Petit-déjeuner-débat du 20 septembre 2017

« Objets connectés et usages numériques : sécurité et protection des données »

placé sous la présidence de

Laure de la RAUDIERE
députée d'Eure-et-Loir, membre de la Commission des Affaires économiques

avec

Myriam QUEMENER
magistrat, conseiller juridique auprès du Délégué ministériel
aux industries de sécurité et à la lutte contre les cybermenaces, ministère de l'Intérieur

avec le soutien de nos partenaires

La présentation en présence de madame Laure de la Raudière, députée, est issue d'un rapport sur les objets connectés réalisé par les auditions de la 28ème session de l'INHESJ qui va être publiée[1].

En 2017, d'après une étude[2], 52% des Français interrogés possèdent au moins un objet connecté hormis leur smartphone et 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.

Selon les chiffres de Gartner[3], 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[4]. 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[5].

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 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 cœur 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.

Les objets connectés peuvent être analysés à la fois en termes de protection et de traitements des données véhiculées par les objets connectés, d'expertise des cybermenaces dont ils sont les cibles et enfin d'opportunités pour les forces de l'ordre.

Objets connectés et protection des données

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. Sur le plan juridique, la loi « informatique et libertés » du 6 janvier 1978 pose un cadre qui est toujours d'actualité en ce qui concerne la collecte et l'utilisation de données à caractère personnel. Cette protection offerte à chaque individu trouve sa limite dès que celui-ci a manifesté son consentement même implicitement (Ex. de l'inscription aux réseaux sociaux Facebook, …).

La question du consentement est un enjeu fort qui va évoluer prochainement dans le cadre du règlement européen, le RGPD. Ainsi, le responsable du traitement devra respecter 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.

En outre, 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.

Sur le sujet des données personnelles, il s'avère donc nécessaire d'adapter la règlementation au moins au niveau européen, de sensibiliser les consommateurs aux usages et risque liés aux objets connectés, de renforcer les règles en matière de consentement des utilisateurs, de 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 et de renforcer les moyens des instances de contrôle (CNIL, ARCEP, …) avec le possibilité pour celles-ci de déléguer à d'autres instances les contrôles.

Au-delà des données personnelles échangées via les objets connectés se pose la question de leur traitement via des mécanismes de plus en plus complexes, les algorithmes. 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*[8] » est aujourd'hui devenu un incontournable de notre vie quotidienne.

Les techniques algorithmiques mises en œuvre aujourd'hui par les grands opérateurs (GAFA[9]) de l'Internet démontrent des capacités insoupçonnées jusqu'alors : détection des cancers de la peau par exemple mais aussi des capacités de manipulation des utilisateurs à leur insu comme l'a démontré l'expérimentation de Facebook sur 700 000 utilisateurs en 2012. La confiance que l'utilisateur peut accorder aux algorithmes doit donc reposer sur la transparence de ceux-ci.

Sur le plan juridique, la question de la responsabilité se pose : les algorithmes dits « 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 résident en France, ni même dans l'UE.

Comme le dit Alain Bensoussan, avocat spécialisé dans le droit des robots :

« *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 » ?* »

Dans le domaine du traitement des données personnelles, il s'avère donc nécessaire de fixer a priori les responsabilités juridiques des différents acteurs élaborant et mettant en œuvre des algorithmes de type « intelligence artificielle ».

Les objets connectés face aux cyberattaques

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. 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.

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. Les dernières attaques sont souvent le fait d'un logiciel malveillant de type ransomware qui 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. Ainsi « Wannacry » a infecté entre le 12 et le 23 mai 2017 plus de 300.000 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 touchés 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 de l'histoire d'Internet, Europol[10] la qualifiant « *d'un niveau sans précédent* » et ajoutant « *qu'il ne faut en aucun cas payer la rançon* ».

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[11]. 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 cyber menaces (DMISC), dans son premier rapport[12] 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* ».

Parmi les solutions de sécurisation, on peut citer l'action des plateformes de « *bug bounty* »[13] 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 elles pourraient contribuer à sécuriser le marché des objets connectés à la condition d'être labellisées par l'ANSSI par exemple.

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 aux systèmes de traitement automatisé de données, en cas d'accès ou de maintien frauduleux. En effet, on peut assimiler un objet connecté à un système de traitement automatisé de données (STAD).

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 réprimés 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.

Dans le domaine de la sécurisation des objets connectés et des données personnelles qu'ils véhiculent et traitent, il s'avère nécessaire de rendre effectif le « *privacy by design* » et favoriser le rôle des entreprises de type « bug Bounty » pour la sécurisation des IoT.

Objets connectés et opportunités pour la sécurité

Les objets connectés présentent de nombreuses opportunités pour les activités des forces de l'ordre, que ce soit pour la police judiciaire, la sécurité publique ou le renseignement.

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[14]), 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…).

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. Ainsi le *Washington Post* rapporte de son côté[15] 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. 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 et l'exploitation forensique[16] 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.

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.).

Les opérations techniques liées à l'exploitation des objets connectés en matière pénale paraissent couvertes, sur le 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.

Dans le domaine de l'usage des objets connectés pour l'administration de la preuve pénale, il est nécessaire de former les acteurs (sécurité et justice) aux problématiques et techniques spécifiques à l'IoT et 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.

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.

Les possibilités technologiques de la vidéo intelligente sont 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, les nouvelles techniques actuellement testées ont été impulsées par un projet européen après les attentats terroristes de novembre 2015 à Paris.

Dans le domaine de la sécurité intérieure, les drones occupent une place de plus en plus importante dans la stratégie opérationnelle. 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.

Dans le domaine de l'utilisation des objets connectés comme moyens de sécurisation, il est souhaitable d'assouplir la réglementation pour l'utilisation des drones à usage régalien dans l'espace public aérien et d'accélérer le processus d'adoption de la vidéo intelligente par l'évolution du cadre juridique et assurer l'interopérabilité des systèmes publics et privés.

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.

Une nouvelle instance, la Commission nationale de contrôle des techniques de renseignement (CNCTR), autorité administrative indépendante française, est chargée de veiller 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 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.

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'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 » connaissant de plus en plus de choses sur chacun grâce aux données personnelles qui sont captées, traitées et échangées par l'Internet des objets.

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, …).

Notes :

[1] https://inhesj.fr/

[2] Deuxième baromètre des objets connectés OpinionWay à l'occasion du salon Distree#Connect.

[3] Gartner, « Internet of Things. Endpoints and Associated Services, Worldwide », étude prévisionnelle de décembre 2015.

[4] L'IDATE anticipe 80 milliards d'appareils connectés d'ici 2020, CISCO en envisage 50 milliards.

[5] 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[5]. 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[5].

[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.

[8] Définition du Larousse : http://www.larousse.fr/dictionnaires/francais/algorithme/2238

[9] Google, Amazon, Facebook, Apple

[10] https://www.europol.europa.eu/wannacry-ransomware

[11] Un modèle actuel de voiture connectée n'émet que 10 Mo de données par mois

[12] http://www.interieur.gouv.fr/content/download/101311/797853/file/Etat-de-la-menace-Janvier-2017.pdf

[13] 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.

[14] tablettes Néo pour la Police nationale et Néogend pour la gendarmerie nationale cf partie B « Les objets connectés comme moyens de sécurisation » de ce rapprot

[15] 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.

[16] 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).