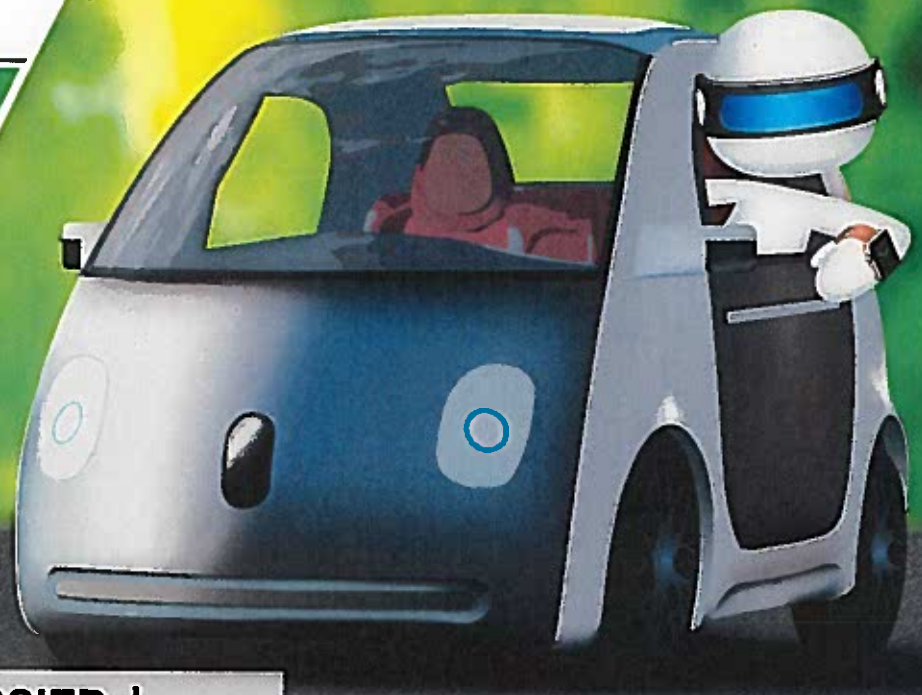
Dalloz IP / IT

DROIT DE LA PROPRIÉTÉ INTELLECTUELLE ET DU NUMÉRIQUE

Numéro 09 - Septembre 2016

9 782997 516092



DOSSIER | P. 388

LES OBJETS CONNECTÉS : 4E RÉVOLUTION INDUSTRIELLE

AU FIL DU MOIS
Loi pour une République numérique
Interview de la ministre Axelle Lemaire

PRATIQUES
Text & Data Mining, l'impossible exception
Laurence Ballet

TEXTES ET DÉCISIONS
Droit de communication au public : harmonie, vous avez dit harmonie ? CJUE, gr. ch., 31 mai 2016
Valérie Laure Benabou

Version numérique incluse*

DALLOZ

CYBERSÉCURITÉ ET OBJETS CONNECTÉS

Les Objets Connectés et l'internet des objets offrent un nouveau terrain de jeux pour les cybercriminels. Une présentation sommaire de leurs spécificités techniques permet de comprendre pourquoi ces technologies peuvent susciter la convoitise des apprentis délinquants et des criminels confirmés. L'étude de leurs particularités permet de révéler, en outre, les forces et faiblesses de la réponse qu'apporte le droit pénal, qui est toutefois renforcée par les dispositifs applicables en matière de protection des données à caractère personnel et de cyberdéfense. Il est enfin envisagé dans cet article de prendre en compte les exigences sécuritaires dès la conception de ces objets, au moyen de l'utilisation de cette même technologie à des fins de prévention de la cybercriminalité.

