverture hyper-individualisée sera d'autant plus grande qu'elle répondra à un double impératif d'efficacité médicale et d'économie générale pour les acteurs de la santé.

---

[15] Voir sur ce point la législation actuellement étudiée aux États-Unis sur l'obligation qui serait faite aux employés américains de subir des tests génétiques sous peine de sanctions économiques.
Employees who decline genetic testing could face penalties under proposed bill (Washington Post, 11 mars 2017)
https://www.washingtonpost.com/news/to-your-health/wp/2017/03/11/employees-who-decline-genetic-testing-could-face-penalities-under-proposed-bill/

[16] *Santé: faut-il faire payer les assurés en fonction de leur mode de vie ?* (Le Monde, 6 septembre 2016)
http://www.lemonde.fr/economie/article/2016/09/06/assurance-votre-vie-privee-vaut-bien-une-ristourne_4993378_3234.html

[17] *« Une nouvelle étude publiée dans la revue JAMA Oncology estime qu'en appliquant des connaissances que nous avons depuis des décennies (ne pas fumer, boire avec modération, maintenir son poids corporel sain et faire de l'exercice), plus de la moitié des décès par cancer pourraient être évités et les nouveaux cas de cancers pourrait baisser dans une proportion de 40 à 60 %. »*
Scientists have determined how we can prevent half of all cancer deaths (Washington Post, 19 mai 2016)
https://www.washingtonpost.com/news/wonk/wp/2016/05/19/scientists-have-determined-how-we-can-prevent-half-of-all-cancer-deaths/

En raison de leur impact sur nos modes de vie, les évolutions technologiques sont aussi susceptibles de remettre en cause certains de nos droits fondamentaux, qu'il s'agisse de notre droit à la protection de nos données personnelles, du droit au respect de la vie privée ou encore de la liberté de déplacement, de la liberté d'information ou encore de la non-discrimination.
Ces évolutions, loin de n'être que technologiques ou économiques, auront aussi des conséquences sociales et politiques majeures. Afin que les citoyens puissent décider des formes que devront prendre les structures de soins et plus largement l'ensemble des dispositifs de la protection sociale, ces évolutions devront donc faire l'objet d'un véritable débat démocratique dans nos sociétés.

Quelle acceptabilité sociale pour les objets connectés ?

L'échec industriel des Google Glass

Le rejet des objets connectés constitue déjà un risque pour la diffusion de ces objets et l'une des modalités « sociales » de la régulation de ce secteur. L'un des produits emblématiques de cette tendance correspondait aux lunettes à réalité augmentée Google Glass. Un spécialiste de l'ergonomie sur Internet a analysé les risques que ces lunettes constituaient pour une société où ces lunettes deviendraient chose commune[18] :

> *« Tout d'abord, imaginez les flux vidéo de chacune des Google Glass, dans le monde entier. Que la vidéo ne soit enregistrée que temporairement, comme dans la version actuelle, ou en permanence, comme cela sera certainement possible dans de futures versions, tous ces flux vidéo seront envoyés sur les serveurs cloud de Google. Ajoutez à cela la reconnaissance faciale reliée à la base de d'identité de Google Plus (qui contient les identités réelles des personnes) : Il sera alors possible aux serveurs de Google de traiter des fichiers vidéo, pour identifier toutes les personnes qui y figurent. Et si Google Plus ne semble pas suffisant, Mark Zuckerberg a déjà promis que Facebook développerait des applications pour le Google Glass. Enfin, considérons le logiciel que Google emploie déjà pour la reconnaissance de la parole, à la fois dans ses serveurs et sur les Google Glass elles-mêmes. Toutes les bandes-son des vidéos*

[18] *The Google Glass feature no one is talking about* (Creative Good, le 28 février 2013)
http://creativegood.com/blog/the-google-glass-feature-no-one-is-talking-about/

pourraient être converties en texte, associées aux personnes qui ont parlé, et par la suite devenir intégralement consultables par le moteur de recherche de Google… »

La crainte suscitée par la mise en place d'une surveillance croisée des personnes à proximité des porteurs de ces lunettes a été à l'origine d'une intense campagne de lobbying « Anti-Glass » organisée par les associations de protection des libertés individuelles aux États-Unis. Google a été par la suite contraint d'annoncer au début 2015 la fin anticipée du projet Glass et ce avant même les débuts de la commercialisation auprès du grand public…[19]. Il est à noter que la controverse autour des Google Glass a commencé quelques mois avant les révélations d'Edward Snowden, mais que les raisons évoquées par ses détracteurs ne se limitaient pas aux seuls risques liés à la surveillance de masse. Pour les usagers, il s'agissait d'un objet qui remettait directement en cause des normes sociales établies en matière de communication interpersonnelle[20].

Le plébiscite des Adblocks

Le refus par les usagers de l'Internet de certaines pratiques ou de certaines architectures techniques peut parfois être à l'origine de contre-réactions radicales. Face au caractère intrusif des publicités qui venaient perturber leur expérience de navigation sur le Web (en particulier sur les mobiles), les usagers ont plébiscité le développement d'une nouvelle génération des logiciels de blocage des fenêtres et bandeaux publicitaires (AdBlocks). Cette tendance a été telle qu'elle a inquiété les acteurs de la publicité les incitants à reconnaître via leurs représentants qu' « *ils avaient négligé l'expérience utilisateur au profit de gains à court terme…* »[21].

Les préoccupations liées à la protection de la vie privée mais aussi à l'évolution de nos sociétés (en particulier avec l'hyperindividualisation de la couverture des risques)

---

[19] Marc Rotenberg, le président du l'Electronic Privacy Information Center déclarait à ce propos : *" Du point de vue du respect de la vie privée, nous sommes évidemment heureux de voir Google arrêter ce produit, et ce n'est pas rien de voir Google reculer, en particulier après l'immense campagne marketing lancée pour les Google Glass… "*
A Retreat for Google Glass and a Case Study in the Perils of Making Hardware (New York Times, 18 jan 2015)
http://bits.blogs.nytimes.com/2015/01/18/a-retreat-for-google-glass-and-a-case-study-in-the-perils-of-making-hardware/

[20] *Did Edward Snowden Ruin Google Glass?* (Motherboard Vice, 4 janvier 2014) http://motherboard.vice.com/blog/did-edward-snowden-ruin-google-glass

[21] *IAB to Advertisers and Content Providers: 'We Messed Up'* (Advertising Age, 15 octobre 2015) http://adage.com/article/digital/iab-advertisers-content-providers-messed/300919/

pourraient pousser les opinions publiques européennes à favoriser le développement de nouvelles générations d'objets connectés qui ne généreront pas les mêmes effets de bord sociaux, économiques ou politiques.

Vers une « invisibilité » des objets connectés

Si des réactions sociales *a posteriori* (après la création d'un objet connecté) peuvent exister pour des objets « visibles » dans le champ social, à terme la plupart des objets et des services utilisant des capteurs seront « invisibles ». Susciteront-ils autant de levées de boucliers dans la mesure où ils n'apparaîtront pas comme des obstacles à la communication entre les usagers mais plutôt comme autant d'outils d'aides à la décision ? Ainsi, un quart de siècle après Mark Weiser et son texte visionnaire sur les technologies qui « disparaissent », le P.-D.G. de Google Sundar Pichai énonce les transformations de l'Internet des objets en ces termes[22] :

> « *La prochaine grande étape des technologies correspondra à la disparition des appareils eux-mêmes… Au fil du temps, l'ordinateur - quelle que soit sa forme - deviendra un assistant intelligent qui vous aidera tout au long de votre journée… Nous allons passer de l'ère du mobile à l'ère de l'Intelligence Artificielle…* ».

