Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
INHESJ
INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

TRAVAUX DES AUDITEURS

28e session nationale « Sécurité et Justice » 2016-2017
Groupe de diagnostic stratégique (GDS) n° 5

OBJETS CONNECTÉS ET USAGES NUMÉRIQUES : APPORTS POSSIBLES À LA SÉCURITÉ ? COMMENT ASSURER LA PROTECTION DES DONNÉES ?

JUIN 2017
ISSN 2265-447X

Les membres du Groupe de diagnostic stratégique n°5

Présidente :
Myriam QUEMENER, magistrate

Vice-président :
Pierre GREFFET, administrateur de l'INSEE, direction centrale de la police judiciaire, ministère de l'Intérieur

Tuteur :
François-Xavier POISBEAU, colonel de l'armée de Terre

Lionel ABT, chef de programme OT-Morpho
Geoffroy FOUGERAY, commissaire divisionnaire
Valentine FOURNIER, directrice fonctionnelle des services de la protection judiciaire de la jeunesse, ministère de la Justice
Grégoire GERMAIN, directeur du développement de l'offre cyber, Thalès Communications & Security
Olivier ISNARD, adjoint au chef du service de crise, Institut de radioprotection et de sûreté nucléaire.
Najet JAOUADI, commissaire de police générale premier degré, Tunisie
Régine LALLE, administratrice des finances publiques, direction régionale des finances publiques d'Ile-de-France
Paul MASSART, capitaine de vaisseau, ministère des armées
Julia PASCUAL, journaliste, Le Monde
Alexandre PICHON, commissaire divisionnaire
Pascal ROZE, adjoint au directeur opération, direction de projet Eole, SNCF
Caroline TOBY, avocate

REMERCIEMENTS

L'équipe du GDS-5 remercie particulièrement les personnes suivantes pour leur contribution à ce rapport :

Gérard Haas (Haas associés)

Christine Feral Schuhl – ancien bâtonnier de Paris

Alain Bensoussan, Nathalie Plouviet , Virginie Bensoussan Brule (& Nao)

Général Marc Watin Augouard

Jean-Philippe Gay (Groupe Orange)

Clémence Scottez (Cnil)

David Senouf (Sentai SAS)

Wilfried Ghidalia (SG forum des compétences)

Etienne Saclier d'Agrain (Thales)

MM. Gout, Longuespe et Pedreno (SCITT – service central de l'informatique et des traces technologiques)

M. Vincent Gorre, état-major de la direction de la sécurité de proximité de l'agglomération parisienne (DSPAP).

M. Philippe Saunier, cabinet du directeur général de la police nationale

« *They who can give up essential liberty, to obtain a little temporary safety, deserve neither liberty nor safety.* » - Benjamin Franklin, 1755

« *Objets inanimés, avez-vous donc une âme (...)* ?» - Alphonse de Lamartine, 1830

κυβερνήτική (cybernétique) : art de piloter, art de gouverner.

INTRODUCTION

Selon les chiffres de Gartner[1], 8,4 milliards d'objets connectés sont dénombrés aujourd'hui dans le monde et, d'ici 2020, il devrait y en avoir environ 20 milliards[2]. Sans définition officielle, on appelle couramment « objets connectés » l'ensemble des objets physiques interagissant entre eux et/ou avec des individus via des réseaux de communication, et qui collectent des données relatives à leur état et à celui de leur environnement. Les objets connectés occupent désormais une place centrale en tant qu'outils au service des utilisateurs et collecteurs de données, bouleversant le fonctionnement de nos sociétés[3].

Tous les objets ou produits peuvent a priori devenir des objets connectés. Il serait en conséquence vain de tenter de dresser une liste exhaustive de leurs usages possibles. L'internet des objets revêt un caractère universel et concerne tous les domaines d'activité : e-santé (cf. notion de « Quantified Self »[4], domotique, loisirs (sport, drones, jouets), gestion (transport, logistique, smart cities) mais aussi sécurité (surveillance et protection, armes, sauvetage...) Il est toutefois possible d'identifier quelques fonctions principales que leur connexion avec capteurs et effecteurs ajoute aux usages primaires des objets : fonction de surveillance, fonction de contrôle, fonction d'optimisation et d'anticipation, fonction d'autonomie et fonction d'identification/localisation.

L'ordinateur, et de plus en plus, le smartphone, qui sont des objets connectés par excellence car leur connexion en est quasiment l'essence, jouent un rôle pivot dans cet univers connecté. Ils constituent le plus souvent l'interface grâce à laquelle l'utilisateur contrôle et exploite les potentialités de son environnement numérique peuplé d'objets connectés.

En 2017, d'après une étude[5], 52% des Français interrogés possèdent au moins un objet connecté hormis leur smartphone.En 2020, chaque individu aura en moyenne trois objets connectés sur lui. D'ici là, deux milliards d'objets de ce type seront vendus en France. Le droit ne peut donc pas ignorer ce nouveau média qui s'inscrit désormais dans une véritable démarche de communication et de consommation. En effet, les liens entre le fabriquant, l'annonceur, le marchand et le consommateur s'accroissent. Il est désormais possible d'entretenir et de faire vivre cette relation en proposant des services complémentaires, voire de nouvelles expériences de fidélisation.

Ainsi, l'internet des objets est une autre façon d'appréhender la problématique de manière globale, sous l'angle du réseau que constituent les objets connectés, y compris ceux de la

---

(1) Gartner, « Internet of Things. Endpoints and Associated Services, Worldwide », étude prévisionnelle de décembre 2015.
(2) L'IDATE anticipe 80 milliards d'appareils connectés d'ici 2020, CISCO en envisage 50 milliards.
(3) L'internet des objets (IoT) est considéré comme la troisième évolution de l'Internet, baptisée Web 4.0. Il est en partie responsable de l'accroissement du volume de données générées sur le réseau, à l'origine du Big Data. L'IoT revêt un caractère universel pour désigner des objets connectés aux usages variés, dans le domaine par exemple de la e-santé , de la domotique ou du Quantified Self.
(4) Notion qui regroupe les outils, les principes et les méthodes permettant à chacun de mesurer ses données personnelles, de les analyser et de les partager2. Les outils du quantified self peuvent être desobjets connectés, des applications mobiles ou des applications Web.
(5) Deuxième baromètre des objets connectés OpinionWay à l'occasion du salon Distree#Connect.

vie courante, dès lors qu'ils sont au moins munis de codes, de puces RFID[6] ou d'URL[7]. Du fait de sa capacité à recueillir des données de manière massive, l'internet des objets (Internet of Things ou IoT) accroit de façon très significative le volume de données générées sur le réseau, il est donc l'une des sources à l'origine du « Big Data ». A ce titre, IBM estime que le volume total de données échangées par les objets connectés en 2016 se compte en zettaoctets.

Ces évolutions soulèvent de nombreuses questions concernant la croissance économique, les mutations sociales, la législation, mais aussi les libertés individuelles et la souveraineté nationale. Le développement exponentiel des objets connectés allant jusqu'aux « smart et safe cities » pose des défis en termes de libertés et de sécurité, tant pour les citoyens que pour les services de police et de gendarmerie, sans toutefois sombrer dans une société de surveillance généralisée.

Les objets connectés sont en effet au coeur d'enjeux sociétaux importants car ils se développent en exploitant des données personnelles ce qui les rend à la fois vulnérables mais aussi utiles comme moyens d'enquête sophistiqués. L'analyse du sujet se fera à la fois en termes de protection et de traitements des données véhiculées par ces objets connectés, d'expertise des cybermenaces dont ils sont les cibles et enfin d'opportunités pour les forces de l'ordre.

On constate aujourd'hui que des données souvent personnelles sont captées de façon croissante et font l'objet de traitements de plus en plus complexes par les objets connectés en fonction de leur degré de sophistication ce qui n'est pas sans incidences techniques et juridiques (I).

La sécurité des informations échangées et conservées est essentielle pour garantir la confidentialité des données issues des objets connectés, mais aussi leur intégrité et leur disponibilité. Ainsi, les objets connectés deviennent des cibles et des vecteurs de cyberattaques qui appellent des réponses à la fois technologiques et juridiques. (II).

Enfin, il convient de souligner l'opportunité que présentent les objets connectés pour les activités des forces de l'ordre, que ce soit pour la police judiciaire, la sécurité publique ou le renseignement (III).

---

(6) *Radio Frequency IDentification* méthode pour mémoriser et récupérer des données à distance en utilisant des marqueurs appelés « radio-étiquettes » (« *RFID tag* » ou « *RFID transponder* » en anglais).

(7) *Uniform Resource Locator* : format de nommage universel pour désigner une ressource sur Internet.

QUELLES PROTECTIONS POUR QUELLES DONNÉES ?

Des objets plus ou moins « intelligents »

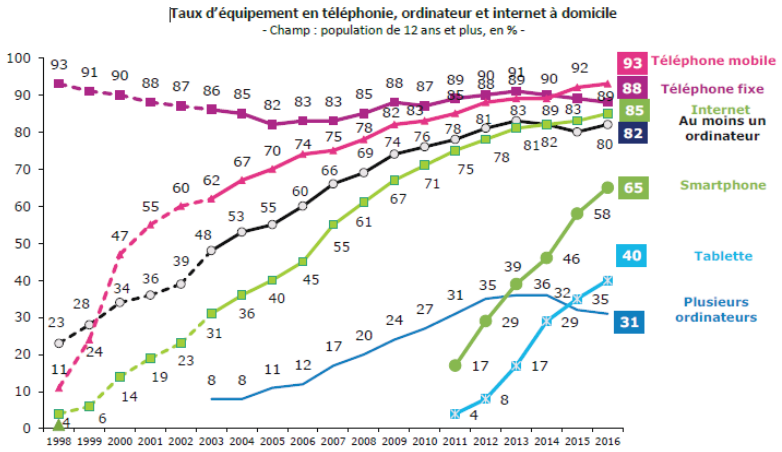
Selon la CNIL, un objet connecté renvoie à cinq critères : « C'est un objet physique, à la main de l'utilisateur, qui permet de capter des informations, dans l'environnement de l'utilisateur, et qui n'a pas vocation à transmettre des informations à un tiers. »

Des smartphones et tablettes…

En 2016 plus d'1,5 million de smartphones ont été vendus dans le monde. Le smartphone est par essence connecté, ses versions les plus modernes disposent de plus d'une dizaine de capteurs capables d'acquérir la position géographique (GPS), l'accélération du boitier, son altitude, la luminosité ambiante mais également des vidéos et l'environnement sonore. Les usages du smartphone sont multiples comme assistant personnel dans le monde du travail, système de navigation sur la route, lecteur de vidéo mais également lien avec l'ensemble de la sphère des réseaux sociaux ; accessoirement comme outil d'appels téléphoniques.

Le baromètre du numérique de l'Autorité de régulation des communications électroniques et des postes (ARCEP), dans son édition 2016, montre que les taux d'équipements en smartphones ou en tablettes connaissent depuis 5 ans une progression vertigineuse : +282% pour les smartphones et plus encore pour les tablettes avec +900%.

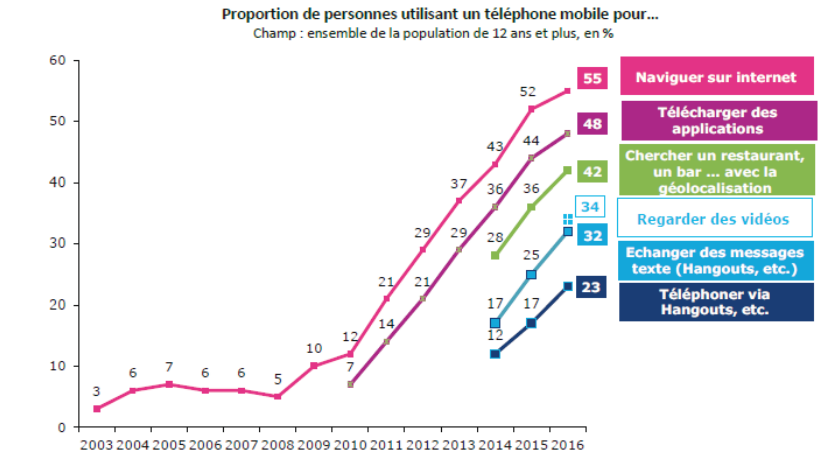
Figure 1 : taux d'équipement en téléphonie, ordinateur et internet à domicile



Source : CREDOC, enquêtes «Conditions de vie et Aspirations » (vague de juin de chaque année).
Note : avant 2003 (en pointillés), les résultats portent sur les 18 ans et plus. A partir de 2003, les résultats portent sur les 12 ans et plus.

Les usages plébiscités par les utilisateurs sont en premier lieu la navigation sur internet (+28% depuis 2014) et le téléchargement d'application (+33%) mais la géolocalisation qui arrive en troisième position connaît une progression bien plus forte (+50%) sur les trois dernières années.

Figure 2 : principaux usages du téléphone mobile



Source : CREDOC, Enquêtes sur les « Conditions de vie et les Aspirations ».

Des « *wearables* »...

L'internet des objets pour les utilisateurs concerne également celui des « wearables », définissant un ensemble d'objets connectés que l'utilisateur porte sur lui pour mesurer sa vie courante comme ses performances sportives (« Quantified Self »). La santé personnelle au travers des objets connectés est également un élément important de l'internet des objets pour les utilisateurs. Un rapport sur les objets connectés présenté le 10 janvier 2017 à la commission des affaires économiques de l'Assemblée nationale recommande la prise en charge « au moins partielle » par l'assurance maladie des objets participant à la politique de prévention à destination des populations fragiles.

Des voitures connectées...

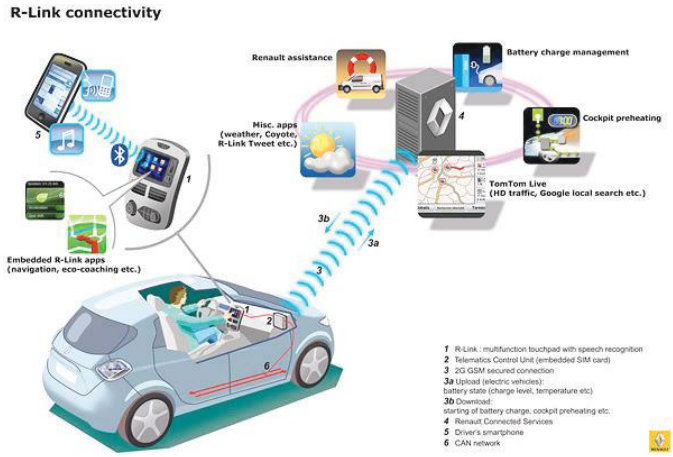
En attendant la voiture connectée complètement autonome et capable de transporter des passagers sur des routes « intelligentes », certains modèles actuels disposent déjà de systèmes permettant de garer le véhicule sans assistance, utilisant des capteurs connectés pour mouvoir le véhicule dans un environnement contraint.

Mais aussi des capteurs pour l'industrie ou pour les forces de sécurité...

L'espace industriel regroupe l'usage des objets connectés dans l'ensemble de l'industrie tel que la fabrication, la logistique, le transport, l'énergie (pétrole et gaz notamment), l'aéronautique... Cet usage est tourné vers l'optimisation, la rationalisation et l'efficacité des processus de ces industries. La maintenance préventive d'infrastructures industrielles critiques est un enjeu clé où les objets connectés, les capteurs ont ainsi un rôle central à jouer. On peut notamment citer la surveillance par capteurs connectés de certains matériels de centrales de production d'énergie (nucléaire, thermique, hydraulique) ou de zones de triage pour le transport ferré. Le domaine médical est également un secteur de l'industrie

qui cherche à intégrer de manière rapide de nombreux objets connectés pour proposer des solutions et services aux personnes âgées ou souffrant de maladies chroniques par exemple. Ces services intègrent entre autres la surveillance de statistiques vitales, la configuration à distance de moyens médicaux. Il fait écho à l'emploi dans l'espace privé d'objets connectés pour« mesurer » sa santé. L'espace des services publics correspond davantage à l'usage d'objets connectés dans un contexte de « smart cities » permettant d'optimiser la conduite de services comme la gestion du trafic routier, la demande en transport public en temps réel, l'orientation de l'usager vers des places de parking libres ou la surveillance de zones sensibles par caméras.

Figure 3 : le véhicule connecté



Source : http://img4.autodeclics.com/photos/3/86264/la-voiture-connecte-devient-accessible.jpg

Le domaine de la sécurité dans l'emploi d'objets connectés pour les services publics est crucial. Il permet la détection et l'optimisation d'une réponse à toute situation identifiée comme potentiellement génératrice de risque pour la population ou l'environnement. Lorsque le risque est avéré et qu'une situation d'urgence se développe, la réponse efficace des services publics repose sur des informations précises et proches du temps réel acquises grâce à des capteurs (caméra) placés dans l'environnement ou directement sur les forces de sécurité.

Les espaces des utilisateurs et des services publics s'entremêlent dans l'emploi des smartphones où les données acquises par ces derniers servent de sources de masse (« crowd-sourcing »). On peut citer par l'exemple l'initiative « Street-Bump » de la ville de Boston aux Etats-Unis qui, à partir d'une application installée sur smartphone, utilise les capteurs de ce dernier pour renseigner en temps réel les services de la ville sur les conditions et l'état des routes.

Conceptuellement, les objets connectés possèdent trois déterminants :

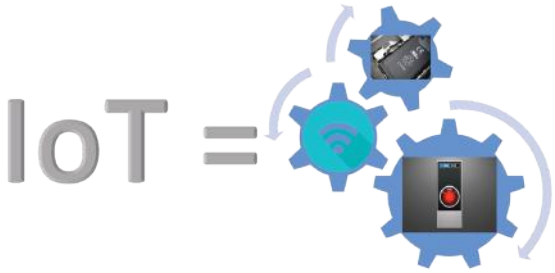
- Leur capacité de communication plus ou moins rapide, à plus ou moins grande distance avec les technologies Bluetooth, WiFi, 4G, LoRa, SigFox ... ;
- Leur « intelligence » embarquée, c'est-à-dire, leur capacité à pouvoir traiter en interne une plus ou moins grande quantité d'information sur une certaine durée grâce à des puces de type ARM, etc. ;
- Leur énergie embarquée : un objet connecté doit pouvoir être alimenté électriquement pour fonctionner de façon autonome et pour cela il dispose d'une batterie de plus ou moins grande capacité : batteries Li-ion sur les smartphones, tablettes, ...

Ces trois grandes qualités sont interdépendantes : les capacités de communication et de traitement sont liées à la quantité d'énergie dont ils disposent. Certaines d'entre elles peuvent être externalisées par rapport à l'objet connecté qui, par exemple, peut ne pas disposer de sa propre source d'alimentation et pour cela être relié au secteur (exemple d'un ordinateur fixe ou d'un réfrigérateur connecté.)

La capacité de traitement peut aussi être externalisée pour tout ou partie.C'est le cas pour le service fourni par l'assistant (« chatbot ») Siri sur les smartphones d'Apple : l'iPhone ne fait que retransmettre le message vocal de l'utilisateur aux serveurs d'Apple (cloud) chargés de traiter cette commande et en retour transmettent une réponse à l'utilisateur. Il est à noter que cette fonctionnalité ne peut être opérante sans communication avec le « cloud » d'Apple.

C'est aussi le cas des montres connectées qui ne disposent pas de connections directes aux réseaux mobiles et pour cela doivent être « jumelées » à un smartphone pour fonctionner (Par exemple Apple Watch v2 ou Samsung Gear S2).