Emmanuel Daoud
Avocat au barreau de Paris - Cabinet Vigo, Membre du réseau GESICA

et Flora Plénacoste
Avocat au barreau de Paris - Cabinet Vigo, Membre du réseau GESICA

L'internet des objets (IdO) a aujourd'hui dépassé le stade de la conceptualisation. Les analystes divergent sur les échéances mais la communauté d'acteurs prévoit une extension et une généralisation de l'usage des Objets Connectés dont le nombre devrait avoisiner les 50 milliards dans le monde d'ici 2020[1]. La multiplication de ces objets implique nécessairement de relever le défi qu'elle présente en matière de cybersécurité. En effet, toute nouvelle technologie de communication est visée par la cybercriminalité. Il ne fait donc aucun doute que l'IdO sera touché. La question est plutôt celle de savoir si le droit positif est suffisamment armé pour répondre de manière adéquate aux cyberattaques à venir. Pour le déterminer, il est nécessaire d'exposer et de tenir compte des particularités techniques de l'IdO (I). Le rapprochement entre la technique et le droit révèle que le droit pénal applicable en matière de cybercriminalité n'assure que partiellement la sécurité de l'IdO (II). D'autres champs du droit viennent toutefois compléter ce dispositif (III). Il semble par ailleurs que la technologie de l'IdO porte en elle-même les moyens d'assurer sa propre sécurité. Peut-être conviendrait-il donc de rendre obligatoire la sécurité des Objets Connectés dès leur conception (IV) ?

I - DÉFINITIONS ET PARTICULARITÉS TECHNIQUES

A - L'Objet Connecté

Définition de l'Objet Connecté. L'objet dit « connecté » est avant tout un objet matériel

[1] Ministère de l'Économie et des finances et du redressement productif, *Rapport internet des objets et logistique, « Vers des nets avec des objets », Situation internationale, perspectives des acteurs et débats* [en ligne] [consulté le 2 mai 2016], disponible http://www.economie.gouv.fr/files/files/directions_services/cge/Rapports/2013_07_01_2012_25_Rapport.pdf.

préexistant quelconque, électronique ou non. Sa particularité réside dans le fait qu'il ne s'agit cependant pas de considérer l'objet initial comme une finalité, mais comme un moyen de délivrer et de bénéficier de nouveaux services. Ces services reposent sur la donnée que les objets captent, comme source de création de valeur. En résumé, un objet connecté peut donc être défini comme un dispositif matériel permettant de collecter, stocker, transmettre et traiter des données issues du monde physique[2].

En théorie, tout objet peut être connecté. Leur typologie s'annonce donc déjà très riche. L'Objet Connecté a vocation à toucher tous les secteurs : le milieu de l'automobile travaille sur le « véhicule autonome » qui a vocation à assurer sa propre conduite en fonction des données qu'elle recueille ; le secteur du bâtiment travaille sur la conception d'une « maison intelligente » qui réagit et adapte la consommation d'eau ou d'électricité à son environnement. Pour le moment, les Objets Connectés les plus populaires sont les objets dits « *wearables* » qui se portent à même le corps ou équipent les vêtements et accessoires : caque audio servant de GPS, montre-bracelet qui traque l'activité physique, etc. Ces objets *wearables* captent les données les plus intimes et éventuellement des données dites « sensibles » au sens de la loi Informatique et Libertés de 1978[3] – c'est-à-dire notamment celles qui portent sur le corps et l'état de santé du propriétaire et donc sur son activité physique, sur les calories brûlées, le rythme cardiaque, etc.

Ces objets wearables captent les données les plus intimes

De manière générale, l'ensemble de ces données collectées – données « sensibles » et autres – *via* des périphériques divers (téléphone, capteurs, bracelet, montres...) ont pour centre une application qui recueille et procède à leur exploitation massive grâce à la technologie du *Big Data*. Une fois ces données analysées, ces objets réagissent et peuvent par exemple diffuser un message à l'utilisateur ou encore commander d'envoyer un choc électrique indolore lorsque le porteur ne respecte pas son engagement de s'adonner à une activité sportive.

B - L'internet des objets

La notion d'Objet Connecté renvoie à celle d'« internet des objets » ou l'« *internet of Things* » (IdO), souvent présenté comme la troisième révolution de l'internet – le Web 3.0. Le caractère polysémique du terme qui fait tantôt référence à des réalisations immédiates, tantôt à des utopies, le rend difficilement saisissable.