À mesure que le fonctionnement des objets connectés reposera sur des algorithmes dont certaines des fonctions pourraient être de plus en plus cruciales dans notre vie quotidienne, la demande de transparence vis-à-vis de ces algorithmes deviendra de plus à plus importante. Dans son ouvrage *The Black Box Society*[23] Frank Pasquale prévoit que le besoin de transparence vis-à-vis du « Code » et sa manière de traiter nos données personnelles pourrait bientôt devenir un impératif pour les sociétés démocratiques.

En France, la loi pour une République numérique publiée le 8 octobre 2017, introduit un droit à la transparence des algorithmes utilisés par l'administration[24]. Ce droit signifie que chaque citoyen doit être systématiquement informé via une mention d'information qu'un algorithme a été utilisé par une administration afin de prendre une décision le concernant. À sa demande, l'administration concernée doit lui communiquer les règles définissant le

[22] *Google : Lettre des Fondateurs* (Sundar Pichai, *28 avril 2016)*
https://googleblog.blogspot.fr/2016/04/this-years-founders-letter.html

[23] *The Black Box Society* (Harvard University Press, janvier 2015)

[24] Art. L. 312-1-3 de la Loi n° 2016-1321 pour une République numérique
https://www.legifrance.gouv.fr/eli/loi/2016/10/7/ECFI1524250L/jo/texte

fonctionnement du logiciel algorithmique ainsi que ses principales caractéristiques. Au-delà des administrations, cette transparence devra pouvoir s'étendre aux traitements algorithmiques de l'ensemble des services utilisés par les citoyens en particulier dans les domaines de l'information[25], des transports[26] et plus encore de la santé.

Des architectures centralisées vulnérables en termes de sécurité

Vers de nouvelles architectures ?

Les smartphones sont désormais perçus par leurs utilisateurs comme une extension d'eux-mêmes et deviennent en quelque sorte leurs « exo-cerveaux ». Il en va de même aujourd'hui avec les objets connectés dont les capacités de mémoire et de traitement sont souvent transférées aux terminaux mobiles. Cette division des tâches permet de concevoir des objets plus économiques qui disposent du minimum d'intelligence et d'énergie nécessaires à leur fonctionnement. Les données recueillies sont alors transmises à des structures de stockage de masse (de type « cloud computing ») qui permettent de bénéficier d'une puissance de traitement considérable à coût réduit. Cette architecture centralisée d'objets « modérément intelligents » connectés à des terminaux puissants et à des infrastructures distantes pour le stockage et le traitement des informations répond à une logique économique ainsi qu'à de nombreuses possibilités de valorisation des données. Cependant, on perçoit les risques que représentent ces architectures en termes de sécurité et de confidentialité des données ainsi qu'en termes d'évolution des modèles économiques de l'Internet des objets.

À la différence de l'immense majorité des produits industriels traditionnels, les objets connectés dépendent de la connexion vers les serveurs de leurs constructeurs pour fonctionner correctement. Ainsi, en cas d'arrêt d'activité de la société qui a conçu le produit, l'objet cesse lui aussi de fonctionner. En ce sens, il n'a de valeur pour son acquéreur qu'aussi longtemps qu'il est « supporté » par le constructeur. En plus des risques d'obsolescence ou de « mort programmée », cette particularité pose aussi des problèmes de sécurité. En effet, lorsque le logiciel interne d'un objet (ou micrologiciel)

[25] *You may hate Donald Trump. But do you want Facebook to rig the election against him?* (The Guardian, 19 avril 2016) https://www.theguardian.com/commentisfree/2016/apr/19/donald-trump-facebook-election-manipulate-behavior
[26] *Le dilemme macabre des voitures autonomes* (Le Monde, 23 juin 2016) http://www.lemonde.fr/sciences/article/2016/06/23/tuer-un-pieton-ou-sacrifier-le-passager-le-dilemme-macabre-des-voitures-autonomes_4956924_1650684.html

n'est plus mis à jour, cet objet devient encore plus vulnérable aux cyber-attaques et aux intrusions. L'autre caractéristique essentielle de l'architecture des objets connectés est liée à leurs modes de communication. La plupart des objets possèdent une architecture qui établit une double transmission des informations vers l'utilisateur (le plus souvent vers leurs terminaux mobiles) et vers le traitement des données en « cloud ». Cette architecture crée une double vulnérabilité en termes de captation des données ainsi qu'en termes de prise de contrôle possible de ces objets connectés lors de piratages.

Sécurité : le maillon faible des objets connectés

La sécurité des objets connectés fait désormais partie intégrante de la réflexion sur la protection des données personnelles. En plus d'être une préoccupation majeure pour les citoyens, elle est aussi devenue un enjeu de sécurité nationale pour les États[27]. Les technologies et les services liés à la sécurité des objets connectés constituent un marché essentiel pour l'ensemble des acteurs des technologies[28]. Or la sécurité de ces objets reste pour l'instant rudimentaire. De l'absence de mécanismes de chiffrement pour la transmission des données[29], jusqu'à l'impossibilité d'intégrer des mises à jour de sécurité, la sécurité des objets connectés constitue aujourd'hui l'un des maillons les plus faibles des infrastructures de l'Internet. Dans certains secteurs, liés à la sécurité des personnes (comme celui de la santé), ces failles deviennent même critiques. Ainsi, David Talbot dans la revue MIT Technology Review rappelle que *« La présence de virus informatiques est devenue endémique dans les appareils médicaux connectés des hôpitaux… »*[30].

Il est à noter que c'est la constatation d'une vulnérabilité « endémique » des objets connectés qui a décidé la NSA à financer le développement de systèmes de sécurité pour les objets connectés et leurs systèmes de stockage d'informations sur le Cloud par

[27] *The CIA Fears the Internet of Things* (Defense One, 24 juillet 2014)
http://www.defenseone.com/technology/2014/07/cia-fears-internet-things/89660/

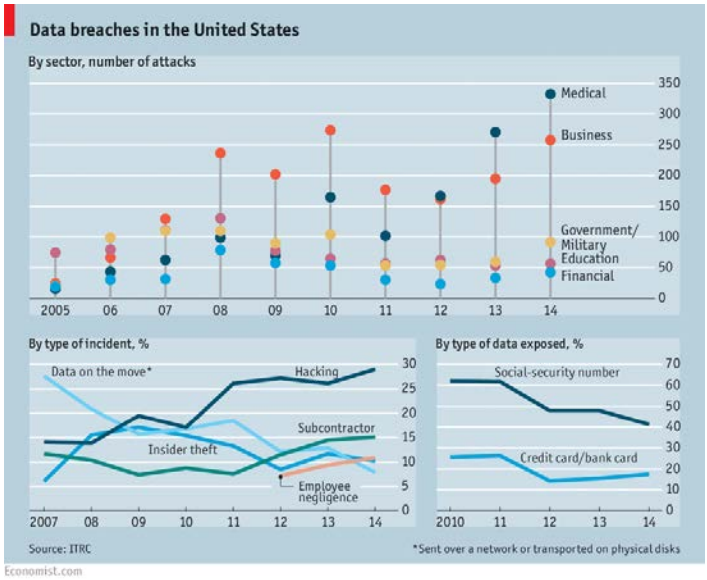
[28] *How the 'insecurity of things' creates the next wave of security opportunities* (TechCrunch 26 juin 2016)
https://techcrunch.com/2016/06/26/how-the-insecurity-of-things-creates-the-next-wave-of-security-opportunities/

[29] In*ternet of Things Security Study : Smartwatches* (Étude Hewlett Packard Entreprise)
http://go.saas.hpe.com/l/28912/2015-07-20/325lbm/28912/69038/IoT_Research_Series_Smartwatches.pdf

[30] *Computer Viruses Are "Rampant" on Medical Devices in Hospitals* (MIT Technology Review, 17 octobre 2012)
https://www.technologyreview.com/s/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals/

l'Université d'Alabama [31]. Cette préoccupation de sécurité répond à une double injonction : assurer de manière « défensive » la résilience de l'Internet des objets américain en cas d'attaque ou d'intrusion et probablement aussi veiller à ce que les solutions de sécurité développées par les industriels puissent inclure des dispositifs de portes dérobées pour faciliter les travaux d'enquêtes ou de surveillance. Or, comme le rappelle l'expert en cybersécurité Bruce Schneier[32], une des plus grandes erreurs que pourraient commettre les pays développés serait de créer volontairement ces failles de sécurité qui seront nécessairement découvertes par des hackers malveillants.