Figure 4 : objet connecté = capacité de traitement + connectivité + source d'énergie



A ce jour, les performances des objets connectés en matière d'« intelligence » et de communications augmentent de façon exponentielle, le seul frein étant la capacité des batteries qui ne progresse pas aussi vite et qui renvoie à la problématique du stockage de l'énergie. La technologie actuelle permet toutefois des gains d'autonomie significatifs, par l'utilisation de puces de plus en plus économes en énergie.

Des objets interactifs dans des marchés en expansion

L'étude deGartner affirme qu'il y aura d'avantage d'objets connectés que d'humains avec 8,4 milliards d'unités IoT utilisées en 2017 partout dans le monde, soit une augmentation de 31 % par rapport à l'année 2016. Les dépenses totales, englobant les produits et les services, devraient dépasser les 2 trillions de dollars en 2017.

Les pays et les régions du monde qui seront à l'origine de cette augmentation des usages sont la Chine, l'Amérique du Nord et l'Europe de L'Ouest. Ensemble, ces trois régions disposeront de 67 % des objets et des capteurs IoT installés dans le monde.

Comme le montre le tableau 1 infra, ce seront les objets connectés pour le grand public qui domineront le marché en 2017. Avec 5,2 milliards d'unités dans le monde, ce secteur représentera 63 % des produits de la base installée. Par rapport à l'année 2016, cela représente près d'1,3 milliard d'objets connectés en plus dans les foyers du monde entier. Le directeur des recherches de Gartner, Peter Middleton, déclare qu'en dehors « des systèmes « d'infotainment » dans les voitures, les applications IoT les plus utilisées par les consommateurs seront les Smart TV et les box TV connectées. »

En 2017, les professionnels utiliseront principalement des compteurs intelligents et des caméras de vidéoprotection connectées. Toujours selon le cabinet, les industriels profiteront d'applications IoT sur mesure comme des machines de production connectées, des capteurs pour gérer la production d'énergie ou encore de la géolocalisation en temps réel des conteneurs de transplantation d'organes dans la santé.

Tableau 1: unités IoT installées par catégorie (millions d'unités)

Catégorie d'utilisateur	2016	2017	2018	2020
Consommateur final	3963	5244,3	7036,3	12863
Acteurs économiques	1102,1	1501	2132,6	4381,4
Acteurs économiques	1316,6	1635,4	2027,7	3171
Total	6381,7	8380,7	11196,6	20415,4

Source: Gartner (janvier 2017)

Table 2: dépenses en équipements IoT par catégorie (millions de dollars)

Catégorie d'utilisateur	2016	2017	2018	2020
Consommateur final	532515	725696	985348	1494466
Acteurs économiques transsectoriels	212069	280059	372989	567659
Acteurs économiques monosectoriels	634921	683817	736543	863662
Total	1379505	1689572	2094881	2925787

Source: Gartner (janvier 2017)

Les objets connectés connaissent depuis quelques temps déjà un certain succès tant auprès des utilisateurs finaux que des acteurs économiques, en raison des services à valeur ajoutée qu'ils apportent. Pour l'utilisateur final, il s'agira de pouvoir enrichir l'usage d'un objet de la vie quotidienne comme par exemple l'accès à des fonctions de partage d'informations (tracker d'activité), de contrôle à distance (caméra de sécurité), de surveillance de sa consommation électrique (compteur connecté). Pour les entreprises, il s'agira essentiellement d'optimiser des processus par l'utilisation de capteurs « intelligents ». Le développement de ce marché, s'il est souhaitable, ne doit pas se faire sans un minimum de garanties pour les utilisateurs.

Il est nécessaire dans l'intérêt des citoyens et des entreprises d'imposer des règles permettant à la fois de protéger les libertés individuelles tout en garantissant la cybersécurité des objets connectés. Il devient nécessaire envisager la régulation nationale des stocks de données, avec la création d'un grand service public national des données publiques.

C'est en ce sens que le règlement général sur la protection des données[8] (RGPD) du 27 avril 2016 est adapté aux questions que posent par exemple les « smart cities », car il responsabilise les concepteurs quant au respect du droit des données personnelles en imposant les principes de « privacy by design » et de « privacy by default ».

(8) 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

L'Internet des objets : au centre de l'échange des données

Toute étude concernant l'évolution, les opportunités et les menaces qui entourent l'internet des objets doit, dans un premier temps, s'intéresser à la nature des flux de données générés par ces objets. Une analyse de la nature des données concernées puis de leurs flux permet de modéliser l' « économie de la connaissance »[9] propre aux objets connectés. Cette approche permet d'élaborer des recommandations en matière de sécurité liée à l'usage des objets connectés.

De quelles données s'agit-il ?

La figure ci-dessous récapitule les catégories de données concernées par les objets connectés. Ces données peuvent être générées ou utilisées par ces objets, il s'agit de :

- ✓ données relatives aux individus (personnes physiques) : ces données *personnelles* peuvent être recueillies par les objets que l'individu possède et porte sur lui (smartphone, montre connectée, vêtements connectés, etc.) ou par des objets situés dans son environnement (distributeur de billets, caméra, terminal carte bancaire, appareils médicaux, etc.). Ces données peuvent être captées avec le consentement[10] et la conscience de la personne connectée ou à son insu, en particulier dans l'espace public. D'ores et déjà mais il s'agit d'un phénomène amené à se développer rapidement avec la généralisation des objets connectés, les individus laissent derrière eux un « sillage numérique[11] » considérable permettant potentiellement de reconstituer très précisément l'état des individus (finances, santé, habitudes, préférences, etc.). La maîtrise de ces données constitue un enjeu stratégique majeur pour les entreprises[12] et les Etats. Du point de vue des forces de sécurité, ces traces numériques représentent aussi une opportunité. Cet aspect est développé dans la partie 3.B de ce rapport.

- ✓ données relatives à des équipements : les objets connectés génèrent également des données. Ces données diffèrent notablement si l'objet connecté est fixe ou mobile. Dans ce dernier cas, un grand nombre de données recueillies en temps réel concerne la cinématique de l'objet (ex : véhicule connecté). Les équipements connectés recueillent aussi des informations concernant leur environnement (ex : objets connectés consacrés à la surveillance et la sécurité). Enfin, les objets connectés complexes peuvent élaborer des informations concernant leur fonctionnement (ex : une imprimante qui indique à distance le nombre de copies qu'elle a réalisées et le niveau de Toner). Ces informations permettent d'optimiser leur fonctionnement, de piloter leur entretien préventif et d'augmenter ainsi significativement leur disponibilité et leur rentabilité.

- ✓ Données relatives à des organisations (personnes morales) : les organisations (administrations, associations et entreprises notamment) peuvent s'assimiler à des « méta-objets » du fait de la numérisation d'une grande partie de leurs activités. Si elles créent peu de données, elles ont vocation à en traiter une quantité considérable et croissante, y

(9) « L'économie de la connaissance - Idriss Aberkane in « libérez votre cerveau (Robert Laffont)

(10) Actuellement, la plupart des applications utilisant des données personnelles notifient la capture de données et requièrent le consentement des utilisateurs. Cependant, la complexité des textes de mise en garde, la facilité d'acceptation (une case à cocher) et la nécessité d'obtenir un service poussent les utilisateurs à accepter ces conditions de manière assez automatique.

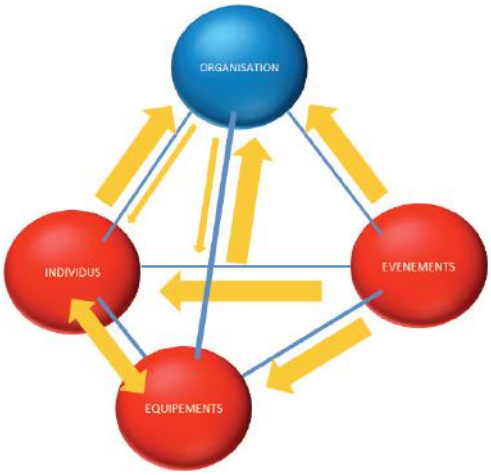
(11) Dans l'ouvrage « L'homme nu, les auteurs, Marc Dugain et Christophe Labbé relèvent : « *Avec un objet connecté, on en sait plus sur vous qu'avec votre empreinte digitale* » (Eric Peres, vice-président de la CNIL, décembre 2014)

(12) Par exemple les assureurs.

compris des données à caractère personnel (relatives à des personnes physiques, clients, fournisseurs, employés...). Pour les Etats, comme pour les entreprises, et en particulier celles dans le domaine des technologies de l'information e de la communication (TIC), la maîtrise d'une quantité croissante d'informations devient un enjeu stratégique majeur[13]. A tel point que le Danemark a décidé fin janvier 2017 de désigner un ambassadeur numérique auprès des GAFA[14].

- Données relatives à des événements : entité de nature virtuelle, un événement est cependant générateur de données. Qu'il soit accidentel (catastrophe naturelle), social (événement culturel, politique, revendicatif, etc.) ou privé (agenda personnel, réunion, maladie, etc.), tout événement est susceptible de provoquer l'intérêt des capteurs connectés et la collecte de données. Comme pour les individus, la collecte d'information peut se faire avec ou sans l'assentiment des acteurs concernés, en particulier sur l'espace public ou via les réseaux sociaux fortement sollicités pour les événements collectifs. L'événement, par nature, n'est pas en capacité de recevoir des données et n'est qu'un émetteur.

Figure n°5 : taxonomie des données et des flux de données concernant l'IOT



Quels flux de données ?

La figure n°5, ci-dessus, permet de visualiser une cartographie des données et de leurs flux.

Cette cartographie fait apparaître des flux importants créés par les équipements et les individus :

- Les équipements génèrent un flux automatisé de données à destination principalement des organisations (entreprises commerciales et services publics) mais aussi vers les individus. Ces flux permettent aux organisations d'enrichir leurs bases de données et d'améliorer leur service ou leur compétitivité contribuant ainsi à l'efficacité professionnelle, au confort et la sécurité des individus et des biens. Par exemple, une caméra de surveillance connectée produit un flux d'images en temps réel mis à la disposition des usagers ou des administrations.

(13) Ainsi les GAFA (Google, Apple Facebook, Amazon) sont en passe de constituer une puissance de nature quasi impériale s'appuyant sur la maîtrise des données combinée à la puissance de calcul et à l'intelligence artificielle (bigdata).
(14) http://www.thelocal.dk/20170127/in-world-first-denmark-to-name-a-digital-ambassador

- ✓ Les individus produisent un flux de données, volontairement ou non, principalement vers des équipements ou des organisations. Ces flux permettent aux individus d'obtenir, en compensation des données cédées, des prestations de services, des liens sociaux, des loisirs ou une meilleure sécurité. Citons l'exemple de l'application collaborative Waze, qui permet de partager en temps réel l'état du trafic routier.

Cette cartographie des flux permet d'affirmer que les organisations commerciales ou publiques sont les plus consommatrices de données.

Il est donc possible de déduire que les individus concèdent des données personnelles via les objets connectés qui se situent dans leur environnement. En contrepartie, les individus peuvent obtenir un certain nombre de services et de facilités dans leur vie quotidienne ou professionnelle. Via les objets connectés, les individus échangent, consciemment ou non, de la liberté contre des services et de la sécurité. Il s'agit bien d'une transaction puisque ces données constituent une véritable matière première qui est exploitée et valorisée par les prestataires de services et les grands acteurs de l'économie numérique (GAFA[15]), mais aussi par les forces de sécurité.

Le paragraphe précédent met en évidence un paradoxe qu'il paraît important de souligner : alors que les données personnelles recueillies par les objets connectés couvrent un nombre croissant de domaines touchant à la vie privée[16], à la sécurité voire au secret professionnel, les individus n'ont pas toujours conscience de cette captation. Pour protéger le public d'une exploitation abusive qui peut être faite, à leur insu, de données personnelles ou professionnelles, il est essentiel d'améliorer l'information du public concerné. En effet, si l'aspect « connecté » de certains objets est assez évident (exemple d'un smartphone), d'autres objets de la vie courante (appareil ménager, vêtement, domotique), sont susceptibles d'être connectés de manière de plus en plus banale et discrète, aussi bien dans les lieux privés, les lieux de travail[17] que sur la voie publique.

Sur le plan technique, les experts en sécurité informatique soulignent la nécessité de protéger chaque objet par mot de passe, d'implémenter une authentification via des certificats avec la mise en œuvre d'une politique transparente de confidentialité et d'archivage des données. Le *déploiement rapide des corrections de failles de sécurité et l'incitation des consommateurs à prendre conscience de la nécessité de protéger leurs données personnelles* s'imposent également.

Quelle protection des données ?

Dans quelle mesure le cadre législatif actuel, relatif à la collecte et au traitement des données et déterminant les responsabilités des acteurs concernés, reste-t-il adapté ?

Outre des dispositifs techniques, la protection des données transitant par les objets connectés nécessite également des dispositifs législatifs. En effet, les objets connectés peuvent être la cible de cybercriminels convoitant les nombreuses données, notamment personnelles plus ou moins sensibles qu'ils contiennent.

---

(15) Dans l'ouvrage « L'homme nu - La dictature invisible du numérique, les auteurs, Marc Dugain et Christophe Labbé citent les « NATU pour Netflix, Airbnb, Tesla et Uber

(16) « *La vie privée est un concept qui a émergé lors du boom urbain de la révolution industrielle. Si bien que cela pourrait très bien n'être qu'une anomalie.* déclarait Vinton Cerf, Chief Internet Evangelist chez Google et Ingénieur en chef sur le projet ARPANET. (http://www.businessinsider.fr/us/google-vinton-cerf-declares-an-end-to-privacy-2013-11/)

(17) Ainsi, en 2015, un service de renseignement « du premier cercle a dû neutraliser l'ensemble des machines à café de ses « points de convivialité suite à la découverte que ces machines connectées à internet (non chiffré) communiquaient en temps réel les informations nominatives concernant leur utilisation par les agents, permettant ainsi de reconstituer les horaires et activités de ces agents.

Il s'agit donc d'évaluer la pertinence du système juridique actuel de protection des données appliqué aux objets connectés.

Selon la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés – dite loi « Informatique et libertés » – « constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ». Certaines données protégées telles celles concernant l'état de santé des individus méritent des dispositions particulières.

La même loi encadre la collecte et l'utilisation des données à caractère personnel. Elle confère des droits aux personnes dont les données sont collectées et traitées et impose le respect de plusieurs obligations aux responsables du traitement de ces données.

Cependant, cette loi offre une protection réduite si la personne a consenti, car le consentement est au cœur du dispositif légal. Par principe, un traitement de données à caractère personnel est licite s'il a reçu le consentement de la personne concernée. Ce système est le système de l' « opt in ».

Or, le consentement ne sera plus obligatoire lorsque le traitement est nécessaire à l'exécution d'un contrat. Le législateur présume que la personne a implicitement consenti au traitement des données la concernant dès qu'elle contracte. A titre d'exemple, lorsqu'une personne s'inscrit sur un réseau social tel que Facebook ou Twitter, elle fournit des données personnelles lors de son inscription. Si la personne souhaite s'inscrire sur le réseau, elle n'a pas le choix. Si elle ne veut pas voir ses données collectées, la seule solution est de renoncer au bénéfice de l'utilisation que lui procure le service ou le produit.

La question du consentement est donc un enjeu fort. Celle-ci va être amenée à évoluer prochainement dans le cadre de l'élaboration du règlement européen pris sur la base de la Directive européenne ePrivacy. La Commission européenne a proposé une première version de ce texte qui vise à renforcer la protection des données des internautes et qui a été mis en ligne le 10 janvier 2017. L'article 9 de ce projet vise à renforcer le consentement avec notamment la possibilité pour les utilisateurs finaux de le retirer à tout moment s'agissant du traitement de données de communications électroniques, cette possibilité leur étant rappelée tous les six mois tant que le traitement se poursuit.

Le responsable du traitement devra néanmoins respecter de son côté les principes imposés par la loi (proportionnalité, pertinence, durée et finalité) ainsi que l'obligation de déclaration à la CNIL ou la demande d'autorisation pour les traitements les plus sensibles.

Des difficultés apparaissent concernant le droit effectif d'opposition lorsque le constructeur n'est pas européen et concernant le droit de regard des puces par les utilisateurs. Ces difficultés sont amplifiées par l'hyper connectivité des objets.

Compte tenu de ces menaces, l'article 34 de la loi Informatique et libertés impose au responsable du traitement des données « de prendre toutes précautions utiles (...) pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès »[18].

Le règlement (UE) n° 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

(18) Le non-respect de ces dispositions est puni par l'article 226-17 du Code pénal de cinq ans d'emprisonnement et de 300 000 euros d'amende, celle-ci pouvant atteindre 1 500 000 euros pour les personnes morales.

personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données ou GDPR), s'intéresse à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données. Il clarifie la notion de données personnelles incluant désormais non seulement les identifiants en ligne, les données de géolocalisation des individus mais aussi les adresses IP.

Ce règlement européen met à la charge du responsable du traitement une obligation de sécurité du traitement. Ce dernier doit ainsi garantir un niveau de sécurité adapté aux risques, notamment avec des mesures techniques et organisationnelles appropriées.

Il peut s'agir de « pseudonymisation » et de chiffrement des données à caractère personnel ; des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ; ou encore une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement. Le responsable de traitement a en outre l'obligation de notifier la violation de données à caractère personnel à l'autorité de contrôle compétente, c'est-à-dire en France à la CNIL. Les concepteurs d'objets connectés collectant des données à caractère personnel devront donc se soumettre à ces obligations accrues en matière de sécurité[19].

Le principe de Privacy by Design

Les opérateurs économiques vont se voir imposer par le règlement général de la protection des données une obligation de protéger la vie privée dès la conception, obligation communément désignée par l'expression « Privacy by Design » ; il s'agit d'intégrer la protection des données dès la conception des systèmes et des technologies informatiques et implique notamment que les développeurs s'imposent de ne pas recueillir de données sans lien avec le service rendu. Le règlement met à la charge des responsables de traitement une obligation d'anticipation de tous les risques liés au traitement de données à caractère personnel via l'adoption de mesures techniques et organisationnelles en amont de tout projet.

Les entreprises sont ainsi incitées à intégrer la protection des données dès la conception des outils techniques et favoriser des approches par analyse de risques pour la mise en place des mesures de sécurité, c'est-à-dire à promouvoir la Privacy by Design. Ces approches permettent d'adapter les mesures de sécurité aux risques réels. Il s'agit d'une application du principe de proportionnalité qui vise à limiter le type et la quantité de données collectées dès la conception des systèmes informatiques mais ce principe est complexe dans sa mise en œuvre.

Le principe d' « accountability »

Ce principe implique que le responsable du traitement de données personnelles doit veiller à la conformité de chaque opération de traitement et en apporter la preuve ; le règlement instaure sa responsabilité. Dans les entités publiques et dans les entreprises traitant des données personnelles à une échelle importante, ce responsable sera un DPO (Data protection officer), correspondant, en France, à l'actuel correspondant informatique et libertés (CIL).

---

(19) Les « CNIL nationales pourront prononcer des sanctions pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires annuel global de l'entreprise.

Le droit à la « portabilité des données »

Ce droit est prévu à l'article 20 du règlement général et permet aux utilisateurs de récupérer les données qu'ils ont fournies à un prestataire de service dans un format structuré, couramment utilisé et lisible par machine. En vertu de l'article 48 de la loi pour une République numérique, le consommateur dispose en toutes circonstances d'un droit de récupération de l'ensemble de ses données auprès des fournisseurs de services de communication en ligne.

Les dispositions du règlement européen entreront en vigueur le 28 mai 2018 et constituent un enjeu majeur qu'il convient d'accompagner par un partage de bonnes pratiques mais également un contrôle accru de la CNIL.