Des préoccupations de même nature avaient déjà été à l'origine du conflit juridique autour de la puce de chiffrement *Clipper Chip*. Développée par la NSA, cette puce devait être intégrée de manière obligatoire à l'ensemble des ordinateurs produits aux États-Unis afin de sécuriser les échanges mais aussi, le cas échéant, permettre l'accès aux ressources de ces ordinateurs par les agents de la NSA. Ce projet a été définitivement abandonné en 1996 après que des hackers sont venus à bout de sa sécurité. Cette puce avait aussi été accusée de contrevenir au premier amendement de la Constitution américaine relatif à la liberté d'expression.



Évolution des cyberattaques par secteur d'activité aux États-Unis
(The Economist, 7 novembre 2015)

[31] *UAH developing architecture to build design-phase cybersecurity into systems (6 aout 2015)*
http://www.uah.edu/news/research/uah-developing-architecture-to-build-design-phase-cybersecurity-into-systems
[32] *Data and Goliath* (Bruce Schneier, Ed. Norton & Company 2015)

La codification des mesures de sécurité des objets connectés et plus largement du traitement des données issues de ces objets constitue désormais un enjeu crucial en termes de protection des libertés mais aussi en termes de confiance pour l'ensemble des acteurs des technologies. À mesure que se développent de nouvelles formes de cyberattaques basées sur les objets connectés, le devenir économique de cette filière pourrait dépendre de la capacité des industriels européens à développer des solutions de sécurité qui protégeront à la fois les données issues de ces objets ainsi que leurs utilisateurs. En ce sens, les dispositifs de codification de la sécurité des objets connectés pourraient constituer un volet essentiel des politiques industrielles européennes permettant d'assurer le développement de ce secteur technologique.

II / L'INDISPENSABLE SYNERGIE ENTRE REGULATION ET POLITIQUE INDUSTRIELLE

La régulation actuelle et ses limites

L'Union européenne a adopté ou publié plusieurs textes fondamentaux sur la régulation de la protection des données personnelles, données générées entre autres par les objets connectés. On note en particulier la directive de 1995 sur la protection des données personnelles et la directive de 2002 sur le traitement des données à caractère personnel et la protection de la vie privée (dite directive ePrivacy)[33]. La première sera remplacée par le Règlement Général de l'Union européenne sur la Protection des Données (RGPD)[34] applicable à partir du 25 mai 2018[35] ; la seconde, est en cours de révision. Or, ces dernières années, le paysage technologique a radicalement évolué, avec la montée en puissance des solutions de cloud computing, souvent reliés aux systèmes de capteurs.

Le RGPD introduit ainsi le principe d'une protection des données dès la conception (Privacy by Design) et de protection des données par défaut (Privacy by Default)[36]. Cela

[33] 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.
http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32002L0058&from=FR
[34] Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
http://eur-lex.europa.eu/legal-content/fr/TXT/PDF/?uri=CELEX:32016R0679
[35] https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels
[36] Art. 25 RGPD.

signifie que le responsable du traitement doit adopter, en amont, dès qu'il envisage de collecter des données, des mesures « *destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données* ». Ces mesures, comme la pseudonymisation et l'anonymisation des données, seront déterminées en fonction de l'état des connaissances ainsi que de leurs coûts de mise en œuvre. Elles doivent également tenir compte du degré de probabilité et de gravité des risques. Dans ce domaine, la détermination du périmètre d'utilisation de ces technologies est laissée à l'appréciation des acteurs en fonction d'une analyse au cas par cas. Or, comme le rappellent les documents stratégiques de la Commission européenne sur l'Internet des Objets, les questions relatives à la mise en œuvre des solutions de sécurité sophistiquées basées sur la cryptographie restent encore à déterminer[37]. La capacité des entreprises européennes à développer ces solutions de sécurité à grande échelle (et les intégrer de manière ergonomique dans les objets et services de l'Internet des Objets) pourrait se révéler cruciale pour l'ensemble de la filière européenne des technologies.

Parmi les nouveautés adoptées par le RGDP, figurent également « *l'encouragement* » à la mise en place de codes de conduite[38] et « *des mécanismes de certification en matière de protection des données ainsi que de labels et de marques* »[39]. À l'instar des étiquettes-énergie qui résument les performances énergétiques et permettent de guider le choix des consommateurs, une certification de conformité basée sur le RGPD ou un label de confiance (*Trusted IoT*) pour les objets connectés développés par les acteurs du secteur à destination du grand public pourrait être créée afin d'assurer la transparence sur les différents niveaux de confidentialité et de sécurité. De leur côté, les services de la Commission envisagent de réfléchir à un dispositif de certification des objets connectés[40] qui disposeraient de technologies d'authentification sécurisée, depuis le matériel jusqu'aux couches réseau. Ce dispositif de certification nécessitera de la part des constructeurs une analyse des fonctions de chaque objet ainsi qu'un traitement sécurisé des données.

---

[37] "Advancing the Internet of Things in Europe", accompanying the document "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Digitising European Industry - Reaping the full benefits of a Digital Single Market COM(2016) 180" (publié le 19 avril 2016)
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0110&from=EN

[38] Art. 40 du RGPD.

[39] Art. 42 du RGPD.

[40] *« The Commission services consider important to reflect upon possibilities for certification of networked devices that would provide a minimum level of secure authentication, from the hardware level to network integrity. This would entail some analysis of the functions with which each device is equipped, secure data processing and secure connectivity for the devices to which data are transmitted. »*
Advancing the Internet of Things in Europe (page 31)
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0110&from=EN

Pour sa part, la proposition de règlement concernant le respect de la vie privée et la protection des données à caractère personnel (*« ePrivacy draft regulation »*[41]) mentionne explicitement l'Internet des Objets dans son champ de régulation et, en particulier, la communication de machine à machine[42] (M2M). Cependant, ce texte ne s'applique qu'à l'industrie des communications électroniques ce qui signifie, qu'en l'état il ne couvre pas l'ensemble du secteur de l'Internet des objets.

La philosophie générale de ces textes s'inscrit dans la continuité des actions de la Commission qui promeuvent une approche de « régulation non intrusive » vis-à-vis des acteurs industriels. Cependant, la position de fragilité des acteurs européens dans la compétition internationale dans les segments stratégiques de l'Internet des Objets (Big Data, Cloud Computing, plateformes mobiles, objets connectés de santé, Smart Grids…) pourrait nécessiter désormais une réévaluation des dispositifs européens qui ont été mis en œuvre jusqu'alors et qui n'ont pas permis d'accompagner l'émergence d'acteurs de taille mondiale. À cet égard, la protection des données personnelles et plus largement la protection des données des entreprises peuvent désormais devenir des facteurs de compétitivité essentiels pour les pays de l'Union. Si un consensus existe quant à la nécessité de la prise en compte de la protection des données personnelles dès la conception des objets connectés, les modalités de mises en œuvre juridiques et surtout technologiques de cette protection restent à formaliser. Les modèles économiques des objets connectés (et donc de leurs données) pourraient ainsi être amenés à évoluer à mesure que les préoccupations liées à la protection de la vie privée monteront en puissance sous la pression conjuguée des usagers, des pouvoirs publics et des industriels pour lesquels ces préoccupations deviendront stratégiques.