L'usage des objets connectés va aussi amener à interroger le droit de la responsabilité.

Recommandations

Recommandation n°1 :
Adapter la réglementation aux objets connectés, sur le plan au moins européen pour ce qui concerne la protection des données personnelles.

Recommandation n°2 :
Sensibiliser les consommateurs aux usages et risques des objets connectés par un plan national d'information. Apposer une signalétique spécifique « IoT » précisant le caractère connecté de l'objet ainsi que son niveau de sécurité (type critère commun de l'ANSSI, cf Figure n°6). Y associer les startups françaises de type « bug bounty » Yogosha et Bounty Factory.

Recommandation n°3 :
Renforcer les règles en matière de consentement des utilisateurs avec la possibilité d'alerter sur les risques associés à cette transmission et garantir la proportionnalité entre le service rendu et le type de données collectées.

Recommandation n°4 :
Valoriser les bonnes pratiques des entreprises et mettre en place une notation « Empreinte numérique » (type Fitch, S&P, ...) par la CNIL permettant d'évaluer les objets connectés de manière équitable et transparente.

Recommandation n°5 :
Renforcer les moyens des instances de contrôle (CNIL, ARCEP, ...). Mettre en place une certification délivrée par ces mêmes instances à certaines structures agréées pour exercer ce contrôle. Prévoir et publier les sanctions.

Traitements algorithmiques des données et droit des robots

Après avoir traité des données collectées par les objets connectés, il convient de s'interroger sur la place faite aux algorithmes d'intelligence artificielle dans les choix et programmations réalisés à la place de l'homme. Il peut s'agir d'assistants personnels, de « blockchains[20] », voire de voitures autonomes pour lesquels se pose la question de la responsabilité juridique (droit des robots).

Les algorithmes dans notre vie quotidienne

Dans nos actes de consommation réalisés via Internet, qu'il s'agisse d'acheter des paires de chaussures ou de regarder un film en VOD depuis une « Smart TV » ou via une « Box internet », dans les relations avec une banque en ligne, il y a une forte probabilité qu'un algorithme intervienne à un moment ou à un autre de l'opération.

Cet « *ensemble de règles opératoires dont l'application permet de résoudre un problème énoncé au moyen d'un nombre fini d'opérations*[21] » est aujourd'hui devenu un incontournable de notre vie quotidienne.

De nouveaux usages algorithmiques plus inattendus apparaissent dans d'autres domaines tels le diagnostic de cancers, le recrutement de salariés, l'affectation d'effectifs de forces de l'ordre sur certains territoires, l'établissement des primes d'assurance, les listes « noires » des compagnies aériennes.

De façon plus expérimentale, des algorithmes sont utilisés pour générer des rapports d'analyse à partir de données brutes. C'est ainsi que la campagne électorale de Donald Trump a pu bénéficier de l'expertise de comportementalistes qui ont mis en œuvre des algorithmes pour cibler les électeurs qui pouvaient lui être favorables.

Les algorithmes ont le mérite, de par leurs fondements mathématiques, d'introduire une part de logique voire de rationalité lors de la prise de décisions subjectives mais en contrepartie on peut leur reprocher leur manque de transparence, leur effet « boîte noire » alors que notre société est de plus en de plus exigeante sur les principes éthiques et l' « accountability[22] ».

Certains scientifiques mettent en garde contre le fait de suivre aveuglément des formules mathématiques pour établir un résultat juste. Selon la « data scientist » Cathy O'Neil, « les algorithmes ne sont pas intrinsèquement impartiaux parce que c'est la personne qui les élabore qui définit les conditions de leur réussite ».

Elle ajoute que si certains algorithmes sont indéniablement utiles à la société, d'autres peuvent avoir des effets néfastes. Dans son ouvrage *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, elle livre des exemples en ce sens :

- ✓ Des établissements scolaires publics de la ville de Washington ont licencié en 2010 plus de 200 enseignants dont certains ayant une solide réputation sur la base de résultats produits par un algorithme d'évaluation de leur performance ;

(20) La chaîne de blocs (en anglais *blockchain*) est une base de données distribuée transparente, sécurisée, et fonctionnant sans organe central de contrôle
(21) Définition du Larousse : http://www.larousse.fr/dictionnaires/francais/algorithme/2238
(22) (Voir partie B) Le fait pour une entité de rendre compte à un groupe d'individus voire à la société toute entière.

- Un homme souffrant de bipolarité s'est vu refuser des postes auprès de sociétés de distribution parce qu'un test de personnalité basé sur un algorithme a mis en évidence un risque élevé ;
- Des cours de justice s'appuient sur des algorithmes pour la détermination des peines introduisant une discrimination auprès de certaines minorités par la prise en compte de facteurs tels que la délinquance commise par leurs voisins, leurs amis ou leur famille ;
- Dans la finance, des opérateurs collectent et analysent automatiquement de grandes quantités de données sur Internet pour prendre des décisions en matière bancaire ou assurantielle, méthode conduisant à amplifier les discriminations.

Un rapport de la Maison Blanche de 2016 alertait sur « la faillibilité des systèmes basés sur des algorithmes dans la mesure où ils s'appuient sur des composantes potentiellement imparfaites : données, logique, probabilités voire personnes qui les conçoivent ». Le rapport relevait que ces systèmes « intelligents » pouvaient dans le meilleur des cas réduire certains biais humains mais il mettait aussi en garde sur leur capacité à systématiser une forme de discrimination à l'encontre de groupes d'individus.

Pour Zeynep Tufekci, professeure à l'Université de Caroline du Nord qui étude les liens entre la technologie et la société, les outils d'aide à la décision s'appuient souvent sur la collecte de données individuelles et dans certains cas sur des données collectées à l'insu des individus.

Elle ajoute que ces systèmes informatiques peuvent déduire quantité d'informations sur chaque individu à partir de leur « sillage numérique »[23]. Ainsi ils peuvent prédire vos orientations sexuelles, les caractéristiques de votre personnalité, vos convictions politiques et ceci avec une grande précision.

Selon elle, la problématique repose sur le paradoxe consistant à demander à une machine de fournir une réponse unique à des questions qui en attendent plusieurs.

Il en va ainsi de l'embauches de salariés dans une société, des suggestions d'extension de votre réseau social de relations voire de la récidive criminelle.

Frank Pasquale, professeur de droit à l'Université du Maryland et auteur de l'ouvrage The Black Box *Societé* : The Secret *Algorithms That Control Money And Information* partage ces préoccupations. Il suggère ainsi de traiter les effets discriminatoires générés par les algorithmes par la stricte mise en application des lois de protection des consommateurs ou celles relatives aux tromperies et pratiques mensongères.

Selon lui, le règlement général de l'Union européenne sur la protection des données[24] qui reconnaît aux individus dès 2018 un certain nombre de droits quand ceux-ci sont impactés par une décision relevant d'un processus algorithmique (profilage) est un modèle à généraliser. Il est convaincu que cela obligerait les algorithmes à davantage de transparence sous peine d'être exclus.

La technique algorithmique

Les traitements algorithmiques pouvant être effectués sur les données collectées et échangées dans le cadre de l'IoT sont de différentes sortes et présentent selon leur nature des problématiques spécifiques et en partie inédites.

---

(23) Voir partie 1.B1.
(24) Voir partie 1.B.4 de ce rapport.

Ainsi le traitement algorithmique peut être très simple, sans intelligence particulière, lorsqu'il s'agit par exemple d'appliquer une règle logique déterministe sur une donnée unique. Il peut s'avérer beaucoup plus complexe, présenter une forme de raisonnement de type « intelligence artificielle » (IA), faire des analyses de corrélation entre des données très hétérogènes, parvenir à des décisions qui dépassent parfois les capacités du raisonnement humain ou les capacités de traitement manuel. Il s'agit ici de présenter les enjeux liés à cette nouvelle génération d'algorithmes, de type « IA », qui ont des impacts majeurs dans le monde de l'IoT, offrant de nouvelles perspectives dans l'usage des objets connectés et posant également de nouvelles problématiques dans l'encadrement de ces technologies (règlementation, éthique, ...).

Ces nouveaux types d'algorithmes sont aussi à analyser sous l'angle de la capacité à garantir la sécurité des données échangées ou produites. Assurer une traçabilité, une transparence des opérations, la non répudiation des données, devient aujourd'hui primordial. De nouveaux types de technologies permettent d'atteindre une plus grande sécurité des traitements effectués ou des données produites comme par exemple les « blockchains ».

L'Intelligence artificielle et le « machine learning »

Schématiquement, il existe deux catégories d'algorithmes.

La première catégorie est celle des dite des « algorithmes classiques » basés sur des logiques de décision mathématiques. Toute décision est une suite logique, déterministe et facilement reproductible, que l'on peut démontrer.

La seconde catégorie est celle des algorithmes de nouvelle génération de type « intelligence artificielle », basés sur des techniques d'apprentissage ou « Machine learning » (les méthodes d'apprentissages sont variées, on peut citer par exemple le « deep learning[25] », « Convolutional Neural Network[26] », ...).

Cette nouvelle génération de traitement algorithmique est en plein essor et présente un énorme potentiel, permettant d'exploiter des données massives (le « big data »), augmentant la précision des résultats obtenus, offrant de nouvelles perspectives dans le domaine de la prédiction.

De nombreuses solutions basées sur ces algorithmes de nouvelle génération sont dès à présent disponibles dans des domaines d'applications très variés. L'illustration ci-dessous (Figure n°7) diffusée par l'AFP montre quelques exemples d'applications de l'IA en 2016, on y voit que la plupart sont dans le domaine de l'IoT. On y trouve des solutions d'assistants personnels ou de domotique, le système d'intelligence artificielle Watson d'IBM sélectionné par différentes sociétés dont récemment la SNCF[27], les essais de véhicules autonomes.

Dans le domaine de la sécurité routière, l'apport de l'IA aux véhicules autonomes pourrait se traduire par une baisse conséquente des accidents de la route grâce à des voitures autonomes rendues plus réactives (en écartant la problématique de cyber sécurité, piratage des systèmes, voir partie II) : exemple de la voiture Tesla qui a pu éviter un accident en ayant détecté un ralentissement avant que celui-ci ne soit visible par le conducteur.

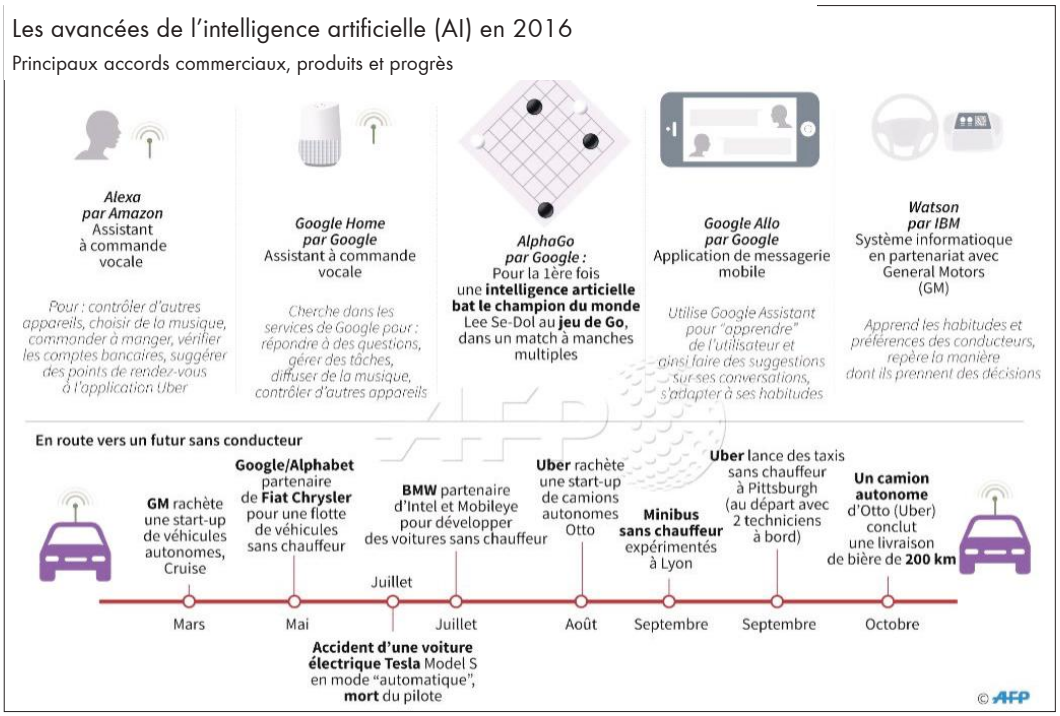
---

(25) L'apprentissage profond[1] (deep learning) est un ensemble de méthodes d'apprentissage automatique s'appuyant sur des architectures articulées de différentes transformations non linéaires.

(26) En apprentissage automatique, un réseau de neurones convolutifs est un type de réseau de neurones artificiels acycliques (*feed-forward*), dans lequel le motif de connexion entre les neurones est inspiré par le cortex visuel des animaux.

(27) https://www-03.ibm.com/press/fr/fr/pressrelease/51634.wss

Figure n°7 : exemples d'usages de l'intelligence artificielle



A noter également l'exemple de l'IA d'AlphaGo, un logiciel conçu par des chercheurs de Google ayant battu le champion du monde de jeu de Go, qui illustre la supériorité potentielle de cette nouvelle forme d'intelligence sur les capacités humaines. D'autres applications d'IA dépassent les capacités d'analyse de l'humain : un programme d'IA atteint un taux de détection des cancers de la peau plus élevé que les spécialistes[28].

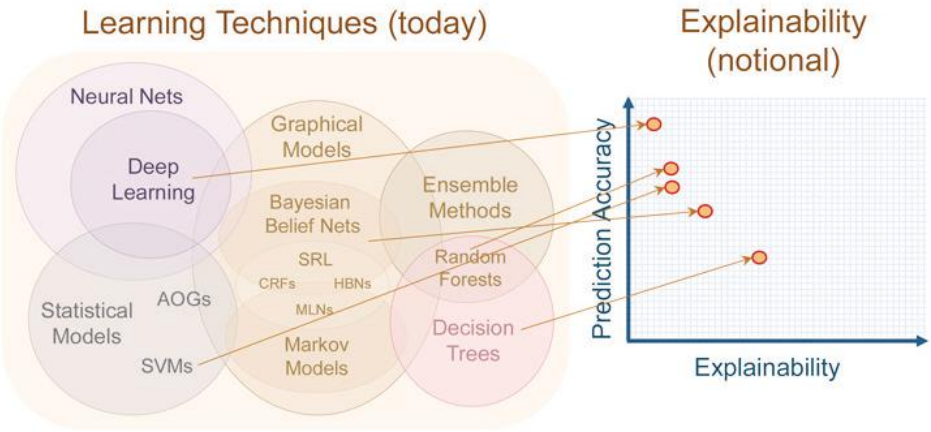
Problématiques des algorithmes de type IA dans le cadre de l'IoT : l'efficacité aux dépens de la transparence ?

L'apprentissage automatisé, le « deep learning » par exemple, a l'avantage de pouvoir atteindre des capacités de traitement très supérieures à celles des algorithmes classiques et des niveaux de fiabilité des résultats (ou des prédictions) très élevés. Par contre on ne maîtrise plus la logique de déduction de ces algorithmes et il devient donc, même pour le programmeur, difficile sinon impossible d'expliquer comment on arrive aux résultats atteints par l'algorithme. A ce sujet, Facebook a testé sur la semaine du 11 au 18 janvier 2012 la mise en œuvre de ce type d'algorithme auprès de 689 003 utilisateurs. Il a été clairement démontré à son issue qu'il était possible de manipuler leur état émotionnel[29].

La Figure n°8[30] illustre le fait que plus l'algorithme d'apprentissage est efficace (*Neural network* par exemple qui atteint des résultats précis et exacts), plus il sera difficile d'expliquer le raisonnement suivi et les décisions prises par cet algorithme. Des algorithmes plus transparents, dont le raisonnement est plus facilement explicable, tel que les arbres de décisions, seront par contre beaucoup moins efficaces.

(28) revue Nature http://www.nature.com/articles/nature21056
(29) https://www.forbes.com/sites/kashmirhill/2014/06/28/facebook-manipulated-689003-users-emotions-for-science/#75c346e5197c
(30) Article Le Monde Blog - 30-10-2016 – « l'intelligence artificielle va-t-elle rester impénétrable

Figure n°8 : relation entre les capacités prédictives de l'algorithme et sa transparence



Cela pose la question de la légitimité que l'on peut donner aux décisions ou aux prédictions de ces nouvelles formes d'algorithmes, et de la confiance que l'on peut leur accorder.

Des solutions sont évoquées dans le milieu scientifique pour répondre à cette problématique : faut-il par exemple prévoir que le programme soit en mesure de documenter lui-même de façon compréhensible pour l'homme ce qu'il a suivi comme raisonnement, faut-il se limiter à utiliser des algorithmes suffisamment transparents aux dépens de l'efficacité du traitement, etc.

Comme le rappel le livre blanc de l'ACERP sur l'IoT (*Préparer la révolution de l'internet des objets*, 7 novembre 2016), la confiance est au cœur de l'Internet de Objets. L'ACERP cite dans les principaux enjeux :

« L'adoption de l'internet des objets est conditionnée par la capacité d'assurer la confiance de l'utilisateur et du producteur de données ».

« Si la confiance des consommateurs et des entreprises productrices de données n'est pas établie, l'adoption de l'internet des objets sera limitée. Cette confiance se décline selon plusieurs aspects [....] : dans la protection des données et dans les traitements qui en sont faits de manière souvent centralisée ».

Cette confiance ne semble possible qu'avec un minimum de transparence dans les traitements effectués. Cette transparence est également une des recommandations (n°9) du rapport d'information objets connectés de l'assemblé nationale du 10 janvier 2017 : « Faire évoluer le Code de la consommation pour prévoir que les opérateurs de services aux personnes par l'intermédiaire d'objets connectés sont tenus de délivrer à ces personnes une information loyale, claire et transparente sur les conditions générales d'utilisation de ces services, portant notamment sur le recueil et l'éventuelle exploitation commerciale de données individuelles ».

Big Data et corrélation de données

Ces nouveaux algorithmes sont également très adaptés au traitement de données en masse (le « big data ») grâce à leurs capacités de traitement. L'étude des corrélations des données peut permettre de faire émerger des informations nouvelles. Ces nouveaux types de traitement des données sont donc fortement propices à trouver autre chose que ce que l'on cherchait. Cela pose des questions dans la maîtrise des données exploitées et l'utilisation potentielle qui peut en être faite. L'intelligence artificielle augmente ainsi les possibilités de détournement de la finalité des données collectées.

Cette problématique est mentionnée dans le livre blanc de l'ACERP sur l'IoT[31] « L'agrégation et le traitement de données provenant de sources hétérogènes constitue le cœur de l'internet des objets. Le détournement de la finalité des données collectées représente l'une des préoccupations majeures. »

Algorithme prédictif

Le traitement de données en masse est également propice au développement de systèmes de prédiction qui seraient en mesure, à partir de l'exploitation de données en temps réel et de modèle d'apprentissage, de prévoir des situations à risques par exemple avec un certain degré de probabilité et de prendre des décisions de manière autonome sur la base de ces risques potentiels.

Le croisement de ces données associé à une grande puissance de calcul autorise également l'apprentissage autonome continu et donc la capacité des logiciels de traitement à proposer des diagnostics inédits, selon un cheminement qui dépasse l'entendement humain.