---

[41] Proposition de Règlement du Parlement Européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques») http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241

[42] *Connected devices and machines increasingly communicate with each other by using electronic communications networks (Internet of Things). The transmission of machine-to-machine communications involves the conveyance of signals over a network and, hence, usually constitutes an electronic communications service. In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, it is necessary to clarify that this Regulation should apply to the transmission of machine-to-machine communications. Therefore, the principle of confidentiality enshrined in this Regulation should also apply to the transmission of machine-to-machine communications. Specific safeguards could also be adopted under sectorial legislation, as for instance Directive 2014/53/EU.*
Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (p 13 et 14)

De nouvelles mesures technologiques et juridiques pourraient être envisagées au niveau européen pour veiller en particulier à ce que les usagers gardent le contrôle sur les informations qui seront captées et transmises par ces objets.

Pour une codification du « droit au silence des puces »

La désactivation temporaire ou définitive des objets connectés est à la fois à un enjeu juridique et industriel. S'il est relativement simple de désactiver un objet électronique élaboré, comme un smartphone, il en va tout autrement lorsqu'il s'agit d'une puce RFID utilisée pour « taguer » un objet industriel ou une denrée alimentaire…

Ces puces, qui permettent d'assigner un identifiant à un objet, sont pour les plus simples d'entre elles dotées d'un processeur rudimentaire et d'une antenne qui permet l'activation du processeur via une brève impulsion électromagnétique. Leur fonction est de répondre à cette impulsion en déclinant la série de chiffres codés sur le processeur. Issues du monde de la distribution où leur utilité ne pouvait exister au-delà du point de vente, ces puces RFID pourraient devenir un maillon essentiel des services de l'Internet des objets, par exemple pour transmettre des informations à un appareil électroménager (réfrigérateur, four à micro-ondes ou encore lave-linge…). Leur prix unitaire est de quelques centimes d'euros et elles ne contiennent ni source d'énergie interne (qui pourrait s'épuiser), ni pièces mobiles (qui pourraient s'user), ce qui les rend particulièrement durables. De plus, pour la plupart, ces puces RFID ne contiennent ni mécanismes de désactivation, ni mécanismes de chiffrement ou dispositifs de sécurité. Intégrer ces mécanismes pour protéger ces puces contre des interrogations issues d'utilisateurs indélicats (aussi appelées « skimming ») ou chiffrer les données pour éviter qu'une donnée sensible issue par exemple d'un produit médical ne puisse être captée frauduleusement pourrait représenter un surcoût significatif pour les acteurs industriels.

Si les puces RFID ont parfois été expérimentées en remplacement des codes-barres pour les objets de grande consommation, elles n'ont pas été largement déployées jusqu'ici par les acteurs de la distribution en raison de leur coût unitaire. Ce surcoût ne pouvant être assumé par les producteurs ou distributeurs de ces objets que s'il correspond à un service valorisable durant l'ensemble de la vie d'un objet (jusqu'à son recyclage) et pas si (comme c'est le cas aujourd'hui) l'identifiant présent sur le code-barres sert essentiellement aux acteurs de la logistique et accessoirement à établir des comparaisons de prix sur mobile.

Le concept du "*Droit au Silence des Puces*" a été élaboré en 2006[43] dans le but de permettre aux usagers de maîtriser les informations issues des puces à radiofréquences (RFID). Ce droit a pour objectif de placer le citoyen usager en situation de maîtrise des données qui seront échangées à partir de ces objets présents dans son environnement. Il implique en particulier que soient inclus dès la conception de ces dispositifs connectés des dispositifs de désactivation/réactivation associé à des dispositifs de chiffrement pour les données sensibles, en particulier les données médicales ou les données relatives à la sécurité des personnes. Pour autant, ce droit au « Silence des Puces » n'est toujours pas codifié, qu'il s'agisse d'une codification dans les textes juridiques ou dans l'architecture de ces technologies (dans une démarche de « Privacy by Design »).

Le droit au silence des puces a été évoqué à l'origine en mai 2008 lors de la première réunion ministérielle européenne sur l'Internet des Objets [44], puis repris par la Commission européenne[45] [46], le Parlement européen[47] et le Conseil des ministres des télécoms de l'UE. Le droit au silence des puces est également cité par le Conseil d'État dans son rapport de 2014 « *Le numérique et les droits fondamentaux* »[48], qui l'envisage comme l'une des pistes de réflexion pour l'avenir de l'Internet des Objets. Cependant, il n'a

[43] Le concept de « *Droit au silence des puces* » a été introduit dans le texte *Architecture et Gouvernance de l'Internet* paru dans la revue Esprit (Bernard Benhamou, mai 2006).
http://www.netgouvernance.org/ArchitectureEsprit.pdf
Il a par la suite été détaillé et formalisé dans le texte « *Les Mutations Economiques, Sociales et Politique de l'Internet des Objets* » (Bernard Benhamou, Cahiers de la Documentation Française, janvier 2013).
http://www.netgouvernance.org/IOT%20Cahiers%20DOC%20FRANCAISE.PDF

[44] « *Internet des objets, Internet du futur* » conférence ministérielle européenne organisée dans le cadre de la Présidence Française de l'Union Européenne (Nice 2008).

[45] *The right to the "silence of the chips". The Commission will launch a debate about whether individuals should be able to disconnect from their networked environment at any moment. Citizens should be able to read basic RFID (Radio Frequency Identification Devices) tags – and destroy them too – to preserve their privacy. Such rights are likely to become more important as RFID and other wireless technologies become small enough to be invisible.*
(*Europe prepares for the internet revolution* European Action Plan, 18 juin 2009)
http://europa.eu/rapid/press-release_IP-09-952_en.htm

[46] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:FR:PDF

[47] *Motion For A European Parliament Resolution On The Internet Of Things* (Committee on Industry, Research and Energy, Rapporteur: Maria Badia i Cutchet, 10 mai 2010).
http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2010-0154&language=EN

[48] *Le numérique et les droits fondamentaux* (Étude annuelle 2014 du Conseil d'Etat, septembre 2014).
http://www.ladocumentationfrancaise.fr/docfra/rapport_telechargement/var/storage/rapports-publics/144000541/0000.pdf

encore fait l'objet d'aucune mise en œuvre législative. Parmi les réserves émises par les industriels européens et américains figurent des interrogations sur la modification de l'équilibre économique que ces mesures pourraient engendrer. Si les fabricants de puces RFID étaient contraints par voie légale d'intégrer des dispositifs de sécurité ainsi que des mécanismes de désactivation/réactivation, cela entraînerait nécessairement un surcoût. Se pose donc ici la question d'un arbitrage entre le développement de nouvelles filières industrielles et la nécessaire protection des données personnelles des citoyens européens. Or la montée en puissance des risques liées à la sécurité des objets connectés et la prise en compte par les usagers de nouveaux risques sur leurs données personnelles pourraient modifier les conditions de cet arbitrage. Cela d'autant plus que les objets connectés via des puces RFID pourraient surpasser en nombres l'ensemble des autres types d'objets connectés. La désactivation sélective des appareils électroniques pour des motifs juridiques suscite aussi de nouvelles interrogations sur le niveau de contrôle réel que possédera l'usager sur ses objets connectés. Ainsi, la société Apple a récemment déposé un brevet[49] qui permettrait la prise de contrôle à distance des terminaux mobiles, par exemple par les responsables d'un lieu public, afin d'éviter que les spectateurs ne puissent activer leur caméra dans des lieux comme des salles de concert.