Le récent rapport d'information du 10 janvier 2017 de l'assemblée nationale, déposé par la commission des affaires économiques sur les objets connectés, a émis une recommandation concernant « La principale force de l'utilisation des objets connectés : créer de la prédiction ». Cette recommandation (n°3) conseille de « Confier au pôle interministériel de prospective et d'anticipation des mutations économiques (PIPAME) une mission centrée sur le potentiel prédictif des objets connectés et sur leur impact dans les processus de décisions humaines »

Dans le domaine de la sécurité, des tentatives d'utilisation d'algorithme prédictif sont en cours et parfois sujet à questionnement. Prenant l'exemple du système *PREDPOL*[32], logiciel de police prédictive américain, qui prétend pouvoir prédire des lieux, date, heure de délits probables[33], afin d'influencer directement l'organisation de la police locale, il serait question d'un algorithme plus intelligent que les prévisions humaines. Cette assertion serait toutefois contestée par plusieurs analyses[34]. Il faut se garder d'accorder une confiance excessive aux prétendues capacités d'un tel algorithme de type « boîte noire ».

Intelligence Artificielle et responsabilité juridique

Le traitement des données dans un monde où les objets connectés, le big data et l'intelligence artificielle sont de plus en plus présents soulève également des questions d'ordre juridique.

Une des questions que l'on peut se poser, extraite d'un article publié sur le site d'Alain Bensoussan, avocat spécialisé dans le droit des robots[35], se résume ainsi :

« Qui est responsable de l'erreur inhumaine des « chatbots » (ces agents conversationnels capables de prendre des décisions, algorithme concentré d'intelligence artificielle) : le concepteur, l'utilisateur, le propriétaire ou le « chatbot » ? »

Ces algorithmes intelligents sont souvent centralisés, le traitement ne se fait donc pas sur l'objet connecté directement mais sur un système central déporté, ce qui complexifie la problématique de la responsabilité légale si ce système n'est pas résidant en France, ni même dans l'UE.

---

(31) Préparer la révolution de l'internet des objets, 7 novembre 2016.
(32) Ce système serait déployé dans les villes de Los Angeles, Atlanta, Charleston, New York City et Memphis
(33) http://www.predpol.com/
(34) http://www.internetactu.net/2015/06/23/predpol-la-prediction-des-banalites/
(35) https://www.alain-bensoussan.com/avocats/chatbots-erreurs-inhumaines/2016/05/06/

L'exemple des smart et safe cities, concentrés d'objets connectés

« Les « smart cities » sont des villes cherchant à résoudre les problèmes publics grâce à des solutions basées sur les technologies de l'information et de la communication grâce à des partenariats d'initiative municipale et en mobilisant de multiples parties prenantes[36] ». Ces « smart cities » *fusionnent des concentrés d'objets connectés et donc de capteurs mis en réseau grâce aux opérateurs de télécommunications, afin d'améliorer la qualité de l'espace urbain*.

L'émergence de ces cités intelligentes fait naître des questions juridiques et éthiques. En effet, elles récupèrent des quantités énormes de données : informations démographiques, de géolocalisation, style de vie et préférences des gens, données biométriques, santé, etc. Autant de données qui traversent plusieurs systèmes d'information et réseaux, provenant des objets connectés. Ces projets peuvent être positifs pour la sécurité publique car les données recueillies peuvent permettre d'établir des statistiques sur le niveau de délinquance urbaine dans certaines zones comme par exemple à Lyon.

Enjeux juridiques

Les questions posées par cette nouvelle gouvernance urbaine se situent avant tout au niveau de la protection des données personnelles. Il y a imbrication des sphères publique et privée, source de complexité supplémentaire.

Il faut rappeler qu'une obligation générale de sécurité incombe au responsable du traitement. En effet, l'article 34 de la loi Informatique et Libertés lui impose « de prendre toutes précautions utiles (...) pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ». Le non-respect de ces dispositions est puni par l'article 226-17 du code pénal de cinq ans d'emprisonnement et de 300 000 € d'amende, celle-ci pouvant atteindre 1 500 000 € pour les personnes morales.

La protection de la vie privée des personnes

La protection de la vie privée des personnes dont les données sont recueillies pour faire fonctionner une « smart city » est un enjeu majeur car le droit à la vie privée est un droit fondamental reconnu par les textes nationaux et internationaux.

Il y a lieu de concilier le recueil, l'utilisation de données personnelles, le respect du droit à la vie privée et l'existence d'un risque de surveillance de masse.

L'exemple de la géolocalisation montre les avantages et les inconvénients d'une ville intelligente. Cette technique permet de suivre les déplacements d'une ou plusieurs personnes grâce à un téléphone. Les opérateurs de télécommunications propriétaires des antennes sont capables de localiser des personnes dont ils détiennent le numéro de téléphone.

La responsabilité des acteurs

En matière de circulation routière, la question est essentielle. Les véhicules autonomes sont des voitures intelligentes pouvant se conduire toutes seules, sans que le conducteur ait quoi que ce soit à faire, grâce au fait qu'elles sont connectées à un système central les aidant à faire des choix (changement de file, etc.). Si un accident est causé par des dispositifs urbains interconnectés, à qui imputer la faute ? De multiples intervenants seraient susceptibles de voir leur responsabilité engagée (autorité publique locale qui est chargée de réguler la circulation, société ayant fabriqué le système intelligent...).

(36) Parlement européen « Mapping Smart Cities in the EU – Janvier 2014

Le statut des données

Les données personnelles caractérisent une personne. Elles sont détenues par des personnes morales (opérateurs de télécommunications, services publics sociaux, hôpitaux...). La question n'est pas tranchée concernant la propriété. La ville intelligente étant bâtie sur une multitude de données, il convient de déterminer qui en est le propriétaire, ceci afin de cadrer leur utilisation et leur éventuelle réutilisation. Si l'on identifie le propriétaire d'une donnée, lui seul pourra par la suite, sans contestation possible, utiliser cette donnée comme bon lui semble.

Le Conseil d'État, dans son rapport sur le numérique et les droits fondamentaux[37], a pris position pour ne pas reconnaître un droit de propriété sur ces données. Il prône la reconnaissance d'autres droits, comme un droit de regard sur l'utilisation des données concernant les citoyens.

Recommandations

Recommandation n°6 : fixer *a priori* les responsabilités juridiques des différents acteurs élaborant et mettant en œuvre des algorithmes de type « IA[38] ».

Type d'objets connectés par degré de sophistication	Nature juridique	Risques	Réponses juridiques ,techniques et problématiques
Objet de base Caméra, bracelet, etc	STAD	Cyberattaques, atteintes aux données personnelles	Loi dite Godfrain : atteintes aux STAD (art. 32161 à 323-4 du Code pénal Loi informatique et libertés et RGPD Responsabilité du fait des produits défectueux (art. 1386-1 à 1386-18 du code civil
Drones civils	STAD	Mise en danger Survol illégaux	les drones équipés d'un appareil photo, d'une caméra, d'un capteur sonore ou d'un dispositif de géolocalisation ne doivent pas :- porter atteinte à la vie privée (article L226-1 du code pénal),- prendre des vues aériennes pour des usages commerciaux, publicitaires ou professionnels (article D133-10 du code de l'aviation civile).
Bionique ,prothèse intelligente	STAD	Cyberattaques, responsabilité	vers un statut de l'homme augmenté
Objets connectés + IA =Robots	STAD et le propriétaire est le maître du système	Atteintes à l'innovation que constitue le robot -fraudes informatiques Cyberattaques en déni de service exploitant des objets connectés (cf rapport ANSSI 2016	Règles spécifiques par type de robots : vers un droit des robots ? Normes ISO pour les robots industriels Code d'éthique et charte

(37) Rapport, Le numérique et les droits fondamentaux www.conseil-etat.fr/.../Rapports.../Etude-annuelle-2014
(38) Intelligence artificielle

QUELLES RÉPONSES AUX CYBERATTAQUES ?

Du fait de leur développement, les objets connectés, à la fois cibles et vecteurs de cyber risques, augmentent considérablement la surface d'attaques numériques pour les cybercriminels. En effet, les risques portant sur la sécurité des systèmes d'information s'amplifient et il est à craindre que le développement de l'internet des objets n'accroisse encore ces failles. Les objets connectés sont largement vulnérables et peuvent ouvrir des brèches importantes sur les réseaux auxquels ils se connectent.

Il en a été ainsi lors de la cyberattaque contre l'hébergeur OVH qui a été attaqué massivement par des caméras de vidéoprotection infectées en vue de saturer son infrastructure. En cas de vol ou d'intrusion dans le terminal mobile contrôlant les objets connectés d'une maison, les alarmes, serrures et coffres forts seront alors déverrouillés et accessibles aux cambrioleurs.

Il conviendra d'étudier tout d'abord la typologie des cyberattaques visant les objets connectés (A) avant d'envisager les réponses techniques et juridiques et les préserver de ces dérives (B)

Constat et typologie des cyberattaques (usurpation, déni de service, falsification, divulgation, élévation de privilège)

Une cyberattaque est un acte malveillant dont l'objectif est de perturber un dispositif informatique via un réseau. Elle peut émaner de personnes isolées, d'un groupe de pirates ou d'organisations criminelles.

La cyberattaque peut viser des données personnelles, être dirigée envers une entreprise précise ou même viser un domaine de l'économie voire un Etat. Les conséquences de ces cyberattaques peuvent être économiques et financières, juridiques, « réputationnelles » voire politiques[39].

Avec le renforcement de la dépendance des entreprises à l'informatique (réseau, web, ...), l'émergence de nouveaux moyens de communication (smartphone, réseaux sociaux, ...) et le recours de plus en plus fréquent à l'externalisation (« cloud computing », « data centers », ...) on assiste à une montée en puissance des cyberrisques.

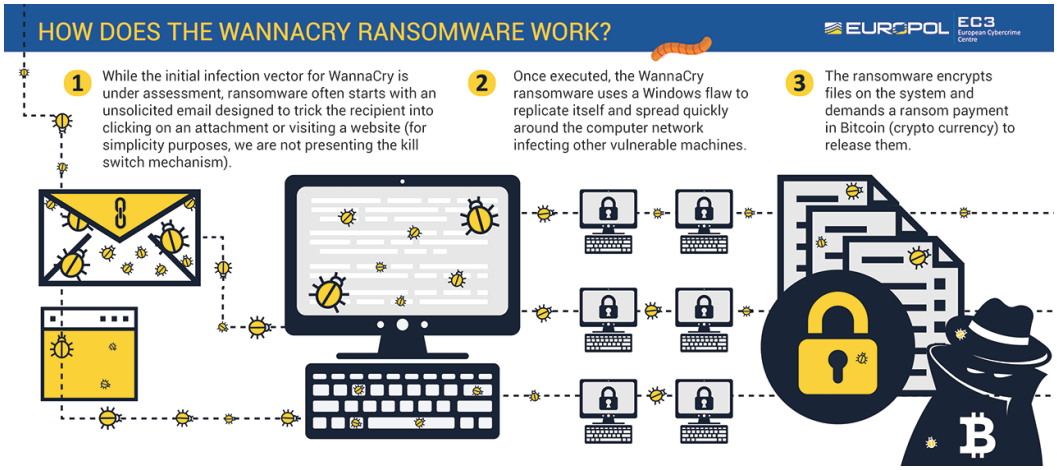
Le développement de cyberattaques extrêmement ciblées met en évidence les limites des mesures de sécurité et constitue une véritable menace pour les Etats ou les entreprises qui sont ciblés. Le site Consoglobe estime qu'il y a près de 120000 cyber attaques chaque jour dans le monde.

---

(39) Cf les propos de l'ex-Président Obama : *Il ne fait aucun doute que lorsqu'un quelconque gouvernement étranger essaye d'influencer l'intégrité de nos élections (...), nous devons prendre des mesures et c'est ce que nous ferons*. http://www.lemonde.fr/elections-americaines/article/2016/12/16/presidentielle-obama-annonce-que-les-etats-unis-vont-riposter-au-piratage-russe_5049770_829254.html#CyTIO3SruPaTtjpm.99

Le Cesin (Club des experts de la sécurité de l'information et du numérique) note que les entreprises françaises ont, en moyenne, dû affronter plus de 29 attaques en 2016, contre 13 l'année précédente. L'attaque la plus répandue est le « ransomware » (ou rançongiciel). Ce type de programme malveillant chiffre les données contenues sur un poste de travail ou un serveur et ne donne la clef pour les déchiffrer que moyennant le paiement d'une rançon. En 2015, 61 % des entreprises déclaraient en avoir été victimes. La dernière attaque en date, par ce type de logiciel malveillant, « Wannacry » a infecté entre le 12 et le 23 mai 2017 plus de 300000 ordinateurs dans 150 pays à travers le monde. Selon le concepteur de logiciels antivirus Avast, basé en République Tchèque, la Russie, Taïwan, l'Ukraine et l'Inde ont été les plus touchés. Les équipements les plus atteints utilisaient le système obsolète Windows XP et plus généralement toutes les versions antérieures à Windows 10 n'ayant pas effectué les mises à jour de sécurité. Cette cyberattaque est considérée comme le plus grand piratage à rançon de l'histoire d'Internet, Europol[40] la qualifiant « d'un niveau sans précédent » et ajoutant « qu'il ne faut en aucun cas payer la rançon ».

Figure 9 : fonctionnement du rançongiciel « Wannacry »



Parmi les plus importantes organisations touchées par cette attaque, on retrouve notamment les entreprises Vodafone, FedEx, Renault, Telefónica, le National Health Service, le ministère de l'Intérieur russe ou encore la Deutsche Bahn.

En 2016, deux chercheurs américains et un journaliste du magazine américain Wired ont récemment démontré que l'on pouvait prendre le contrôle à distance d'un véhicule connecté. Les chercheurs, depuis leurs salons, s'introduisent dans le système de contrôle d'une Jeep conduite par le journaliste. Ils prennent le contrôle à distance de la voiture en passant par le logiciel Uconnect, qui relie la Jeep à Internet. Ils actionnent ensuite, sans que le conducteur ne puisse rien faire, la ventilation, la radio puis le lave-glace. Par cette démonstration, les chercheurs et le journaliste souhaitent montrer la vulnérabilité des véhicules connectés face aux hackers. Pour un exemple de cyberattaque de grande envergure, voir l'annexe 2 sur les attaques des objets connectés par le malware Mirai.

Sécuriser les IoT peut souvent être difficile comme l'a souligné Flashpoint, une société de sécurité. Selon son enquête sur les récentes attaques DDoS à grande échelle, il n'est pas possible de modifier les informations d'identification par défaut de certains périphériques IoT car elles sont codées en dur dans ces périphériques, ce qui constitue une mauvaise pratique de sécurité et laisse ces appareils vulnérables indéfiniment.

(40) https://www.europol.europa.eu/wannacry-ransomware

Suite à des avancées technologiques et des demandes en matière de cybersécurité, la Commission européenne prépare une nouvelle législation[41] pour protéger les objets connectés. Elle vise à créer des règles qui obligeront les entreprises à respecter certaines normes de sécurité et à passer par des processus de certification complexes avant la mise sur le marché de ces produits.

L'ENISA travaille activement dans le domaine de l'IoT et des infrastructures intelligentes et a déjà publié plusieurs rapports[42] qui mettent en évidence les défis sécuritaires dans ce domaine en évolution ainsi que des bonnes pratiques et des recommandations.

« Les attaques par déni de service, en particulier avec l'essor d'objets connectés non sécurisés, vont continuer à harceler nos organisations. Malheureusement, ce que nous voyons n'est que le début en termes de « botnets » à grande échelle et de dommages disproportionnés », prédit Ben Johnson, ex-hacker pour l'agence de renseignement NSA et cofondateur de la société de sécurité informatique Carbon Black. Pour lui, la raison est simple : « Internet continue de se reposer sur des protocoles et une infrastructure conçus avant que la cybersécurité ne soit un problème ».

Développer une politique d'anticipation des risques

Aujourd'hui, les solutions de sécurisation des objets connectés ne constituent pas une priorité des constructeurs, et ne font pas encore réciproquement l'objet d'une demande clairement identifiée de la part des utilisateurs. Le manque de sécurisation des objets connectés ne résulte pas nécessairement d'un manque de vigilance : la sécurité rend difficile le fonctionnement même de certains objets, calibrés pour n'émettre parfois que quelques kilo-octets de données[43]. La sécurité des objets communicants ne constitue pas une préoccupation réelle des industriels selon la délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces (DMISC), dans son premier rapport[44] et ce sont les utilisateurs qui risquent de payer ce manque de vigilance. Elle considère qu'il existe « des risques pour la confidentialité des données personnelles, mais aussi pour l'intégrité physique des personnes ».

Le cryptage, qui complexifie le traitement des paquets envoyés et reçus, excéderait les capacités de l'objet connecté. En outre, les prestataires de services de sécurité pratiquent des tarifs souvent élevés, alors que le recours à l'internet des objets devrait être une source d'économies.

Parmi les solutions de sécurisation, on peut citer l'action des plateformes de « bug bounty »[45] qui peuvent permettre de contrôler par exemple avant commercialisation si les objets connectés contiennent des failles de sécurité. Le recours à ces plateformes largement développées aux Etats-Unis par des grandes entreprises comme par exemple Microsoft pourraient l'être également en France et en Europe car celles-ci pourraient contribuer à sécuriser le marché des objets connectés à la condition d'être labellisées par l'ANSSI par exemple.

---

(41) https://www.euractiv.com/section/innovation-industry/news/commission-plans-cybersecurity-rules-for-internet-connected-machines/

(42) Voir ENISA -, *Cyber Security and Resilience of smart cars* (janvier 2017), *Securing Smart Airports* (décembre 2016), *Cyber security and resilience for Smart Hospitals* (novembre 2016), *Architecture model of the transport sector in Smart Cities* (janvier 2016), *Security and Resilience of Smart Home Environments* (décembre 2015)

(44) http://www.interieur.gouv.fr/content/download/101311/797853/file/Etat-de-la-menace-Janvier-2017.pdf

(43) un modèle actuel de voiture connectée n'émet que 10 Mo de données par mois

(45) Un bug bounty est un programme proposé par de nombreux sites web et développeurs de logiciel qui permet à des personnes de recevoir reconnaissance et compensation après avoir rapporté des bugs, surtout ceux concernant des failles et des vulnérabilités.

Les réponses techniques/ juridiques aux cyberattaques

Du fait de la généralisation de l'usage des TIC et du développement de nouveaux usages (ie les réseaux sociaux cf. « Sécurité numérique et médias sociaux dans les entreprises en 2015 » Insee Résultats[46]), les entreprises ont parfaitement intégré les risques liés aux usages numériques : en 2015, 27% des sociétés de 10 personnes ou plus implantées en France déclarent avoir une politique de sécurité des TIC formellement définie (32% au niveau européen). Ce taux devrait continuer à s'accroître si l'on se base sur les menaces qui pèsent sur elles : 26% des sociétés de 250 personnes ou plus ont été touchées en 2015 par au moins un incident de sécurité au cours de l'année précédente, portant atteinte à l'intégrité, à la disponibilité ou à la confidentialité des systèmes et données informatique.

Réponses juridiques

Les objets connectés sont des systèmes de traitement automatisés de données (STAD) dont les atteintes sont sanctionnées par la loi « Godfrain ».

Si les évolutions technologiques ont permis de démocratiser la possession d'objets connectés, elles ont aussi conduit au développement de risques numériques et la commission d'infractions. Il peut s'agir de piratages sanctionnés en tant qu'atteintes auxSTAD, en cas d'accès ou de maintien frauduleux. L'article 323-2 du Code pénal réprime le « fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données ». Cette disposition pourra trouver à s'appliquer dans le cadre de dépôt de virus, chevaux de Troie et autres bombes logiques au sein du système d'information de l'IoT. Ce texte permet aussi de sanctionner l'introduction sans titre ni autorisation dans un service quelconque du réseau pour, par exemple, perturber les dispositifs de sécurité ou fausser le fonctionnement du système.