Quelles perspectives technologiques pour la protection des données ?

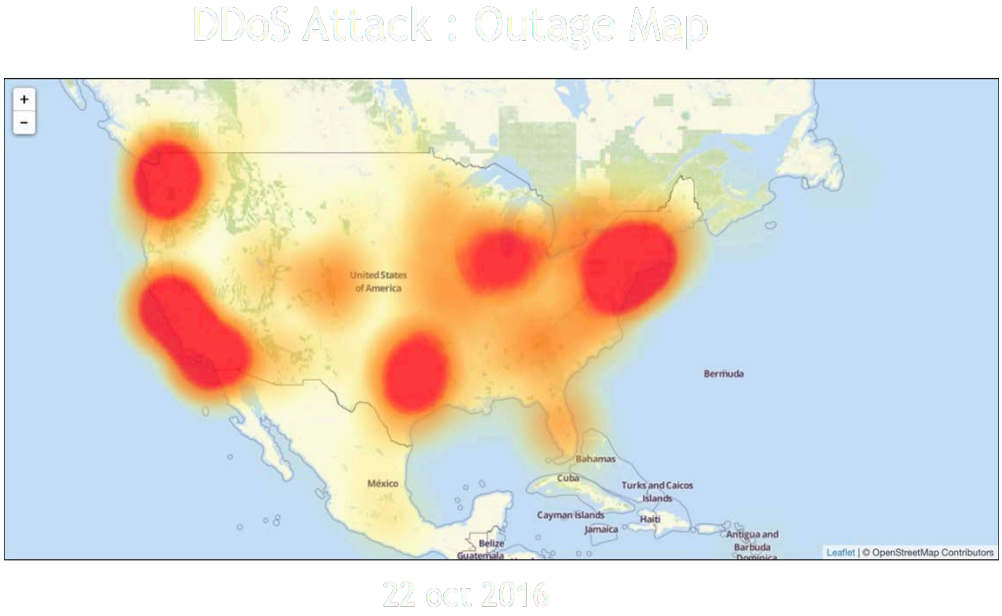
Il convient désormais d'étudier les perspectives liées aux évolutions actuelles de l'Internet des Objets. La collecte des informations personnelles via les objets connectés devra être analysée sous deux angles ; en amont à la fois en fonction des risques que feraient courir ces dispositifs en matière de liberté individuelle, mais aussi en aval en fonction des risques d'attaques de ces objets. Si nous venons d'assister à la première attaque massive de l'Internet via les objets connectés utilisés comme vecteurs d'attaques en déni de service (DDoS[50]), la prochaine génération d'attaques pourrait cette fois utiliser les objets connectés comme vecteur d'attaque non pas contre les ordinateurs mais bien contre les personnes elles-mêmes (qu'il s'agisse d'attaques sur les objets connectés médicaux, les voitures connectées ou encore les infrastructures énergétiques…[51]).

---

[49] *Apple Wins a Patent for an Infrared Camera System that Originally Caused Some Controversy* (PattentlyApple, 28 juin 2016) http://www.patentlyapple.com/patently-apple/2016/06/apple-wins-a-patent-for-an-infrared-camera-system-that-originally-caused-some-controversy.html

[50] http://motherboard.vice.com/read/blame-the-internet-of-things-for-destroying-the-internet-today

[51] *Sécurité et IoT : pourquoi le pire est encore à venir (*Silicon.fr 2/11/2016*)* http://www.silicon.fr/securite-iot-encore-rien-vu-161630.html



Carte de l'attaque par déni de service (DDoS) du 21 octobre 2016[52]

Au-delà de la protection des données, la sécurité pourrait constituer un nouveau motif pour instaurer une désactivation (temporaire ou définitive) des objets connectés. À mesure que ces objets seront présents dans la durée dans l'environnement des usagers, certains d'entre eux cesseront d'être supportés par les entreprises qui les auront conçus. Or, avec ce défaut de mise à jour de sécurité, ce sont de nouveaux risques d'attaques qui pourraient être diffusées à l'ensemble des objets ainsi « fragilisés ». Désormais, à la possibilité d'une désactivation de l'objet pourrait être associée une obsolescence programmée des objets connectés[53]. L'utilisation de solutions « open source » pourrait aussi figurer parmi les mesures permettant une meilleure prise à compte des aspects de sécurité des objets connectés. La complexité des objets connectés vis-à-vis de leurs équivalents traditionnels nécessitera aussi que soient précisées les conditions technologiques et juridiques[54] dans lesquelles les données pourront être transmises[55].

[52] *A massive cyberattack knocked out major websites across the internet* (Business Insider, 21 octobre 2016) http://www.businessinsider.fr/us/amazon-spotify-twitter-github-and-etsy-down-in-apparent-dns-attack-2016-10/

[53] *Why Gadgets in the Internet of Things Must Be Programmed to Die* (Wired, 23 mai 2014) http://www.wired.com/2014/05/iot-death/

[54] *When Everything Works Like Your Cell Phone* (The Atlantic, 28 septembre 2014) http://www.theatlantic.com/technology/archive/2014/09/when-everything-works-like-your-cell-phone/379820

[55] *The Internet Of Someone Else's Things* par Jon Evans (TechCrunch, le 11 octobre 2014) http://techcrunch.com/2014/10/11/the-internet-of-someone-elses-things

Des architectures à la fois plus sûres pour les objets connectés et plus protectrices pour la confidentialité des données de leurs utilisateurs pourraient être spécifiquement développées en Europe. Ces architectures alternatives pour les objets connectés sont parfois envisagées en particulier pour des raisons de sécurité, avec l'intégration de systèmes de chiffrement et de traitement des données entre les utilisateurs eux-mêmes et pas sur des serveurs distants, ces initiatives des concepteurs d'objets connectés restent pour l'instant minoritaires.

À terme, la sécurité de nos sociétés pourrait davantage reposer sur le renforcement des technologies de protection des données et donc sur une plus grande « opacité » des données. Pour le juriste Lawrence Lessig[56], les prochaines étapes de la régulation de la vie privée passeront davantage par le développement de nouvelles générations de technologies de chiffrement des données que par les seules mesures d'encadrement de l'utilisation des données. L'un des exemples de ces technologies est le projet Enigma[57] mené par le MIT qui se propose d'utiliser les technologies de chiffrement de la Blockchain pour protéger l'utilisation des données personnelles. Cependant, comme l'a démontré le récent piratage de la plateforme DAO (Decentralized Autonomous Organization) qui utilise la crypto-monnaie *Ether*[58], les technologies de la Blockchain pourraient être remises en cause. Ce piratage est intervenu au cœur de la technologie de sécurité du projet et rappelle la fragilité d'un dispositif économique dont le « code » est largement accessible. Ce piratage a aussi remis en lumière les origines des algorithmes de sécurité de la Blockchain qui ont été conçus par la NSA[59] et en particulier le risque que des failles (ou portes dérobées) aient été codées en leur sein. Or, comme le prévient Patrick Murck, du Berkman Center for Internet & Society à Harvard : *« Vous ne pouvez pas « coder » votre irresponsabilité légale…[60] ».*