Les cyberattaques d'objets connectés peuvent aussi être réprimées sur le fondement de l'article 323-3 du code pénal qui sanctionne l'introduction frauduleuse de données dans un système de traitement automatisé, de l'extraction, de la détention, de la reproduction, de la transmission, de la suppression ou de la modification frauduleuse des données qu'il contient. L'installation d'applications parasites au sein du réseau de l'IoT pourra par exemple être sanctionnée sur ce fondement juridique. Pourra également être retenu l'article 323-1 du code pénal réprimant l'accès ou du maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données.

Quels défis pour la sécurité ?

Au niveau européen

La transposition de la directive NIS[47] approuvée le 18 décembre 2015 constituera également un progrès. Cette directive reprend dans une large mesure des dispositions similaires à l'article 22 de la loi de programmation militaire[48] en les généralisant à l'ensemble des États de l'Union européenne. Son domaine d'extension est au demeurant plus large, puisqu'il ne concernera pas les seuls OIV[49], mais tous les opérateurs dits essentiels à l'économie. La

(46) https://www.insee.fr/fr/statistiques/2121545?sommaire=2045120
(47) Directive on security of network and information systems (NIS Directive) voir https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
(48) https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&categorieLien=id

directive va s'appliquer aux opérateurs dans les secteurs suivants : l'énergie, les transports, les banques, les marchés financiers, la santé, le secteur de l'eau, l'infrastructure numérique (les points d'échange internet, les prestataires de services relatifs au système des noms de domaine, registres de nom de domaine de premier niveau), et également les entreprises importantes du secteur numérique ou « fournisseurs de services numériques ».

La directive prévoit également que les opérateurs concernés doivent prendre des mesures préventives afin de détecter tout risque concernant la sécurité du réseau informatique et mettre en place des mesures techniques de sécurité appropriées afin de gérer les risques liés à la sécurité des réseaux et aux systèmes d'information. Ces derniers auront également l'obligation de déclarer à l'ANSSI toute attaque et intrusion dans leur système informatique.

Les entreprises commercialisant des objets connectés investissant ces domaines seront donc soumises à ces obligations.

Au plan international

A titre d'exemple, la Federal Trade commission (FTC) américaine poursuit un fabricant, l'accusant de mettre en danger la sécurité des consommateurs et la confidentialité de leurs données, en raison de la sécurité inadéquate de son routeur et de ses webcams. L'objectif est de contraindre les fabricants à augmenter le niveau de conception des objets connectés, même ceux d'entrée de gamme[50].

Recommandations

Recommandation n°7 :
Rendre effectif le « privacy by design » et favoriser le rôle des entreprises de type « *bug Bounty* » pour la sécurisation des IoT.

(49) Opérateur d'importance vitale (décret sur la sécurité des activités d'importance vitale)
(50) https://www.droit-technologie.org/actualites/internet-objets-fabricants-mis-pression-augmenter-securite-objets-connectes/

QUELLES OPPORTUNITÉS POUR LES FORCES DE SÉCURITÉ ?

Une source de données à exploiter pour l'administration de la preuve pénale

S'agissant de l'exploitation des objets connectés en matière de police judiciaire, on pense en premier lieu à l'utilisation de terminaux mobiles de consultation de fichiers (cf. équipement prochain des policiers et gendarmes en tablettes connectées[51]), de capteurs automatisés (cf. lecteurs automatisés de plaques d'immatriculation ou LAPI) ou aux dispositifs mis en œuvre dans le cadre de techniques spéciales de surveillance (balises, dispositifs de sonorisation, drones...). Leur utilisation fera l'objet de développements plus poussés dans la sous-partie suivante, « B. Les objets connectés comme moyens de sécurisation ».

On songe moins naturellement à l'exploitation des objets connectés utilisés par des victimes ou par des criminels, et susceptibles à ce titre de contenir des informations utiles à la manifestation de la vérité dans le cadre d'enquêtes pénales.

Selon Mark Stokes, responsable de la police scientifique à Scotland Yard interrogé par le quotidien britannique *The Times*[52], « *les appareils ménagers dotés de capteurs et de microprocesseurs qui enregistrent les mouvements et les commandes des utilisateurs, permettront aux policiers de trouver des preuves lors d'investigations. Des empreintes numériques qui fourniront un aperçu crucial des derniers moments d'une victime, pourront confirmer ou démentir un alibi ou encore détecter des incohérences dans un témoignage* ».

Le *Washington Post* rapporte de son côté[53] que suite à un meurtre à Bentonville dans l'Arkansas, la justice a demandé à Amazon de livrer les enregistrements stockés sur leur serveur, car un objet connecté, un assistant virtuel « echo », se trouvait sur les lieux du crime. Cette enceinte est dotée d'un micro qui détecte la voix et peut exécuter un ordre (« Alexa, appelle-moi un Uber! ») ou répondre à une question (« Alexa, quel temps fait-il ? »).

Amazon refuse pour l'heure de déférer aux réquisitions qui lui ont été adressées par la justice américaine, invoquant le premier amendement de la Constitution américaine et le respect du droit à la vie privée.

Figure 10 : assistant connecté « echo » d'Amazon

En France, les services techniques spécialisés, et notamment le service central de l'informatique et des traces technologiques (SCITT) de la sous-direction de la police technique et scientifique (SDPTS) de la direction centrale de la police judiciaire (DCPJ), perçoivent le potentiel des objets connectés pour les enquêtes. Pourtant, si la saisie

(51) tablettes Néo pour la Police nationale et Néogend pour la gendarmerie nationale cf partie B « Les objets connectés comme moyens de sécurisation de ce rapport
(52) http://www.thetimes.co.uk/article/washing-machine-will-turn-detective-djq30jdff
(53) https://www.washingtonpost.com/news/the-switch/wp/2016/12/28/can-alexa-help-solve-a-murder-police-think-so-but-amazon-wont-give-up-her-data/?utm_term=.9ea29f421d66.

et l'exploitation forensique[54] des ordinateurs, des supports informatiques associés (disques durs externes, clés USB) et des téléphones mobiles sont désormais quasi systématiques, celles des autres objets connectés, pourtant potentiellement utiles et juridiquement possibles, demeurent pour l'heure marginales et exploratoires.

Le type de données exploitables

Comme les smartphones et tablettes, nombre d'objets connectés contiennent d'abord des données de géolocalisation : c'est le cas des GPS, dont c'est la fonction, mais également des véhicules connectés, des « wearables » de type bracelets électroniques, montres ou lunettes connectées, ou encore des drones.

L'analyse des journaux d'événements -actions commandées à l'objet connecté ou enregistrées par lui- peut également s'avérer intéressante pour l'enquêteur : ouvertures de portes de véhicules (pouvant indiquer la présence d'un passager), appairage de smartphones avec un véhicule ou une enceinte portable (pouvant indiquer la présence d'une personne donnée à un endroit donné), appareils de domotique (pouvant donner des indications sur la présence d'individus dans un domicile -horaires, durée, voire nombre-).

D'autres objets connectés sont susceptibles d'être exploités pour accéder à des contenus : outre les smartphones là encore, on pense aux enregistrements vidéos de caméras de vidéosurveillance, aux vidéos ou photos enregistrées dans la mémoire de drones, aux données liées à des appareils du domaine « santé-bien être », pour des enquêtes en recherche des causes de la mort, ou encore aux messages qui peuvent être échangés via les consoles de jeux, voire certains appareils électroménagers.

Le commissaire Cyril Gout, chef du SCITT, déclare ainsi lors de son interview par le groupe de travail[55] : « *on a recensé tous les objets pouvant avoir un intérêt, jusqu'à la domotique ou les appareils électroménagers, ce sont des choses qui pourraient être utiles en matière d'investigation. Ce n'est pas pour savoir quand est-ce que la bouteille de lait a été bue, mais plutôt l'usage détourné de ces appareils. Par exemple des parents ont expliqué que leur enfant se radicalisait. Les parents avaient supprimé le téléphone et les ordinateurs. Mais le gamin, avec la Playstation, jouait en réseau et s'en servait comme objet de connexion. De la même manière, le frigo peut s'ouvrir sur d'autres communications* ».

Les fragilités des objets connectés en termes de sécurité peuvent par ailleurs dans certains cas servir de portes d'accès aux contenus de smartphones (via les appariements à des véhicules par exemple). Dans le domaine plus particulier des enquêtes relatives à des cyberattaques de types DDoS (cf. Annexe 2), l'exploitation forensique des serveurs attaqués peut permettre d'identifier le type de botnets utilisés.

Les techniques d'exploitation disponibles

Selon les objets concernés, les données considérées pourront être récupérées dans les ordinateurs ou smartphones depuis lesquels ils sont pilotés, via les constructeurs et gestionnaires d'applications dédiées, ou encore dans l'objet connecté lui-même, s'il dispose d'une mémoire, d'une carte SIM ou d'une connexion externe (Wifi, Bluetooth, NFC, etc.).

---

(54) La science forensique, ou la forensique, applique une démarche scientifique et des méthodes techniques dans l'étude des traces qui prennent leur origine dans une activité criminelle, ou litigieuse en matière civile, réglementaire ou administrative (in criminologie.com).

(55) Entretien réalisé le 9 février 2017. M. GOUT était entouré de MM. Hugo LONGUESPE et Stéphane PEDRENO, affectés au SCITT.

La première situation ne pose pas de difficultés techniques particulières, dans la mesure où l'exploitation des ordinateurs et téléphones est une technique désormais largement maîtrisée, même si l'accès du FBI à l'Iphone de Syed Rizwam Farook, l'un des auteurs de la tuerie de San Bernardino (Californie) a nécessité le recours à des hackers, en raison des réticences affichées par Apple pour débloquer l'appareil[56].

L'autre cas soulève davantage de difficultés techniques. Souvent dotés de protocoles et formats de données propriétaires, les objets connectés exigent soit l'assistance technique du constructeur, par voie de réquisition (exemple de l'exploitation du boîtier GPS d'un véhicule Renault cité par la SCITT dans une affaire de terrorisme), soit une fastidieuse rétro-ingénierie, soit encore le recours à des outils forensiques spécialisés.

Selon un article consacré par le RCITD (Research Conference In Technical Disciplines) en octobre 2015 à « la pertinence des outils de forensique numérique pour l'enquête en matière de cybercriminalité dans l'Internet des objets et des services », ces outils restent toutefois à construire. A l'en croire, les solutions XRY[57] et UFED[58] sont les plus abouties à ce jour pour extraire de manière sécurisée des données d'appareils connectés de type GPS, MP3 ou tablettes récentes. Le logiciel iVe (Infotainement and Vehicle Systems Forensics permet l'exploitation des données de certains véhicules connectés (toutes les marques ne sont pas reconnues, et certaines marques, y compris européennes, ont des standards différents aux Etats-Unis et en Europe).

Ces outils encore en phase d'expérimentation ne tarderont pas à se développer, donnant plus d'autonomie aux services techniques spécialisés. Compte tenu de l'explosion prévisible du nombre d'objets connectés susceptibles d'être saisis à l'avenir sur les scènes d'infraction ou lors de perquisitions, il convient d'effectuer une veille technologique attentive dans ce domaine, et d'anticiper les investissements conséquents que nécessitera leur acquisition (les licences seront très coûteuses), au plan national ou dans le cadre de mutualisation au niveau européen. On peut citer à cet égard ce que propose déjà Europol avec le dispositif UFED qui permet l'extraction des données de 95 % des téléphones mobiles existants.

Une alternative pourrait être d'imposer aux fabricants souhaitant vendre leurs produits en France (ou mieux, dans l'Union européenne), le respect de certains standards techniques de nature à faciliter l'exploitation des données qu'ils contiennent, dans le cadre d'une potentielle procédure pénale ultérieure.

Au-delà de l'extraction, l'analyse soulève d'autres difficultés, compte tenu de la masse de données susceptibles d'être collectées, à terme, dans les enquêtes criminelles. D'ores et déjà, on compte en dizaines de « teraoctets » (To) les données relatives à de gros dossiers impliquant la saisie de multiples ordinateurs et téléphones (exemple des données -photos, vidéos, téléphonie- transmises pour analyse criminelle à l'équipe Fraternité d'Europol mise en place à la demande de la France et de la Belgique après les attentats du 13 novembre 2015). Le développement attendu de l'Internet des objets conduits certains experts[59] à tabler sur des volumes de données se comptant en « exaoctets » (1 Eo = 1018 octets = 1 000 000 To).

---

(56) Der Spiegel révélait en 2014, documents à l'appui, que la NSA disposait d'un accès libre aux informations contenues dans les iPhone. En l'occurrence le logiciel d'intrusion « DROPOUTJEEP » permettait à l'agence depuis 2008 de télécharger des fichiers contenus dans le smartphone, de consulter les SMS, le carnet d'adresses, l'agenda, d'écouter les messages téléphoniques et même d'activer le microphone et la caméra (http://www.spiegel.de/netzwelt/netzpolitik/nsa-ueberwachung-apple-verneint-kenntnis-von-spionageprogramm-a-941414.html).

(57) Logiciel forensique suédois (micro systemation) permettant d'extraire des données des portables et smartphones.

(58) Outil forensique utilisé par les services français, l'UFED (Universal Forensic Extraction Device) développés par Cellebrite permet l'extraction de données des ordinateurs, tablettes, GPS et smartphones.

(59) International Journal of engineering sciences and research technology (IJESRT) – « A review of cyber-crime Internet of things technologies, investigation methods and digital forensics, octobre 2015.

D'ores et déjà confrontés à ces problématiques de « big data », les services tentent de se doter d'outils adaptés, en favorisant des logiques de mutualisation au niveau européen (par exemple : l'analyse en masse de données vidéo par la plateforme PRISME, l'outil MVI[60] , le projet SIGMA TAU[61] , et, pour la recherche sémantique, l'outil LUXID de la DCPJ, développé avec le soutien d'Europol).

Il semble de plus en plus nécessaire de former les primo-intervenants sur les scènes d'infraction ou de crime et les enquêteurs menant des perquisitions -ainsi que les magistrats- aux opportunités et défis liés à l'Internet des objets. Nombre des nouveaux objets connectés apparaissent encore à leurs yeux comme de simples « gadgets » high-tech qu'un criminel paraît peu susceptible d'exploiter. Pourtant, certains criminels sont de véritables « geeks » cyberdépendants, d'autres sont inconscients des traces qu'ils peuvent laisser sur internet. En tout état de cause l'entourage des criminels, les victimes et les éventuels témoins seront de plus en plus utilisateurs d'objets connectés. L'explosion du marché laisse peu de doutes sur la probabilité croissante de rencontrer de nombreux objets connectés exploitables pour l'enquête (cf. les caméras et les véhicules, etc.).

C'est dans cet esprit que la sous-direction de la lutte contre la cybercriminalité (SDLC) de la DCPJ vient de diffuser une brochure consacrée aux « supports numériques dans la perquisition », expliquant de façon très didactique aux enquêteurs en perquisition ne disposant pas du concours de personnels formés (investigateur en cybercriminalité -ICC- ou primo-intervenant en cybercriminalité -PICC-) les actions à entreprendre et celles à éviter pour « préserver la preuve numérique sans altérer les données, connaître les matériels et la manière de les prendre en compte, ne manquer aucune information susceptible d'aider l'investigation ».

Le cadre juridique applicable

Les opérations techniques liées à l'exploitation des objets connectés en matière pénale paraissent couvertes, au plan national, par les diverses dispositions du code de procédure pénale (CPP) relatives au recueil de la preuve numérique.

Les données enregistrées, contenues ou transmises par un objet connecté peuvent en l'absence d'indications contraires de la jurisprudence être assimilées aux « données informatiques » auxquelles les officiers de police judiciaire sont autorisés à avoir accès lors d'une perquisition (articles 56 et 57 du CPP), y compris en accédant, depuis le lieu de perquisition ou depuis leur service, à un « cloud » ou à des applications distantes utilisées depuis des systèmes informatiques saisis lors de la perquisition.

De la même manière, les articles 60-1 (flagrance), 77-1-1 (préliminaire) et 99-3 (instruction) permettent la réquisition « de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique qui sont susceptibles de détenir des informations intéressant l'enquête, y compris celles issues d'un système informatique ou d'un traitement de données nominatives, de lui remettre ces informations, notamment sous forme numérique, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel », dès lors que les informations concernées ne sont pas des correspondances échangées (cf. arrêt de la Cour de Cassation « Ciprelli », du 6 novembre 2013). Les constructeurs, gestionnaires de « cloud » ou d'applications associés à des objets connectés sont concernés.

---

(60) Morpho Video investigator.
(61) Système d'indexation et de gestion massive audiovisuelle traitement analytique universel.

Les dispositions introduites par la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, relatives à « l'accès, à distance et à l'insu de la personne visée, aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique » (articles 706-95-1 du CPP) sont également utilisables pour des objets connectés « communicants » (de type console de jeu ou appareil ménager).

Il en est de même de la captation de données informatiques prévue par les articles 706-102-1 et 2 du code de procédure pénale, mécanisme assimilable à l'utilisation d'un logiciel « espion » qui prend partiellement le contrôle du terminal informatique visé, afin d'en extraire les données de manière furtive, avec l'avantage de contourner le chiffrement des communications.

Le recours à la géolocalisation en temps réel s'applique également à tout objet, soit par l'exploitation de sa propre technologie, soit au travers de la pose d'une balise, dès lors que les conditions posées aux articles 230-32 à 230-44 et suivants du CPP, issus de la loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation sont respectées. Les opérations permettant de retracer ultérieurement des déplacements ne sont pas concernées-elles relèvent de la réquisition- non plus que le suivi dynamique d'un objet lorsqu'il a pour but de retrouver cet objet ou son propriétaire ou possesseur légitime, victime ou personne disparue.

Les articles 60-3 (flagrance), 77-1-3 (préliminaire) et 99-5 (instruction) ont enfin simplifié l'exploitation de la preuve numérique. Ces dispositions permettent la réalisation de copie de travail sans recours à l'expertise judiciaire, qui demeure toutefois recommandée par la Direction des affaires criminelles et des grâces du ministère de la justice pour des dossiers particulièrement sensibles.

Recommandation

Recommandation n°8 :
former les acteurs (sécurité et justice) aux problématiques et techniques spécifiques à l'IoT. Développer la recherche et l'acquisition d'outils de forensique numérique de nature à faciliter l'exploitation des objets connectés, dans le cadre notamment d'une démarche européenne et en lien avec les acteurs privés, y compris les fabricants.

Les objets connectés comme moyens de sécurisation

« Les innovations techniques ne sont plus des gadgets mais modifient les façons de travailler des forces de sécurité ». Par ces mots, le commissaire Vincent Gorre[62] résume la transformation des méthodes de travail engendrée par les objets connectés qui participent à la modernisation des institutions tant régaliennes que privées dans le domaine de la sécurité.

Certains objets sont d'ores et déjà utilisés au sein du ministère de l'Intérieur qui se positionne ainsi comme l'un des acteurs les plus innovants en matière de technologies numériques. D'autres sont testés à titre expérimental.

Trois types d'objets connectés semblent être les plus novateurs, transversaux et prometteurs pour le ministère de l'Intérieur dans sa mission de police administrative c'est-à-dire avant la commission d'une infraction :

- ✓ La tablette numérique,
- ✓ La vidéo intelligente
- ✓ Le drone

La tablette numérique

La gendarmerie et la police nationales ont lancé un projet ambitieux, s'inscrivant dans le cadre du Plan de modernisation de la sécurité intérieure, respectivement nommés Néogend et Néo (pour Nouvel Equipement Opérationnel). Ce projet a pour but de déployer des équipements connectés (smartphones et tablettes).

Après une phase expérimentale (principalement dans le département du Nord pour la gendarmerie et en Seine-Maritime pour la police nationale), la police nationale a entrepris un plan d'investissement de 50000 appareils sur trois ans (dont plus de 28000 seront livrés dès 2017) et la gendarmerie a choisi d'équiper chaque gendarme de cet outil.

Ces équipements sécurisés, totalement identiques pour les deux forces, bénéficient également des mêmes applications et offrent une mobilité accrue aux utilisateurs et donc davantage d'autonomie, de disponibilité et donc d'efficacité.

Les possibilités offertes par cet outil connecté sont multiples, rapides et évitent notamment de passer par les ondes radio : constatations d'infractions facilitées (application « Crim'in »), interrogations de fichiers, accès aux diverses messageries, à Internet et à l'extranet, verbalisation des infractions, prise de notes. Très fonctionnel[63], l'outil permet de prendre en photo les bandes MRZ[64] sur les titres (carte d'identité, passeport, certificat d'immatriculation), de récupérer les données sans les ressaisir manuellement et consulter les différents fichiers avec cette donnée captée (fichier des personnes recherchées notamment).

---

(62) Entretien du 24 mars 2017 avec le commissaire Vincent Gorre de l'état-major *de la direction de la sécurité de proximité de l'agglomération parisienne (DSPAP).*

(63) Entretien du 7 avril 2017 avec le commissaire divisionnaire Philippe Saunier, conseiller technologies de sécurité intérieure au cabinet du directeur général de la police nationale.

(64) Une zone de lecture automatique, ou zone de lecture optique (Machine-Readable Zone - MRZ) est une zone, sur un document officiel, réservée à la lecture, à l'identification et à la validation de ce document.

Ce nouvel équipement numérique rapproche également les citoyens des gendarmes et policiers. Par exemple, le suivi des usagers inscrits dans le cadre de l'« opération tranquillité vacances » est facilité par la visualisation sur une carte des résidences avec un code couleur révélant celles qui n'ont pas fait l'objet d'une surveillance au cours des derniers jours.

Une application de cartographie opérationnelle permet en outre la géolocalisation des patrouilles environnantes et des événements en cours. Elle constitue un outil d'aide à la décision et facilite la gestion opérationnelle des interventions.

Enfin, une messagerie opérationnelle de type « chat » permet à plusieurs équipages d'échanger directement entre eux et avec leur centre d'information et de commandement sur un événement.

La vidéo intelligente

La surveillance vidéo de la voie publique (rues, routes, etc.) ou d'un lieu ouvert au public (gares, mairies, etc.) peut être autorisée pour différents motifs, le public devant être informé de l'existence du système de vidéoprotection.

La vidéoprotection est un moyen de surveillance accru qui permet d'optimiser la couverture du territoire par des moyens humains, pour empêcher la commission d'infractions voire favoriser l'interpellation en flagrant délit grâce aux opérateurs qui dirigent les forces engagées. Elle permet également aux enquêteurs d'identifier des auteurs d'infraction et d'élucider des affaires judiciaires[65] par l'exploitation des films, en continu ou *a posteriori*.

L'augmentation exponentielle de la vidéoprotection (plus d'un million de caméras en France) rassure une partie de l'opinion bien que la plupart des scènes filmées par les caméras ne soient pas réellement regardées par un agent.

Elle est avant tout un outil dissuasif, sous exploité faute de moyens humains. La vidéo intelligente est née de ce constat. Elle est, en région parisienne, une conséquence du plan zonal de vidéoprotection. L'objet de ce plan est de relier les 1 200 caméras de voie publique de Paris, de la petite et de la grande couronne, puis d'étendre ce maillage à la SNCF, la RATP... Des travaux d'adaptation et de refonte des principales interconnexions avec la RATP ou la SNCF sont actuellement conduits. Techniquement, la qualité de l'image s'améliore puisqu'on passe à la haute définition.

L'avance de Paris en matière de vidéoprotection a été probablement facilitée par les conditions de mise en œuvre dans la mesure où c'est l'Etat qui a financé et organisé le système de vidéoprotection. Au contraire, sur tout le reste du territoire national, cela ressort de la compétence du maire, qui pour des raisons politiques ou budgétaires, peut avoir un avis bien différent de celui des autorités de police en privilégiant l'installation de matériel moins onéreux et moins performant.

Les possibilités technologiques de la vidéo intelligente sont pourtant multiples : reconnaissance faciale et lecture automatisée de plaques d'immatriculation, recherche d'objets particuliers ou de véhicules, reconnaissance de mouvements particuliers (par exemple une personne qui tombe, un changement de rythme, une personne qui circule à contre-sens dans la foule,...), recherche d'une forme, d'une couleur, d'un itinéraire, pistage d'un individu, d'un objet ...

Toutefois, selon la finalité, le cadre juridique diffère. Dans un cadre judiciaire[66], les nouvelles techniques actuellement testées ont été impulsées par un projet européen après les attentats terroristes de novembre 2015 à Paris. Les forces de sécurité travaillent aujourd'hui à un projet

(65) La conservation des images ne peut pas dépasser 1 mois.
(66) Entretien avec le commissaire Cyril GOUT, chef du service central de l'informatique et des traces technologiques, le 7 avril 2017.

global et dimensionnant : « SIGMA-TAU » pour Système d'Indexation et de Gestion en Masse de l'Audiovisuel et Traitements Analytiques Universels. Il s'agit d'un outil « socle » capable de préparer la donnée vidéo (indexation et formatage) avant son traitement et de restituer les résultats après traitement à l'enquêteur. Sur ce socle pourront s'ajouter différents modules d'analyse des vidéos qui seront utilisés selon les besoins.

En revanche, l'utilisation des mêmes outils avant la commission de toute infraction n'est pas autorisée tant qu'une loi (avec une instruction du dossier par la CNIL) spécifique n'est pas votée. Néanmoins, la vidéo intelligente peut être utilisée pour une finalité plus restreinte en police administrative. Elle est par exemple utilisée à titre expérimental en France pour sécuriser et fluidifier les passages aux frontières. Ainsi à Roissy, la vidéo permet de faire une reconnaissance faciale et de comparer les traits du visage avec la photographie du passeport biométrique (système « PARAFE[67] facial »).

D'une manière générale, la pleine efficacité d'un dispositif de vidéoprotection repose sur plusieurs critères :

- ✓ une détection le plus en amont possible des situations sensibles par le vidéo-opérateur (en cela la vidéo intelligente permet justement d'attirer son attention sur une caméra qu'il n'aurait peut-être pas visualisée). L'intérêt de la vidéo intelligente est donc de susciter des alertes pour attirer l'attention de l'opérateur sur une scène susceptible d'être anormale : des individus en train de se battre, recherche d'un objet immobile dans un espace où il y a du passage, vitesse d'un piéton anormale...
- ✓ une bonne coordination du vidéo-opérateur avec les effectifs de terrain ;
- ✓ un pré-positionnement efficace (et une disponibilité) des effectifs sur le terrain, qui doivent intervenir rapidement sur la situation signalée.

Il convient toutefois de rappeler que ce n'est pas tant la gestion des images en masse qui va aider l'enquêteur ou le « télésurveilleur » mais souvent l'accès aux images. Ainsi, il faut accroître la démarche de normalisation des technologies utilisées sur ces dispositifs publics et ceux utilisés par des sociétés privées chargées d'une mission de service public considérées comme sites sensibles (Opérateurs d'Importance Vitale – gares, aéroports ...). Il faut également songer à la captation, à l'acheminement et au stockage de ces images. En effet, aujourd'hui, les enquêteurs sont confrontés à la masse de données à récupérer, à leur dispersion et au transport vers des plates-formes de traitement (plus d'une semaine pour rapatrier les vidéos de Nice).

Cette réflexion est d'autant plus nécessaire que le nombre de vidéos postées sur les réseaux sociaux que les policiers vont devoir exploiter croît de manière exponentielle.

Drones : un enjeu pour la sécurité

Le drone est un moyen aérien radio commandé à faible rayon d'action qui suscite un intérêt croissant et qui se démocratise. Il n'intéresse d'ailleurs pas seulement les forces de sécurité intérieure et de Défense. Le drone connaît en effet un engouement dans des domaines variés auprès de nombreux professionnels : architectes, archéologues, agriculteurs, cinéastes, couvreurs... sans compter le grand public qui apprécie son caractère ludique et pratique. Mais il peut aussi être utilisé par des individus ou des organisations de façon malveillante comme les survols de sites sensibles entre l'automne 2014 et le printemps 2015 l'ont montré.

---

(67) PAssage RApide aux Frontières Extérieures : système permettant un passage automatisé des voyageurs aux frontières avec lecture optique du passeport et des empreintes digitales.

En ce qui concerne les opérations militaires, les interventions en Irak et en Afghanistan ont démontré l'utilité de disposer de moyens aériens militaires pour des missions sans exposer la vie des pilotes. Au Yémen, c'est même officiellement le seul moyen d'action actuel des américains pour lutter contre Al Qaïda.

Dans le domaine de la sécurité intérieure, les drones occupent une place de plus en plus importante dans la stratégie opérationnelle. Un rapport d'inspection[68] les considère comme un complément plutôt qu'une alternative à l'hélicoptère. Si leur emploi est soumis à de fortes restrictions de nuit, en zone urbaine, par temps venteux ou à proximité des aéroports, il n'en demeure pas moins que les progrès technologiques rendent leur utilisation très attractive. Ils pourraient même remplacer les moyens pilotés grâce à leurs qualités d'observation parfois supérieures et leur discrétion.

Le drone présente surtout l'avantage de réduire les risques physiques des personnels engagés lorsque l'environnement est hostile comme par exemple lors de violences urbaines.

Selon le rapport d'inspection, environ 45 drones sont en service en avril 2016, sans compter une dizaine de nanodrones. Ils sont répartis entre le secteur de la sécurité civile (notamment pour la surveillance des feux de forêts), la Police nationale et la Gendarmerie nationale.

Le rapport regrette que les initiatives des directions ministérielles concernées soient intervenues dans un premier temps en ordre dispersé.

Pour les exemples, la doctrine d'emploi et la cartographie des risques, voir l'Annexe 1 « Les drones et la sécurité intérieure ».

Recommandations

Recommandation n°9 :
assouplir la réglementation pour l'utilisation des drones à usage régalien dans l'espace public aérien.

Recommandation n°10 :
Accélérer le processus d'adoption de la vidéo intelligente par l'évolution du cadre juridique et assurer l'interopérabilité des systèmes publics et privés.

(68) Rapport IGA-IGAS-CGEFI-CGA n° 16050-16018-2 : Revues de dépense 2016, « Les hélicoptères de service public ».

Les objets connectés et le renseignement intérieur

« A l'avenir, les services de renseignement pourraient utiliser l'Internet des objets pour l'identification, la surveillance, le contrôle, la localisation, le recrutement, ou pour accéder à des réseaux ou des informations d'identification utilisateur ».

C'est en ces termes ambitieux que James Clapper s'exprimait devant un comité du Sénat américain, en février 2016. Celui qui a été directeur du renseignement américain de 2010 jusqu'à 2017, à la tête des dix-sept agences, s'enthousiasmait des *« nouvelles opportunités »* offertes par le développement du marché des objets connectés.

Début mars, des révélations du site Wikileaks ont donné un aperçu de ces possibilités. Comme le rapporte un article du *Monde* - *« Iphone, Android, télés connectées... comment la CIA espionne »* - WikiLeaks a mis en ligne *« un gigaoctet de fichiers datés de 2013 à 2016, issus du réseau interne de la CIA, qui détaillent certains programmes d'espionnage électronique de l'agence »*. On apprend notamment à cette occasion que la CIA et le MI5, le service de renseignement britannique, peuvent, grâce à un logiciel espion (« malware »), utiliser des téléviseurs connectés en apparence éteints pour enregistrer le son environnant et le transmettre à un serveur distant. D'autres logiciels espions peuvent s'attaquer aux systèmes d'exploitation qui équipent les appareils Apple ou Android. La CIA s'intéresserait également à la possibilité de prendre le contrôle de véhicules grâce à leurs instruments électroniques.

Comme c'est le cas pour des acteurs économiques, mais aussi pour des forces de sécurité intérieure en matière d'ordre public ou de police judiciaire, les services de renseignement utilisent les objets connectés lorsqu'ils procèdent par exemple à la sonorisation d'un lieu ou d'un objet et que le micro émet une information en temps réel. De la même manière, une balise qui renseigne en temps réel sur la position par exemple d'un véhicule ou d'une personne, est un objet connecté. La caméra peut aussi être appréhendée en tant que telle.

D'autres techniques donnent accès à des « données de connexion ». Elles sont abordées ici brièvement, sans viser à l'exhaustivité.

L'algorithme

Le traitement des données de connexion par algorithme est prévu à l'article 851-3 du code de la sécurité intérieure dans les termes suivants : *« Il peut être imposé aux opérateurs et aux personnes mentionnés à* l'article L. 851-1 la mise en œuvre sur leurs réseaux de traitements automatisés destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste ». Interrogée, la Commission nationale de contrôle des techniques de renseignement (CNCTR[69]) assure que « cette technique n'est pas mise en *œuvre* ».

La géolocalisation en temps réel

L'article 851-4 du code de la sécurité intérieure prévoit que « les données techniques relatives à la localisation des équipements terminaux utilisés mentionnées à l'article L. 851-1 peuvent être recueillis sur sollicitation du réseau et transmis en temps réel par les opérateurs à un service du Premier ministre ». Les équipements terminaux peuvent être entendus comme le téléphone, l'ordinateur ou encore la tablette.

(69) Voir annexe 4 sur le rôle de la CNCTR

L'IMSI-Catcher

L'IMSI-Catcher est un équipement portable discret qui simule une antenne-relais pour les téléphones portables de son environnement : il enregistre alentour les numéros IMSI (International Mobile Number Scrubber Identity), c'est-à-dire le numéro de la carte SIM du téléphone, et le numéro IMEI (International Mobile Equipment Identity), celui du boîtier. Il permet donc d'identifier les boîtiers présents en vue d'effectuer leur surveillance.

Ainsi que le prévoit l'article L851-6 du code de la sécurité intérieure, « peuvent être directement recueillies, au moyen d'un appareil ou d'un dispositif technique mentionné au 1°de l'article 226-3 du code pénal, les données techniques de connexion permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur ainsi que les données relatives à la localisation des équipements terminaux utilisés ».

L'IMSI-Catcher est un moyen d'identification qui permet de connaître le numéro de téléphone. Plusieurs catchs établissant la présence récurrente d'un IMEI-IMSI.

L'IMSI-Catcher peut aussi permettre une interception de correspondances, un peu à la façon d'une interception de sécurité de proximité. Il capte ainsi le contenu d'une conversation. Selon la CNCTR, « cette technique est extrêmement peu utilisée ». Seules deux finalités peuvent par ailleurs être invoquées : la prévention du terrorisme et l'indépendance nationale, l'intégrité du territoire et la défense nationale. « Ce type d'utilisation correspond à des situations opérationnelles exceptionnelles », explique la CNCTR dans son rapport d'activité 2015/2016. Interrogée, la CNCTR précise que, dans sa doctrine, l'instance de contrôle veille à ce qu'une telle utilisation reste limitée à un « urgence opérationnelle ».

Les services de renseignement peuvent aussi procéder à du recueil et de la captation de données informatiques[70]. Ainsi que le prévoit l'article L 853-2 du Code de la sécurité intérieure, les services peuvent recourir à « l'utilisation de dispositifs techniques permettant d'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels ». L'objet qui contient ces données informatiques n'est pas précisé. Il peut donc tout aussi bien s'agir d'un ordinateur que d'une machine à laver, d'une brosse à dents ou d'un four si celui-ci stocke ce genre de données.

Les interceptions de sécurité : Technique particulièrement intrusive, elle permet, via l'opérateur, d'intercepter tous les flux, qu'il s'agisse des voix, des SMS, des données Internet telles que les données de navigation ou les mails. Comme toutes les techniques de renseignement, elles doivent faire l'objet d'une autorisation du Premier ministre après avis de la CNCTR.

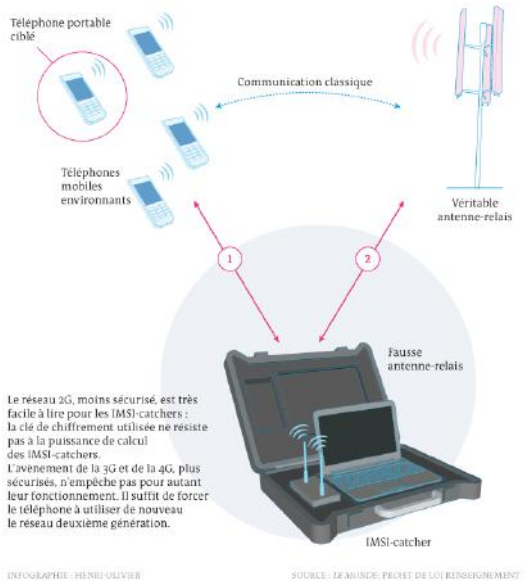
Un contrôle progressif et récent

Le contrôle des techniques de renseignement a longtemps été inexistant. Interviewé par *Le Monde* en 2013 alors qu'il venait de rendre un rapport sur le sujet, Jean-Jacques Urvoas, à l'époque président de la commission des lois à l'Assemblée nationale, disait : « En France, nous sommes au degré zéro en termes de contrôle des activités de renseignement » (*Le Monde*, « Urvoas : «Je n'ai pas rencontré de programme de surveillance similaire en France» », 12 juin 2016). Celui qui allait devenir Garde des Sceaux sous la présidence de François Hollande

(70) La position d'un service de renseignement américain est assez claire à ce sujet : «il faut contrôler toute la botte pour pouvoir y retrouver une aiguille» (général Keith Alexander, ancien chef de la NSA jusqu'en 2014)

ne s'y est pas trompé. Le dispositif de contrôle des atteintes à la vie privée et au secret des correspondances ne reposait alors que sur la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications. Dans les faits, ce contrôle ne s'exerçait que sur certaines techniques, les autres – comme par exemple l'utilisation de balise de géolocalisation, la captation d'image et de son - étant réputées ne pas exister. En réalité, elles étaient mises en œuvre en dehors de tout cadre légal. La loi renseignement du 24 juillet 2015 a contribué à mettre à jour le cadre juridique légal, même si d'aucuns ont critiqué ses lacunes à différents égards. Des critiques ont notamment été formulées vis à vis de l'exception dont peut souffrir le contrôle systématique et anticipé des techniques de renseignement (« en cas d'urgence absolue ») ; ou par rapport au fait que l'entourage des personnes soupçonnées de commettre une infraction peut également faire l'objet de surveillance.

IMSI-catcher exposé au Deutsches Technikmuseum Berlin



CONCLUSION

Il serait vain d'envisager, sous un format aussi contraint que celui de ce rapport, répondre de façon exhaustive à la question du juste équilibre entre la nécessaire protection des données personnelles et l'utilisation de celles-ci de façon poussée par les forces de sécurité pour mener à bien des investigations de plus en plus complexes.

La demande sociale en matière de sécurité, la généralisation d'objets de plus en plus connectés, dont on se demande pour certains si la connexion apporte réellement quelque chose de plus à l'utilisateur ou s'il s'agit seulement pour le fabriquant d'être en capacité de capter massivement de l'information personnelle, sont autant de menaces qui pèsent sur la protection des données personnelles.