---

[56] *Lawrence Lessig: Technology Will Create New Models for Privacy Regulation* (Wall Street Journal, 30/12/15) https://blogs.wsj.com/cio/2015/12/30/lawrence-lessig-how-technology-policy-will-evolve/

[57] http://enigma.media.mit.edu

[58] *A Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency* (New York Times, 17 juin 2016) http://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html

[59] *What Do the Latest NSA Leaks Mean for Bitcoin?* (Motherboard Vice, 12 septembre 2013) http://motherboard.vice.com/blog/what-do-the-latest-nsa-leaks-mean-for-bitcoin

[60] *A Venture Fund With Plenty of Virtual Capital, but No Capitalist* (New York Times, 22 mai 2016) http://www.nytimes.com/2016/05/22/business/dealbook/crypto-ether-bitcoin-currency.html

D'autres mécanismes de protection des données personnelles pourraient être mis en place pour que les informations puissent être utilisées uniquement pendant une durée déterminée. Certaines données pourraient ainsi être « encapsulées » au sein d'une architecture logicielle et se voir attribuer une date de péremption[61]. Ces technologies de « l'effacement programmé », qui ont été évoquées dans un premier temps pour assurer le droit à l'oubli des utilisateurs, pourraient être utilisées pour éviter que des données personnelles ne puissent être stockées (et traitées) indéfiniment par les sociétés ou les États.

En plus de permettre une meilleure protection de la vie privée des citoyens européens, établir une stratégie à la fois juridique et industrielle sur la protection de la sécurité des données issues des objets connectés constituera aussi une opportunité de développement pour les acteurs européens des technologies. Ce que Paul Nemitz, le directeur du département juridique de la Commission européenne[62] évoque en ces termes :

> *« Il est probable qu'à l'avenir les utilisateurs du monde numérique demanderont une meilleure protection de la vie privée et des données personnelles. Comme cela a été le cas avec le mouvement pour l'écologie, qui a commencé en Europe et qui a conduit l'industrie européenne à des gains de compétitivité, mais qui s'est heurté au début dans les années soixante-dix et quatre-vingt à des résistances, il est très possible qu'avec la protection des données nous soyons confrontés à un mouvement similaire qui partira d'Europe… »*

Développer en Europe un écosystème de l'Internet des objets

Pour développer une politique dynamique en matière de normes et standards européens pour les objets connectés, les pays de l'Union devront aussi être en mesure de s'appuyer sur un écosystème industriel puissant et diversifié. Or, la difficulté des start-ups françaises et européennes à trouver des financements, explique la tentation du rachat par des sociétés américaines ou asiatiques. Comme l'a démontré l'affaire Snowden et plus récemment la remise en cause du *Safe Harbor*, les revendications européennes en matière de protection de la vie privée et de lutte contre la surveillance de masse n'auront de traductions que si des technologies alternatives peuvent être mises en place par les acteurs

[61] Voir sur ce point l'ouvrage *Delete* de Viktor Mayer-Schonberger (Princeton University Press, octobre 2009).

[62] *Europe pivots between safety and privacy online* (Christian Science Monitor, 18 jan 2015) http://www.csmonitor.com/World/Europe/2015/0118/Europe-pivots-between-safety-and-privacy-online

européens. À défaut, les Européens doivent être en mesure de participer à l'élaboration des normes et standards sur lesquels fonctionneront ces objets connectés. Les évolutions de l'Internet des objets dans les secteurs clés que seront la santé, l'énergie, l'environnement et les transports pourraient donner à l'Europe l'occasion de faire valoir ses principes en termes de protection des données personnelles et plus largement de protection des libertés. C'est le propos que tenait le vice-chancelier allemand Sigmar Gabriel, en rappelant le caractère crucial de ces normes et standards et ce d'autant plus que ces technologies auront progressivement un impact sur l'ensemble des secteurs économiques[63].

Si des accords internationaux commencent à être négociés sur la limitation du cyber-armement[64], aucun dispositif juridique international n'a encore été envisagé pour limiter les actions des États qui viseraient à affaiblir la sécurité des dispositifs de chiffrement et donc la sécurité et la confiance dans l'ensemble des échanges d'informations sur Internet. Or, l'un des programmes de la NSA révélés par Edward Snowden (le programme *Bullrun*) avait justement pour objectif de fragiliser les systèmes cryptographiques utilisés pour assurer la confidentialité des échanges ainsi que la sécurité des transactions commerciales. Les conséquences économiques de la crise autour des technologies de la cryptographie ont été telles que l'agence fédérale chargée d'élaborer les standards de chiffrement (NIST), a souhaité officiellement s'émanciper de la NSA[65]. Parmi les technologies cruciales pour la protection de la sécurité et la confidentialité des objets connectés figurent les outils cryptographiques. Or, les pays de l'Union européenne ont jusqu'ici laissé les autorités américaines (et en particulier la NSA) écrire le « Code » de ces technologies essentielles pour le fonctionnement de l'Internet et bientôt de l'Internet des objets. L'Europe qui possède les meilleures écoles de cryptographie devra être en mesure de participer au développement des normes et standards des technologies de sécurité de l'Internet des objets. La crise de confiance issue de l'affaire Snowden pourrait ainsi évoluer en une méfiance systématique vis-à-vis de ces technologies si les citoyens doutent

[63] *Industrie 4.0 ou la numérisation de l'économie* (Ministère fédéral de l'Économie et de l'Énergie, BMWi 2016) http://www.bmwi.de/FR/Sujets/Economie/Politique-industrielle/industrie-4-0.html

[64] *U.S. and China Seek Arms Deal for Cyberspace* (New York Times, 20 septembre 2015) http://www.nytimes.com/2015/09/20/world/asia/us-and-china-seek-arms-deal-for-cyberspace.html

[65] *NIST pledges transparency in NSA dealings over crypto standards* (PC Advisor, 24 janvier 2015) http://www.pcadvisor.co.uk/news/tech-industry/3595422/nist-pledges-transparency-in-nsa-dealings-over-crypto-standards/

de la sécurité et de la confidentialité des données transmises par les milliards d'objets connectés présents dans leurs environnements.

Si, dans un premier temps, l'Union européenne a préféré avec le RGPD et la directive *ePrivacy* établir des textes généralistes sur la protection des données qui s'appliquent dans certains cas aux objets connectés, d'autres textes spécifiques sur les dispositifs de contrôle, de désactivation ou encore de sécurité de ces objets devront venir étayer le dispositif actuel. Les questions spécifiques soulevées par l'Internet des Objets tant sur le plan juridique que sur le plan technologique nécessiteront à terme que soit mis en place des volets spécifiques pour la régulation de ce secteur.

Si, par le passé, la protection des données personnelles et les dispositifs destinés à limiter les cyberattaques étaient conçus comme des domaines séparés, la montée en puissance de l'Internet des objets pourrait amener à réexaminer cette séparation à la fois techniques et juridique. Il s'agira aussi de modifier la gouvernance des institutions chargées de coordonner le développement de la filière de l'Internet des Objets en Europe. Dans la perspective de développement d'une politique industrielle européenne pour l'Internet des Objets, le rôle des institutions et des textes encadrant la protection des données personnelles et de la vie privée et le piratage informatique devront être simultanément réexaminés. Des mécanismes nouveaux de coordination devront être établis pour mettre en œuvre des mesures de régulation nouvelles pour l'Internet des Objets. Parmi les structures concernées figurent les « CNIL » européennes et le G29, les régulateurs télécom nationaux et européens (ARCEP/BEREC, ANFR) ou encore les organismes de normalisation et de sécurité (ANSSI, ENISA, CEN, ETSI…). Une coopération renforcée entre ces institutions pourrait être mise en place tant au niveau national qu'européen.