L'individu « consommateur » a pour sa part besoin d'être tenu informé de façon transparente, pertinente et équitable de la transformation massive de biens de consommation qui deviennent de véritables « concierges numériques[71] » *connaissant de plus en plus de choses sur chacun grâce aux données personnelles qui sont captées, traitées et échangées par l'Internet des objets*.

Il paraît clair aujourd'hui que le cadre législatif actuel semble dépassé vis-à-vis du phénomène sociétal des objets connectés et particulièrement pour les plus sophistiqués d'entre eux, les robots. L'intégration de plus en plus d'intelligence artificielle dans les objets connectés, comme la synthèse vocale, la vision par ordinateur, le calcul dans le cloud, du machine learning posera à l'avenir de nouvelles problématiques juridiques et techniques qu'il faut s'efforcer d'anticiper.

Bien évidemment ces objets représentent grâce à leur contenu technologique et leur omniprésence dans tous les compartiments de notre environnement de formidables outils pour les forces de sécurité, tant sur le plan de la conduite « forensique » *d'une enquête que d'un usage* opérationnel pour le maintien de l'ordre ou le renseignement.

Les objets connectés constituent un atout indéniable pour la lutte contre la criminalité mais ils représentent aussi une menace lorsqu'ils sont utilisés de façon malveillante par exemple dans le cas de cyberattaques (ransomware, DDoS,...) mais également pour faciliter la commission de crimes ou de délits (surveillance de logements pour faciliter les cambriolages, pose de balise sur des véhicules afin de pouvoir les voler, ...). Cet angle particulier de l'usage des objets connectés pour faciliter les activités criminelles n'a pu être abordé dans ce rapport mais pourrait constituer à lui seul un sujet de recherche à part entière.

(71) Expression tirée de l'ouvrage de Marc Dugain et de Christophe Labbé

RECOMMANDATIONS

Recommandation n° 1 :
Adapter une réglementation spécifique aux objets connectés au plan au moins européen.

Recommandation n°2 :
Sensibiliser les consommateurs aux usages et risques des objets connectés par un plan national d'information. Apposer une signalétique spécifique « IoT » (cf figure n°6) précisant le caractère connecté de l'objet ainsi que son niveau de sécurité (type critère commun de l'ANSSI). Y associer les startups françaises de type « bug bounty » Yogosha et Bounty Factory.

Recommandation n°3 :
Renforcer les règles en matière de consentement des utilisateurs avec la possibilité d'alerter sur les risques associés à cette transmission et garantir la proportionnalité entre le service rendu et le type de données collectées.

Recommandation n°4 :
Valoriser les bonnes pratiques des entreprises et mettre en place une notation « Empreinte numérique » » (type Fitch, S&P, ...) par la CNIL permettant d'évaluer les objets connectés de manière équitable et transparente.

Recommandation n°5 :
Renforcer les moyens des instances de contrôle (CNIL, ARCEP, ...). Mettre en place une certification délivrée par ces mêmes instances à certaines structures agréées pour exercer ce contrôle. Prévoir et publier les sanctions.

Recommandation n°6 :
fixer les responsabilités juridiques des différents acteurs élaborant et mettant en œuvre des algorithmes de type « IA ».

Recommandation n°7 :
Rendre effectif le « privacy by design » et favoriser le rôle des « Bug Bounty » pour la sécurisation des IoT.

Recommandation n°8 :
Former les acteurs (sécurité et justice) aux problématiques et techniques spécifiques à l'IoT. Développer la recherche et l'acquisition d'outils de forensique numérique de nature à faciliter l'exploitation des objets connectés, dans le cadre notamment d'une démarche européenne et en lien avec les acteurs privés, y compris les fabricants.

Recommandation n°9 :
Assouplir la réglementation pour l'utilisation des drones à usage régalien dans l'espace public aérien.

Recommandation n°10 :
Accélérer le processus de vidéo intelligente par l'évolution du cadre juridique et assurer l'interopérabilité des systèmes publics et privés.

BIBLIOGRAPHIE

Rapports et dossiers

- ANSSI, rapport 2016
- CNIL, Cahier IP no2, mai 2014, Le Corps, nouvel objet connecté, Du « Quantified self » à la M-santé : les nouveaux territoires de la mise en données du monde - www.cnil.fr
- C. Erhel et L. de La Raudière, rapport d'information sur les objets connectés, 19 janvier 2017, http://www.assemblee-nationale.fr/14/rap-info/i4362.asp
- Rapport INHESJ : sécurité des objets connectés : https://www.inhesj.fr/
- Big Data et objets connectés, faire de la France un champion de la révolution numérique rapport institut Montaigne, avril 2015
- OCDE (2015), *Perspectives de l'économie numérique de l'OCDE*, éd. OCDE, Paris, n° 2
- Le livre blanc de l'ACERP sur l'IoT (préparer la révolution de l'internet des objets, 7 novembre 2016),
- Big data et objets connectés, Institut Montaigne, avril 2015
- Rapports de l'ENISA - https://www.enisa.europa.eu
- Rapport IGA-IGAS-CGEFI-CGA n°16050-16018-2 : Revues de dépense 2016, « Les hélicoptères de service public ».
- Rapport Gartner de janvier 2017 sur les objets connectés : http://www.gartner.com

Ouvrages

- Benghozi P.-J., Bureau S., Massit-Folléa F., L'internet des objets, Éditions MSH, 2009.
- T. Piette-Coudol, Les objets connectés. *Sécurité juridique et technique*, LexisNexis, 2015, p. 11 et s.
- C. Avignon, V ; Bensoussan-Brulé et C.Torres, Règlement européen sur la protection des données, textes, commentaires et orientations pratiques, Edition Larcier, 2016
- A.Bensoussan, J.Bensoussan , le droit des robots , Edition Larcier 2016
- G.Haas,J-P Crenn, M.Quéméner, l'internet des objets : la 3ème révolution informatique. Imaginons les usages des échanges d'information de système à système ? Kawa éditions 2017.
- Marc Dugain, Christophe Labbé, « L'homme nu - La dictature invisible du numérique », 21 avril 2016, éditions Robert Laffont – Plon

Articles

- Gérard Haas – Amanda Dubarry – Marie D' Auvergne – Rachel Ruimy Enjeux et réalités juridiques des Objets Connectés – Dalloz IP/IT 2016. 394
- La *Privacy by Design* appliquée aux Objets Connectés : vers une régulation efficiente du risque informationnel ? – Célia Zolynski – Dalloz IP/IT 2016. 404
- Privacy by Designy : Anticiper pour mieux protéger (parties 1 et 2). R. Brun et T. Lapedagne. http://www.cil.cnrs.fr
- Chadi Hantouche, « Peut-on sécuriser l'Internet des Objets ? », Sécurité et stratégie 2016/2 (22), p. 31-38.
- Objets connectés et données personnelles, M. Cahen, http://www.murielle-cahen.com/publications/objet-connecte.asp
- M.Quéméner, Règlementation et sécurité : Quelles évolutions et enjeux juridiques pour l'Iot ?, Sécurité & Défense magazine
- L'internet des objets: Défis technologiques, économiques et politiques, Bernard Benhamou, *Esprit* ,No. 353 (3/4) (Mars-avril 2009), pp. 137-150,Published by: Editions Esprit Stable URL: http://www.jstor.org
- E.Daoud, F Plenascote, Cybersécurité et Objets Connectés,Dalloz IP/IT 2016 p.409
- C.Laverdet, les enjeux juridiques de l'Internet des objets, La semaine juridique, édition générale, n° 23, 9 juin 2014
- http://www.thetimes.co.uk
- https://www.washingtonpost.com
- International Journal of engineering sciences and research technology (IJESRT) – « A review of cyber-crime Internet of things technologies, investigation methods and digital forensics », octobre 2015.

GLOSSAIRE

Algorithme : Formalisation de la solution d'un problème à l'aide d'une suite d'opérations élémentaires (lecture, écriture, itération, schémas conditionnels, ..). Il est souvent exprimé avec une notation très proche du langage naturel et indépendante de tout langage de programmation.

Attaque par déni de service exploite les failles des protocoles de communication des entreprises. Cette intrusion consiste à rendre indisponible un serveur afin qu'il ne soit plus capable d'héberger ses sites.

Big data : traduction de « données massives ». Le gigantesque volume de données numériques produites combiné aux capacités sans cesse accrues de stockage et à des outils d'analyse en temps réel de plus en plus sophistiqués offre aujourd'hui des possibilités inégalées d'exploitation des informations. Les ensembles de données traités correspondant à la définition du big data répondent à trois caractéristiques principales : volume, vélocité et variété.Botnet : Réseaux d'ordinateurs (de bots ou zombies) jouant le rôle d'un relais pour des opérations de spamming, de phishing ou pour des attaques par Déni de service (ou DDos-Distributed Denial of Service). La constitution d'un Botnet est précédée par l'installation, sur les ordinateurs de plusieurs utilisateurs, d'un programme malveillant permettant la prise de contrôle à distance de ces ordinateurs. Les botnets sont souvent loués à des cybercriminels

Blockchain : Technologie permettant de gérer un registre permanent et infalsifiable des données transactionnelles. C'est une base de données contenant l'historique de tous les échanges effectués entre ses utilisateurs. S'il a été le plus souvent associé au Bitcoin, le modèle de blockchain pourrait être adopté dans le cadre d'autres systèmes financiers. Son usage permettrait de mieux sécuriser les transactions.

Chatbot : Un chatbot, aussi appelé « agent conversationnel », est un programme informatique capable de simuler une conversation avec un ou plusieurs humains par échange vocal ou textuel.

Chiffrement (Encryption) : Opération de cryptographique de données permettant de changer la forme de ces données et de les dissimuler. Les données ne seront accessibles (compréhensible) que pour les personnes qui disposent d'une clé (dé)chiffrement.

Cloud computing : Exploitation de la puissance de calcul ou de stockage de serveurs informatiques distants par l'intermédiaire d'un réseau, généralement internet.

CNIL : Autorité administrative indépendante créée en 1978, composée d'un collège pluraliste de 17 commissaires, provenant d'horizons divers (4 parlementaires, 2 membres du Conseil économique et social, 6 représentants des hautes juridictions, 5 personnalités qualifiées désignées par le Président de l'Assemblée nationale (1), par le Président du Sénat (1), par le Conseil des ministres (3). Le mandat de ses membres est de 5 ans.

Cyberattaque (Cyber Attack) : Forme d'attaque informatique, combinée à une attaque physique ou non, qui vise à endommager ou à détruire le système informatique d'un adversaire.

Data center (centre de données) : Site physique sur lequel se trouvent regroupés des équipements constituants du système d'information de l'entreprise (ordinateurs centraux, serveurs, baies de stockage, équipements réseaux et de télécommunications, etc.)

DDoS (Distributed Denial of Service attack) : attaque informatique par déni de service distribué se faisant à partir de plusieurs sources. Voir exemple en annexe 2.

Donnée personnelle : Toute information identifiant directement ou indirectement une personne physique (ex. nom, no d'immatriculation, no de téléphone, photographie, date de naissance, commune de résidence, empreinte digitale...).

Drone : au sens strict un appareil sans pilote à bord. Il est généralement piloté à distance par un opérateur humain, mais peut avoir un degré plus ou moins important d'autonomie (par exemple pour éviter des collisions ou gérer les conditions aérologiques). Un drone est avant tout une plateforme de capteurs mobiles. C'est un engin d'observation, d'acquisition et de transmission de données géolocalisées.

Géolocalisation : Technologie permettant de déterminer la localisation d'un objet ou d'une personne avec une certaine précision. La technologie s'appuie généralement sur le système GPS ou sur les interfaces de communication d'un téléphone mobile. Les applications et finalités de la géolocalisation sont multiples : de l'assistance à la navigation, à la mise en relation des personnes, mais aussi à la gestion en temps réel des moyens en personnel et en véhicules des entreprises, etc.

Hoax, ou canular, est une fausse information propagée sur les réseaux sociaux ou par mails i invite à être partagée par un maximum de personnes. Le but est d'engorger les réseaux, les boîtes mails, de dégrader l'image d'une personne, d'une organisation ou d'un objet. Cette désinformation a aussi pour but de minimiser l'impact des vraies informations qui elles ont de l'importance.

Infotainment : Mot valise fusionnant les mots anglais information et entertainment (divertissement)

Intelligence artificielle (artificial intelligence). : Discipline relative au traitement par l'informatique des connaissances et du raisonnement.

Locky, prise d'otage de fichiers, est la dernière-née des attaques. Un mail avec une pièce jointe nommée «ATTN : Invoice J-XXXXXXX» bloque l'accès aux données et réclame ensuite au propriétaire une rançon.

Permanent Denial of Services (attack) : variante d'une attaque de type DDoS ou les dommages commis par l'attaque sont persistants et nécessitent une intervention matérielle. Bricker Bot est un exemple de programme exerçant ce type d'attaque sur les objets connectés. (cf https://www.infosecurity-magazine.com/news/bricker-bot-follows-mirai-tactics/).

Phishing ou hameçonnage : il représente 65% des incidents. Il prend la forme de faux mails d'entreprises ou d'institutions publiques. Le but est la récupération vos coordonnées personnelles et bancaires.

Pseudonymisation : traitement de données à caractère personnel de telle façon qu'elles ne puissent plus être attribuées à une personne concernée sans avoir recours à des informations supplémentaires, pour autant que celles-ci soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir cette non-attribution à une personne identifiée ou identifiable.

Puces RFID : elles permettent d'identifier et de localiser des objets ou des personnes. Elles sont composées d'une micropuce (également dénommée étiquette ou tag) et d'une antenne qui dialoguent par ondes radio avec un lecteur, sur des distances pouvant aller de quelques centimètres à plusieurs dizaines de mètres. Pour les applications dans la grande distribution,

leur coût est d'environ 5 centimes d'euros. D'autres puces communicantes, plus intelligentes ou plus petites font leur apparition avec l'avènement de l'internet des objets. Certains prototypes sont quasi invisibles (0,15 millimètre de côté et 7,5 micromètres d'épaisseur) alors que d'autres, d'une taille de 2 mm2, possèdent une capacité de stockage de 512 Ko (kilo-octets) et échangent des données à 10Mbps (méga bits par seconde).

Ransomware (Rançongiciel) : logiciel malveillant qui menace de détruire ou de bloquer l'accès aux données d'un utilisateur ou d'une société si une rançon n'est pas versée.

Spamming est un envoi automatique de mails publicitaires en masse. Les adresses électroniques utilisées sont récupérées de manière frauduleuse.

Smart city : La ville intelligente est un nouveau concept de développement urbain. Il s'agit d'améliorer la qualité de vie des citadins en rendant la ville plus adaptative et efficace, à l'aide de nouvelles technologies qui s'appuient sur un écosystème d'objets et de services. Le périmètre couvrant ce nouveau mode de gestion des villes inclut notamment : infrastructures publiques (bâtiments, mobiliers urbains, domotique, etc.), réseaux (eau, électricité, gaz, télécoms) ; transports (transports publics, routes et voitures intelligentes, covoiturage, mobilités dites douces - à vélo, à pied, etc.) ; les e-services et e-administrations.

Sniffing : logiciel qui intercepte et récupère les données, notamment les identifiants et les mots de passe.

Virus : programme néfaste qui se greffe dans un logiciel et qui se déclenche à l'utilisation de ce dernier. Issu de la navigation web ou d'un disque de stockage externe, il perturbe le fonctionnement de l'appareil infecté jusqu'à parfois provoquer son arrêt.

Wearable : terme anglais qui désigne un vêtement ou un accessoire intégrant de l'informatique et de l'électronique. On peut traduire ce terme en français par « technologie portable ».

ANNEXES

Annexe 1 - Les drones et la sécurité intérieure

Les drones : un large domaine d'utilisation

Déjà utilisé dans des missions de police judiciaire, comme par exemple par la section de recherche de la gendarmerie et transports aériens lors des crashs aériens[71] quand les conditions climatiques le permettent, comme celui du Mali le 24 juillet 2014... le drone en police administrative présente un intérêt majeur qui se trouve au cœur de notre étude. Nous ne traiterons donc pas ici de ses éventuelles utilisations ou perspectives d'utilisation dans les constatations de police technique et scientifique en matière de police judiciaire.

Le domaine d'utilisation réelle ou potentielle des drones pour les forces de l'ordre est très varié et large : services d'ordre et opérations de maintien de l'ordre ; violences urbaines et soutien aux opérations de lutte anti-criminalité ; gestion des grands événements ; appui tactique aux interventions des unités spécialisées ; sécurité routière et fluviale, surveillance des réseaux de transports ; traitement des incendies et accidents industriels de grande ampleur, catastrophes naturelles...

Avant de développer son utilisation, les forces de sécurité ont d'abord eu recours à des Evaluations technico-opérationnelles (ETO) tant en milieu urbain que rural pour en démontrer la pertinence[72] et constater les limites opérationnelles. Par exemple, la police nationale a utilisé un drone en 2014 à titre expérimental lors d'un match de ligue 2 à Créteil (stade Duvauchelle).

Au-delà des acteurs régaliens (police et gendarmerie nationales, sécurité civile), d'autres acteurs développent l'utilisation des drones.

Le point de départ du foisonnement technologique des drones date de la publication des arrêtés du 11 avril 2012 relatifs à leur conception et à leur utilisation[73].

La sécurité civile a acquis des drones après la catastrophe de FUKUSHIMA en 2012 qui n'ont toutefois pas été engagés sur des opérations de sécurité civile d'ampleur pour des raisons tant de réglementation que d'opportunité et de moyens (notamment la contrainte de formation des pilotes).

La Brigade de Sapeurs-Pompiers de Paris a opté pour une autre technologie à savoir un ballon captif en milieu urbain : AéroC 2 OD (Aérostat Captif Communicant pour l'Observation et la Désignation).

---

(71) Entretien avec le lieutenant-colonel Gojkovic-Lette, commandant la section de recherche de la gendarmerie des transports aériens, le 4 avril 2017.

(72) Revue de la Gendarmerie Nationale, « Les systèmes de drones au cœur de la transformation numérique », colonel Jérôme BISOGNIN, DGGN.

(73) Arrêté du 11 avril 2012 relatif à l'utilisation de l'espace aérien par les aéronefs qui circulent sans personne à bord et arrêté du 11 avril 2012 relatif à la conception des aéronefs civils qui circulent sans aucune personne à bord, aux conditions de leur emploi et sur les capacités requises des personnes qui les utilisent. Un décret du 29 avril 2013 et un arrêté du 29 décembre 2013 complètent le cadre juridique.

Le ballon captif se gonfle à l'hélium en moins de 30 minutes. « Relié par un treuil, il peut être déployé jusqu'à 150 m de hauteur dans un contexte où le renseignement par images aériennes, en temps réel, est crucial. Il permet la visualisation de jour comme de nuit de la zone d'intervention sur un écran vidéo et ainsi la désignation d'objectifs visibles sur l'écran aux intervenants. L'aéroC²OD peut être prioritairement déployé lors d'interventions majeures, notamment inondations, pollutions, effondrements mais aussi feux d'entrepôts ou feux d'îlots complexes[74] ».

De son côté, la SNCF a largement investi dans cette technique au point d'être le fer de lance des drones en France dans le domaine de la sécurité et d'avoir créé une filiale[75] en avril 2017. Actuellement dotée de 12 drones, la SNCF les utilise pour ses missions de sûreté mais aussi pour l'élaboration des plans topographiques, les inspections d'ouvrage d'art et sa communication.