Cette coopération renforcée sera à la fois nécessaire pour des raisons de protection des citoyens et des infrastructures informationnelles mais aussi pour des raisons de développement industriel de l'Internet des objets européen. Il s'agit ainsi de constituer un cadre de confiance paneuropéen pour le développement de ces technologies. De nombreux autres mécanismes technologiques pourraient être intégrés aux objets connectés pour les rendre à la fois plus sûrs et plus protecteurs pour leurs utilisateurs. Qu'il s'agisse du côté des objets des mécanismes permettant (ou obligeant) à des mises à jour de sécurité, de désactivation sélective ou encore de « *suicide programmé* [66] » des objets,

[66] Dan Geer, le « Chief security officer » du fonds d'investissement de la CIA (In-Q-Tel) voit apparaître un danger dans le nombre croissant d'appareils connectés à l'Internet dont le logiciel n'aura pas été mis à jour pendant de

ces mécanismes pourraient jouer un rôle crucial dans le développement des nouvelles filières liées aux objets connectés.

Data Residency : des enjeux industriels… et géopolitiques

Suite à une plainte d'un étudiant autrichien, Max Schrems[67], l'accord sur la transmission transatlantique des données des citoyens européens (*Safe Harbor*) a été invalidé par la Cour de Justice de l'Union européenne le 6 octobre 2015 en raison des révélations d'Edward Snowden sur les programmes de surveillance de masse de la NSA[68]. À l'issue de la renégociation de cet accord (sous l'intitulé *Privacy Shield*), de nombreuses critiques, notamment du Parlement européen et des autorités de contrôle des données personnelles, ont été émises quant au caractère très favorable des mesures envisagées pour les entreprises et les autorités américaines[69]. Parmi les options envisagées par certains États membres (comme l'Allemagne) figure l'obligation que les données relatives aux citoyens allemands ne puissent être stockées ou traitées que depuis l'un des pays de l'Union européenne[70]. La localisation des données personnelles des citoyens européens pourrait aussi devenir un enjeu politique et stratégique pour le développement d'un écosystème européen des services de stockage et de traitement des données des objets connectés. Si la récente renégociation du *Privacy Shield* maintient le principe d'une circulation transatlantique des données personnelles, des doutes persistent quant à la durabilité de cet accord[71]. L'impact du Brexit sur le transfert transatlantique des données personnelles est

longues périodes, les rendant vulnérables aux piratages informatiques. *«Ils ont des adversaires doués d'intelligence et un Internet des Objets qui serait immortel sera inévitablement pris en défaut."*
Why Gadgets in the Internet of Things Must Be Programmed to Die (Wired, 23 mai 2014)
https://www.wired.com/2014/05/iot-death/

[67] *Privacy Shield : un bouclier à peine brandi déjà ébréché ?* (Claire Levallois-Barth, Lettre de la Chaire Valeurs et politiques des informations personnelles
5 décembre 2016)
https://cvpip.wp.imt.fr/2016/12/05/privacy-shield-un-bouclier-a-peine-brandi-deja-ebreche/

[68] *Les nouveaux défis politiques et économiques de l'Internet* (Bernard Benhamou - Les Cahiers de la Documentation Française, mars 2015)
http://www.ladocumentationfrancaise.fr/var/storage/libris/3303330403921/3303330403921_EX.pdf

[69] *Données personnelles : un accord « Privacy Shield » très favorable pour les Etats-Unis* (Le Monde, 1er juillet 2016)
http://www.lemonde.fr/pixels/article/2016/07/01/donnees-personnelles-un-accord-privacy-shield-tres-favorable-pour-les-etats-unis_4962245_4408996.html

[70] *La CNIL allemande interdit aux géants du net de stocker leurs données hors d'Europe* (Euractiv, 30 octobre 2015)
http://www.euractiv.fr/section/societe-de-l-information/news/la-cnil-allemande-interdit-aux-geants-du-net-de-stocker-leurs-donnees-hors-d-europe/

[71] *This EU Data Deal Will Help U.S. Cloud Companies If It Holds Up* (Fortune, 8 juillet 2016)
http://fortune.com/2016/07/08/eu-privacy-shield

déjà envisagé par les acteurs des technologies[72]. À mesure que seront réexaminés les accords sur le traitement des données par les entreprises britanniques, la nécessité d'imposer une localisation aux données traitées par les objets connectés pourrait être à nouveau examinée.

De plus, le *Privacy Shield* qui prévoit que les fonctions d'arbitrages restent effectuées par les autorités américaines est désormais attaqué[73]. Il pourrait subir un sort comparable à son prédécesseur, le *Safe Harbor*, alors que son élaboration en urgence avait pour but de limiter l'incertitude juridique qui pouvait mener à contentieux coûteux pour les 4000 sociétés protégées par les termes de cet accord. Il est à noter que les plus importants acteurs américains des services en ligne commencent déjà à mettre en place des data centers sur le territoire européen en prévision possible d'un durcissement des textes juridiques européennes sur la localisation des données personnelles[74].

Si le principe du *Data Residency* donnait encore lieu il y a quelques mois à des discussions sur son applicabilité tant technologique que juridique, les évolutions politiques et en particulier la prise de position de l'administration Trump sur l'absence de protection juridique des données personnelles des citoyens « non américains » dans le cadre du Privacy Act, rendent plus crédibles la mise en place d'un principe de « non-transfert » de ces données en dehors des pays de l'Union européenne[75]. Cet *Executive Order* ne devait en théorie concerner que les données transmises aux agences fédérales américaines et pas les données personnelles échangées par les entreprises. Mais cette distinction n'est plus aussi claire depuis les révélations d'Edward Snowden sur la porosité des données stockées par les entreprises américaines. Cependant, si la Commission européenne, a maintenu que ces nouvelles mesures n'étaient pas censées avoir d'effet sur les données couvertes par le *Privacy Shield*, le Groupe Article 29 n'a pas considéré ces déclarations comme suffisantes et a souhaité obtenir du gouvernement américain des nouvelles assurances[76] : *« Au regard de*

---

[72] *Privacy Shield: White House makes EU spying promise* (BBC, 24 juin 2016)
http://www.bbc.com/news/technology-36619416
[73] *Le Privacy Shield attaqué devant la justice européenne* (Silicon.fr 31 octobre 2016)
http://www.silicon.fr/privacy-shield-attaque-justice-europeenne-161604.html
[74] *U.S. Tech Giants Are Investing Billions to Keep Data in Europe* (New York Times,
http://www.nytimes.com/2016/10/04/technology/us-europe-cloud-computing-amazon-microsoft-google.html
[75] *Trump order strips privacy rights from non-U.S. citizens, could nix EU-US data flows* (TechCrunch 26 janvier 2017)
https://techcrunch.com/2017/01/26/trump-order-strips-privacy-rights-from-non-u-s-citizens-could-nix-eu-us-data-flows/
[76] *Privacy Shield : l'Europe demande des garanties aux États-Unis* (Le Monde, 17 février 2017)
http://www.lemonde.fr/economie/article/2017/02/17/privacy-shield-l-europe-demande-des-garanties-aux-etats-unis_5081262_3234.html

ce que nous pourrions redouter, et de la tonalité non favorable aux Non-Américains, nous souhaitons la confirmation écrite des autorités américaines qu'il n'y a pas de remise en cause des engagements pris ». Cependant, la localisation des données ne peut à elle seule protéger ces données vis-à-vis des demandes des autorités américaines qui ont tenté à plusieurs reprises d'imposer aux entreprises américaines de leur transmettre leurs données de citoyens européens dans le cadre d'enquêtes menées aux États-Unis[77].