Doctrine d'emploi des drones et cadre juridique

La doctrine d'emploi est variable selon les directions. Toutefois, d'une manière générale, le drone revêt un intérêt dans la mesure où « il est une aide à la décision pour tout personnel en charge d'un commandement, notamment grâce à la retransmission d'images en temps réel qui permet l'appréciation exhaustive de la situation et l'expression rapide d'ordres en retour... C'est dans l'appui des moyens au sol que les systèmes de drones démontrent toute leur pertinence[76] ».

Sans détailler le régime juridique de l'emploi des drones et la différence entre les forces de sécurité en fonction de leur statut (la gendarmerie est une autorité d'emploi aéronautique mais pas la police), il convient de préciser que l'utilisation des drones obéit à la réglementation de la direction générale de l'aviation civile (DGAC).

Les drones sont répartis en 7 catégories de A à G en fonction de leur poids et de leur capacité[77].

Comme l'indique le tableau ci-dessous, la DGAC décline une réglementation en quatre scénarii en fonction de critères d'utilisation de l'appareil (vue directe ou non par le télépilote, zone de vol, distance entre l'engin et le pilote) afin que puisse cohabiter dans un espace aérien dense les avions traditionnels et les drones.

Scénarii	Vue directe	Zone peuplée	Distance maximum du pilote
Scénario 1	Oui	non	100 m
Scénario 2	Non	non	1000 m
Scénario 3	Oui	oui	100 m
Scénario 4	Non	non	Pas de contrainte

(74) Entretien avec le colonel CHALIFOUR, sous-chef d'état-major, chef de la division Emploi à la Brigade de Sapeurs-Pompiers de Paris, le 22 mars 2017.
(75) Altamétris. Entretien avec M. Nicolas Pollet, directeur, le 23 mars 2017.
(76) Revue de la Gendarmerie Nationale, « Les systèmes de drones au cœur de la transformation numérique », colonel Jérôme BISOGNIN, DGGN.
(77) Catégorie A : Les aéromodèles de moins de 25 kg, propulsés ou captifs, exclusivement utilisés à des fins de loisirs ou de compétition entre aéromodèles ; catégorie B: Les aéromodèles (donc de loisirs) de plus de 25 kg ou qui ne respectent pas les critères de propulsion décrits pour ceux de la catégorie A ; catégorie C : Les aéronefs captifs de moins de 25 kg qui sont utilisés pour un travail aérien (photo, vidéo, thermographie, observations, relevés...) ; catégorie D : Les aéronefs utilisés pour un travail aérien d'une masse au décollage inférieure à 2 Kg (structure + charge) ; catégorie E: Les aéronefs qui n'appartiennent pas aux classes C et D, d'une masse inférieure à 25 kg ou par dérogation dont la masse est inférieure à 4 kg ; catégorie F: Les aéronefs d'une masse inférieure à 150 kg ; catégorie G: Les aéronefs d'une masse supérieure à 150 kg.

La SNCF a par exemple choisi le scénario 4 mais « dérogatoire » dans la mesure où elle peut faire voler des drones plus lourds (jusqu'à 15 kg au lieu des 2 kg maximum prévus dans le scénario 4) et de nuit. Il convient de préciser que la SNCF ne cherche pas à identifier des personnes ou des véhicules mais à repérer une présence. En d'autres termes, la SNCF a choisi d'équiper les drones de caméras qui ne peuvent pas faire de lecture de plaque minéralogique ni de visualiser nettement les individus filmés. Ce choix emporte deux conséquences majeures : un moindre coût (les capteurs sont moins chers) et l'absence de problématique CNIL. La SNCF peut ainsi programmer le vol de drones entre 50 et 100 nuits par an. La rentabilité opérationnelle est évidente. Une équipe SUGE parcoure 10 km de voie en une nuit. Un drone couvre 30 km de voie avec un passage toutes les 15 minutes.

D'un point de vue juridique, le donneur d'ordre (public comme privé) d'une prestation de travail aérien engage sa responsabilité sur la conformité des matériels et du niveau de compétence du personnel requis à cette prestation. Par ailleurs, la captation et l'enregistrement d'images relatives aux personnes physiques relèvent de la loi informatique et Libertés.

Cartographie des risques

La principale difficulté est la sécurité aéronautique. Les conditions de navigabilité et d'insertion dans le trafic aérien sont draconiennes pour éviter tant les dommages collatéraux (risque de collision avec d'autres appareils volants comme les hélicoptères, drones, ULM, avions en phase de décollage ou d'atterrissage) que les contraintes de l'environnement (aspiration de micro-drones par un réacteur d'avion, risque pour la population ou les biens en cas de chute, vulnérabilité liée à un environnement électromagnétique…).

La généralisation de l'utilisation des drones se heurte donc à plusieurs problèmes. Cela suppose d'abord une enveloppe budgétaire pour l'acquisition de ces appareils dont le prix est assez élevé même si des produits plus compétitifs et à moindre coût apparaissent sur le marché. L'achat des drones par les forces de sécurité peut bénéficier de subventions européennes. Il faut ensuite maîtriser la technologie en formant des télépilotes. Le niveau requis est exigeant et requiert des connaissances pratiques du pilotage (« effet de sol » comme le vent…). C'est la raison pour laquelle les télépilotes de la SNCF (scénario 4 dérogatoire) détiennent un brevet de pilote et plus de 100 heures d'expérience en vol à bord d'un avion ou d'un hélicoptère. De même que les pilotes de drone MALE[78] de l'armée de l'air sont tous pilotes de chasse.

Le risque de l'emploi d'un drone est le dommage collatéral sur des biens mais encore plus sur des personnes. La chute d'un drone volant au-dessus d'une foule lors d'une manifestation ne serait pas acceptable pour l'opinion publique et réduirait donc à néant l'emploi de ces engins. Or les risques existent. Outre la chute « accidentelle », un acte malveillant peut provoquer la perte de contrôle de l'appareil en cas de brouillage des fréquences par exemple.

Le risque majeur n'est-il pas l'utilisation du drone à des fins criminelles par des groupes terroristes notamment ? Le drone ennemi focalise l'attention même si les moyens de neutraliser ces engins posent des problèmes techniques actuellement non résolus.

(78) MALE : moyenne altitude longue endurance.

Annexe 2 – De l'objet connectés au « botnet »

Les botnet (de l'anglais, contraction de « robot » et « réseau »), sont des réseaux de bots informatiques, des programmes connectés à Internet qui communiquent avec d'autres programmes similaires pour l'exécution de certaines tâches. La caractéristique principale des botnets est la mise en commun de plusieurs machines distinctes, parfois très nombreuses, ce qui rend l'activité souhaitée plus efficace (puisqu'on a la possibilité d'utiliser beaucoup de ressources) mais également plus difficile à stopper.

Le processus est en trois phases :

1- Le pirate tente de prendre le contrôle de machines distantes, par exemple avec un virus, en exploitant une faille ou en utilisant un cheval de Troie. 2- Une fois infectées, les machines vont terminer l'installation ou prendre des ordres auprès d'un centre de commande, contrôlé par le pirate, qui prend donc ainsi la main par rebond sur les machines contaminées (qui deviennent des machines zombies). 3- Le pirate envoie la commande aux machines infectées (ou poste un message à récupérer, selon le mode de communication utilisé). Celles-ci « travaillent » alors en masse.

Le 20 septembre 2016, « KrebsOnSecurity.com » est devenu la cible d'une attaque massive de type DDoS qui a finalement mis le site hors service. Le site avait pourtant été initialement protégé contre ce type d'attaque par Akamai, le fournisseur de services de sécurité informatique de ce site Web. La société a décidé de retirer son dispositif de protection pro bono, puisque l'ampleur de l'attaque (environ 620 Gbps) était trop vaste pour être supportée sans affecter les autres clients. L'analyse d'Akamai a indiqué l'utilisation d'un « botnet » comprenant de nombreux objets connectés compromis. A partir du moment où Akamai a désactivé son système de protection, le site internet est passé hors ligne jusqu'à ce que Google mette en place son service de protection contre les attaques DDoS, « Project Shield », ce qui a permis de le rétablir. Brian Krebs fournit plus d'informations sur l'attaque à travers son blog.

Juste après les attaques DDoS contre «KrebsOnSecurity.com» et OVH, un utilisateur sur un forum de « hacking » a publié le code source d'un malware surnommé «Mirai»[79]. Le logiciel malveillant cible les périphériques IoT non protégés et les transforme en robots. Le pirate est alors capable de lancer une attaque DDoS à partir de tous ces « bots » par le biais d'un serveur central comme ce qui est fait dans la plupart des botnets communs. Comme l'a noté Brian Krebs dans son blog sur Mirai, dans lequel il affirme que Mirai est lié à l'attaque contre son propre site Web, cette version du code source va bientôt déclencher plus d'attaques DDoS en utilisant des dispositifs IoT non sécurisés. Une analyse technique de Mirai est disponible par «MalwareMustDie».

Le 21 octobre 2016, le fournisseur DNS Dyn a connu une attaque massive de type DDoS et a déclaré initialement que l'attaque provenait de dizaines de millions d'adresses IP à travers le monde (Sophos NakedSecurity a analysé le code source de Mirai pour contester cette affirmation). Une mise à jour ultérieure de Dyn, a noté que les points d'attaque étaient en fait estimés à environ 100 000. L'attaque a causé des dysfonctionnements pour les utilisateurs essayant d'atteindre des sites très populaires tels que Twitter, Amazon, Tumblr, Reddit, Spotify et Netflix tout au long de cette journée. Selon l'information fournie par Dyn, une partie de l'attaque impliquerait des dispositifs IoT infectés par le botnet Mirai. A ce sujet, TrendMicro a publié un article sur les problèmes de sécurité de l'écosystème des IoT soulignant que la sécurité n'a pas été une priorité pour les fabricants et fournisseurs d'IoT, conduisant à de graves incidents.

---

(79) https://www.enisa.europa.eu/publications/info-notes/mirai-malware-attacks-home-routers

Annexe 3 - Vers un droit des robots ?

L'industrie robotique en évolution permanente, fait pression sur le système juridique actuel. Certains inventeurs déclarent que les législations doivent s'adapter à la nouvelle technologie et proposent de créer un régime juridique nouveau pour la robotique.

Selon Alain Bensoussan, il existe trois générations de robots : la première correspondrait à l'ère des simples automates comme les mixeurs et les machines à café, la seconde génération est celle des automates avec capteurs comme les aspirateurs et les tondeuses à gazon autonomes, la troisième génération est constituée d'objets qui possèdent de l'intelligence artificielle et sont connectés comme la voiture autonome. Pour les robots qui disposent d'intelligence artificielle, un statut juridique particulier apparait nécessaire.

Cet avocat spécialiste préconise la création d'un statut juridique pour la robotique qui a un rôle social et souligne que « les lignes de démarcation occidentale entre le vivant et l'inerte ne permettent cependant déjà plus d'appréhender certaines manifestations de la robotique relationnelle : le robot animaloïde Aibo (Sony) a, par exemple, rejoint le foyer de familles japonaises et s'y est intégré parfois à tel point que des funérailles traditionnelles ont été organisées lorsqu'il n'a plus été possible de le réparer... »[80].

La nécessité de créer un droit des robots est argumentée par les défenseurs de cette thèse par le fait que « des robots domestiques, médicaux et de sécurité sont susceptibles de collecter des données à caractère personnel »[81] qui pourraient être aujourd'hui insuffisamment protégées par la loi informatique et liberté du 6 janvier 1978. La multiplication des robots de service qui ont la capacité de collecter des données personnelles peut mettre en danger l'intimité de la vie privée. Cependant la multiplication des drones et leurs usages pour collecter des données personnelles font apparaitre de nouveaux défis, celles de l'encadrement juridique de menaces sur l'intimité de la vie privée. Quelles mesures de protection pour encadrer l'usage de cette nouvelle technologie ?

Mady Delvaux, députée européenne, déclare que « de plus en plus de domaines touchant nos vies quotidiennes sont concernés par la robotique. Pour faire face à cette réalité et garantir que les robots sont et restent au service de l'homme, nous avons besoin de créer de toute urgence un cadre juridique européen. »

Dans son rapport, Mady Délvaux explique qu'il faut reconnaitre les robots les plus autonomes en tant que « *personne électronique et créer une assurance obligatoire pour couvrir les fautes qu'il pourrait commettre*[82] ». Pour Tony Belpaeme[83], la création d'une nouvelle personnalité juridique a peu d'intérêt, il persiste sur l'idée que « *les entreprises qui fabriquent et utilisent les robots devraient continuer à être responsables* ».

Pour Alain Bensoussan , « *il s'agit de la place du robot intelligent dans l'éventail juridique en lui conférant un statut aligné sur ses capacités et son rôle social. Il exprime une catégorisation inédite entre les personnes physiques ou morales et les choses* »[84].

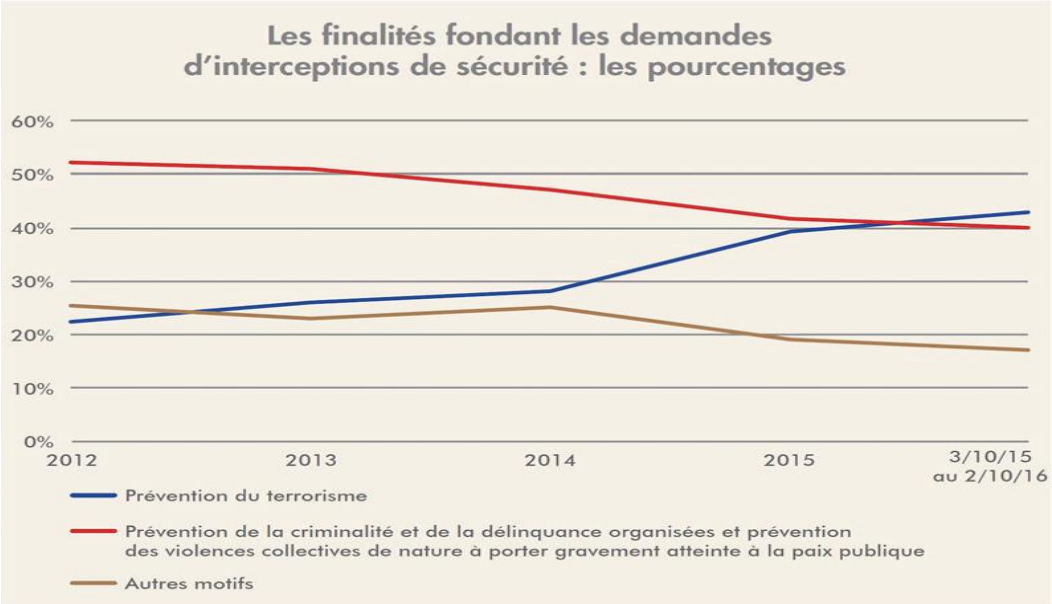
---

(80) Alain Bensoussan, Droit des robots :science-fiction ou anticipation ?,Recueil Dalloz-30juillet 2015-n 28,p1640.
(81) Anthony Bem,La nécessité d'une protection des données personnelles collectées par des robots,2013.
(82) Mady Délvaux,projet d'une résolution européenne
(83) Professeur de « Cognitive Systems and Robotics » à l'université de Plymouth.
(84) Alain Bensoussan,Droit des robots :science-fiction ou anticipation ?,Recueil Dalloz-30juillet 2015-n 28,p1640.

Annexe 4 – Le rôle de la CNCTR

La **Commission nationale de contrôle des techniques de renseignement** (**CNCTR**) est une autorité administrative indépendante française qui veille à ce que les techniques de recueil de renseignement soient mises en œuvre conformément au Code de la sécurité intérieure. Elle a été créée dans le cadre de la loi du 24 juillet 2015 relative au renseignement.

La CNCTR est saisie des demandes d'autorisation de mise en œuvre des techniques de renseignement par les services. Elle donne un avis préalable et c'est le Premier ministre qui statue. Ce contrôle est considéré comme s'exerçant a priori, bien que la CNCTR développe une activité de contrôle a posteriori. La CNCTR apprécie la légalité, en particulier la proportionnalité, de la mise en œuvre des techniques de renseignement au regard de l'atteinte portée à la vie privée. La légalité des techniques repose aussi sur le respect des finalités autorisées : l'indépendance nationale, l'intégrité du territoire et la défense nationale ; les intérêts majeurs de la politique étrangère ; les intérêts économiques, industriels et scientifiques majeurs de la France ; la prévention du terrorisme ; la prévention des atteintes à la forme républicaine des institutions, la reconstitution de groupements dissous, les violences collectives portant gravement atteinte à la paix publique ; la prévention de la criminalité et de la délinquance organisée.



Source : 1er rapport d'activité 2015/2016 de la CNCTR.

La liste des services autorisés à mettre en œuvre les techniques exposées au préalable est elle aussi limitative. Les services sont en outre répartis en deux catégories : le « premier cercle » (DGSE, DRSD, DRM, DGSI, DNRED, Tracfin) et le « second cercle » (certains services de police comme l'UCLAT, des services de la DCPJ, certains de la DCSP, des unités de la police aux frontières ; des services de la gendarmerie nationale comme les sections de recherches, la SDAO, la SDPJ ; des services de la préfecture de police de Paris ou du ministère de la défense ; le service de renseignement pénitentiaire). Une partie des techniques de renseignement ne sont pas accessibles au second cercle.

Interrogée, la CNCTR assure que bien que le champ des objets connectés ne soit pas figé, le cadre légal existant permet d'appréhender son évolution. Pour avoir une idée plus précise de

l'activité des services de renseignement, le rapport de la CNCTR apporte un certain nombre de précisions relatives à sa première année de fonctionnement, d'octobre 2015 à octobre 2016.

Technique de renseignement	Nombre d'avis préalables rendus
Accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure)	48 208
Géolocalisation en temps réel (article L. 851-4 du code de la sécurité intérieure)	2 127
Interceptions de sécurité (I de l'article L. 852-1 du code de la sécurité intérieure)	8 538
Autres techniques	7 711

La CNCTR a rendu 48 208 avis relatifs à l'accès aux données de connexion en temps différé. L'essentiel visait à identifier des numéros d'abonnement ou de connexion à des sites, voire l'ensemble des numéros d'abonnement ou de connexion d'une personne. Dans ce lot, 15 211 demandes ont aussi eu pour ambition d'« obtenir la liste des appels et des correspondants de la personne surveillée ». Ce sont les Fadet, pour facture détaillée.

Pour la géolocalisation en temps réel, 2 127 avis ont été rendus. S'agissant des interceptions de sécurité, le chiffre s'établit à 8 538 avis. Enfin, 7 711 avis ont concerné les autres techniques (balises, IMSI catcher, captation des données informatiques, etc.). La CNCTR n'a pas communiqué le détail de cet ensemble, arguant du secret de la défense nationale.

Hors demandes d'accès aux données de connexion en temps différé, la CNCTR a rendu 1 263 avis défavorables, soit 6,9%. Elle justifie : « Ce taux, plus élevé que celui résultat du contrôle opéré par la CNCIS, peut s'expliquer par le fait que les nouvelles techniques de renseignement sont, pour certaines d'entre elles, plus intrusives que celles prévues par le cadre juridique antérieur, ce qui entraîne un niveau de contrôle d'autant plus rigoureux ». Les services « *ont besoin de s'adapter à la jurisprudence de la commission* », précise la CNCTR, sollicitée par nos soins.

Pendant la première année d'exercice de la CNCTR, 20 282 personnes ont fait l'objet d'une technique de renseignement au moins. Toutefois, ce chiffre ne comprend pas les accès aux données de connexion en temps différé (principalement l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques ainsi que le recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée). Enfin, 47 % des personnes surveillées l'ont été au titre de la prévention du terrorisme.

INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

École militaire - 1 place Joffre - 75007 Paris

Tél: +33 1 76 64 89 00