Si les responsables de la protection des données en Europe craignaient jusqu'à ces derniers mois que la mise en œuvre du Data Residency ne puisse apparaître comme la volonté de créer une « citadelle » en Europe, les incertitudes sur la protection des données des Européens ont été réactivées par les récentes prises de position de l'Administration Trump et rendent désormais plus probable la mise en œuvre du principe de localisation intra-européenne pour les données personnelles des Européens.

Vers un traité transatlantique sur la gouvernance de l'Internet des objets et la cybersécurité

De même que l'encadrement des objets connectés devra désormais être élaboré en prenant en compte toutes les phases de la vie des objets (depuis leur conception jusqu'à leur destruction/recyclage), l'encadrement des actions des États en matière de cyber-sécurité devra prendre en compte les actions « traditionnelles » de surveillance mais aussi les dispositifs de cyberattaques et leurs conséquences possibles sur nos sociétés.

Les actions menées à l'échelle nationale en matière de sécurité numérique n'auront d'impact que si elles s'inscrivent dans une stratégie européenne d'élévation des niveaux de sécurité des infrastructures cruciales. Dans la mesure où les attaques sur l'ensemble des secteurs économiques et sur les infrastructures vitales connaissent une forte croissance, la coordination des agences européennes spécialisées dans la sécurité informatique deviendra une nécessité.

Cependant, le premier accord international de limitation du cyber-armement a été conclu entre les États-Unis et la Chine, sans qu'à aucun moment l'Europe n'ait été associée à ces

[77] *Our search warrant case : Microsoft's commitment to protecting your privacy* (John Frank, Vice President for EU Government Affairs 5 september 2016)
https://blogs.microsoft.com/eupolicy/2016/09/05/our-search-warrant-case-microsofts-commitment-to-protecting-your-privacy/

discussions[78]. Comme l'ont démontré les récentes négociations sur le TTIP (Transatlantic Trade and Investment Partnership) la coordination des positions européenne et en particulier les volets numériques des traités internationaux deviendront des éléments stratégiques de la "cyberdiplomatie" européenne. Un accord transatlantique portant sur la limitation du cyber-armement devrait être élaboré et parmi les engagements qui devraient être inclus dans cet accord, figure l'élaboration conjointe des technologies clés pour la sécurité et la confidentialité des données sur Internet.

La situation nouvelle créée par la mise en place par les États-Unis de leurs programmes de surveillance de masse sur Internet crée une opportunité pour l'Europe de devenir l'artisan essentiel d'un accord transatlantique qui établirait les principes fondamentaux du développement de l'Internet. Cet « Internet Bill of Rights » ou cette « Magna Carta » pourrait placer les principes fondamentaux assurant le fonctionnement de l'Internet au-dessus des lois nationales afin que les États ne puissent unilatéralement modifier l'Internet et remettre en cause sa sécurité à des fins économiques ou politiques. C'est ce principe qu'avait aussi évoqué Viktor Mayer-Schoenberger, de la Harvard Kennedy School, dans son étude de la proposition européenne lors du sommet des Nations unies[79]. Dans cette étude, il notait qu'un « moment constitutionnel » avait été manqué par les États-Unis en 2005 en repoussant la proposition européenne qui prévoyait d'inscrire dans les textes internationaux les trois principes fondamentaux liés à l'architecture de l'Internet (l'ouverture, l'interopérabilité et la neutralité de l'Internet).

À ces trois principes, il conviendrait aujourd'hui d'en ajouter un quatrième qui interdirait aux États de prendre des mesures à même de porter atteinte au fonctionnement du réseau pour l'ensemble de ses utilisateurs. L'adoption d'un accord transatlantique permettrait aussi de fonder une opposabilité juridique internationale aux actions technologiques des États qui mettraient en péril le bon fonctionnement et la sécurité du réseau. Il pourrait dans un second temps être élargi à d'autres régimes démocratiques afin de veiller à ce que de nouvelles crises liées à la confiance sur Internet ne puissent fragiliser le réseau.

---

[78] *U.S. and China Seek Arms Deal for Cyberspace* (New York Times, 20 septembre 2015). https://www.nytimes.com/2015/09/20/world/asia/us-and-china-seek-arms-deal-for-cyberspace.html

[79] *Jefferson Rebuffed - The United States and the Future of Internet Governance* - Viktor Mayer-Schoenberger et Malte Ziewitz – John F. Kennedy School of Government, Harvard University (mai 2006) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=902374

Dans un premier temps, pourraient être associés à ce traité les pays comme l'Allemagne et le Brésil avec pour objectif à moyen et long terme d'en favoriser l'adoption par l'ensemble des pays membres des Nations unies.

Ce traité pourrait être à l'origine de la mise en place d'un observatoire mondial chargé du contrôle et de la protection de l'Internet[80]. Parmi les principes que cet organisme pourrait être amené à surveiller figureraient :

- La préservation des principes généraux de l'architecture du réseau : ouverture, interopérabilité et Neutralité de l'Internet,
- La protection des normes et standards qui sous-tendent le fonctionnement des infrastructures critiques de l'Internet (en particulier les systèmes de chiffrement),
- La protection des citoyens par des mesures d'encadrement des actions de surveillance des États ainsi que par la mise en place de dispositifs juridiques et technologiques de contrôle des données transmises par les objets connectés.

Bernard Benhamou est un expert français de l'Internet et spécialiste de la société de l'information. Anciennement délégué aux usages de l'internet au ministère de la Recherche et de l'Enseignement supérieur, il est actuellement Maître de conférences à l'Institut d'études politiques de Paris et chargé d'enseignement à l'Université de Paris I Panthéon-Sorbonne.

[80] Il est à noter que des propositions similaires commencent à être évoquées à l'échelle des seuls Etats-Unis et pourraient être élargies dans le cadre d'un accord transatlantique. Voir sur ce point : *How to Save the Net: A CDC for Cybercrime* (Wired, 19 août 2014)
http://www.wired.com/2014/08/save-the-net-peter-singer/

MÉCÈNES FONDATEURS
FOUNDING SPONSORS

Groupe Imprimerie Nationale

BNP PARIBAS

orange

LVMH

MÉCÈNE ASSOCIÉ
ASSOCIATE SPONSOR

DASSAULT SYSTEMES

PARTENAIRES QUALIFIÉS
QUALIFIED PARTNERS

CNIL

DINSIC*

** Direction Interministérielle du Numérique et du Système d'Information et de Communication de l'État.*

EN SAVOIR PLUS

Pour recevoir la Lettre trimestrielle de la Chaire et être invité aux événements, consulter la liste des publications et télécharger les Cahiers et le dossier de presse, rendez-vous sur :

www.informations-personnelles.org

MORE ABOUT US

You can register online to receive the quarterly newsletter of the Chair, and invitations to the events. You can also find the list of publications, download the Chair's Notebooks and the press releases on the website:

www. personal-information.org

Vous trouverez sur le compte Twitter de la Chaire une veille continue :
The Chair's Twitter account offers a continuous news watcht:

@CVPIP

YouTube
youtube.informations-personnelles.org

Institut Mines-Télécom

FONDATION Mines-Télécom
La Fondation de l'IMT

TELECOM ParisTech

TELECOM Ecole de Management

TELECOM SudParis

CONTACTS

CLAIRE LEVALLOIS-BARTH
Coordinatrice de la Chaire / Chair Coordinator
claire.levallois@imt.fr

CHANTAL FRIEDMAN
Assistante de la Chaire / Chair Assistant
chantal.friedman@telecom-paristech.fr
+33 1 45 81 72 53

Télécom ParisTech - IMT
46 rue Barrault | F-75634 Paris Cedex 13