Il peut néanmoins être défini comme une infrastructure, une sorte de « réseau de réseaux » dans laquelle des milliards de capteurs intégrés dans différents Objets Connectés du quotidien sont conçus pour enregistrer, traiter, enregistrer et transférer des données. Ces objets interagissent avec d'autres appareils, avec d'autres Objets Connectés, avec des individus, ou avec d'autres systèmes capables de communiquer en réseau. Au sein de cette infrastructure, ces objets « connectés » et ces entités numériques s'identifient et communiquent entre eux grâce à des systèmes d'identification électronique normalisés et unifiés, ainsi que des dispositifs mobiles sans fil. Un système de transmission des données alimente une application intelligente, qui est pilotée *via* une interface quelconque telle qu'un *smartphone* ou un ordinateur.

L'internet des objets est donc composé d'une série de systèmes indépendants fonctionnant avec leurs propres infrastructures. C'est pour cette raison que les experts envisagent non pas un internet prolongé au monde physique comme le décrit le terme, mais plutôt des applications (logiciels ou progiciels) et des systèmes intégrés à ces objets qui utilisent les technologies de l'internet. En ce sens, il est plus exact de parler de nets avec des objets (internets et intranets) que d'internet des objets à proprement parler.

2 G. Plouin et N. Colomer sur le blog Octo [en ligne] [consulté le 2 mai 2016], disponible http://blog.octo.com/tag/objets/>.

3 L. n° 78-17 du 6 janv. 1978 relative à l'informatique, aux fichiers et aux libertés.

II - OBJET CONNECTÉ : DE NOUVEAUX RISQUES POUR LA CYBERSÉCURITÉ

A - Identification des risques

Les Objets Connectés constituent des cibles de hautes valeurs pour les attaquants, au regard notamment des données lucratives qu'ils manipulent.

Au vu des données dites « sensibles » que l'Objet Connecté communique et de la nécessité de garantir le droit au respect à la vie privée, des exigences sécuritaires doivent être intégrées à cette technologie. Par ailleurs, l'absence de prise en considération des risques serait vertigineuse au regard des conséquences qu'elle pourrait entraîner en termes de responsabilité civile et pénale. Que se passerait-il dans le cas où un ou plusieurs objets transmettaient des informations erronées suite à une attaque portant sur la construction de réseaux « ville intelligente » dans lesquels des véhicules, des feux tricolores et des systèmes de mesure de trafic seraient mis en relation ? Ou encore dans le cas où des attaquants auraient pour ambition de détourner les fonctions d'Objets Connectés à des fins malveillantes ?

B - L'Objet Connecté : une technologie particulièrement vulnérable

Il apparaît au regard des particularités techniques de l'IdO décrites ci-dessus que ce dernier offre une surface d'attaque considérable. En effet, ces objets ne disposent pas, d'un point de vue architectural, de plateforme unifiée et sont composés d'un nombre important de systèmes connectés. En outre, la communication entre ces systèmes est permise grâce à des moyens divers. Ce constat augmente considérablement les possibilités et « voies » d'attaques.

Malgré l'existence de ces risques, ces objets sont souvent conçus et développés indépendamment des problématiques de sécurité. Ces objets sont peu supervisés, ils ne présentent qu'une faible détection des attaques et ne proposent que peu ou pas de mises à jour. Ce faible niveau de sécurité fait de l'IdO une proie facile pour les *hackers*, qui sont susceptibles d'exploiter les failles pénétrant les systèmes d'information. Cette lacune rend par conséquent ces systèmes d'information vulnérables à tous les risques et menaces issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises.

Enfin, chaque Objet Connecté dispose d'un « compte à privilège » qui le contrôle et offre ainsi un accès important au système d'information. Chaque objet constitue donc une faille dans laquelle les cybercriminels peuvent s'engouffrer.

Cibles de hautes valeurs pour les attaquants, au regard notamment des données lucratives qu'ils manipulent

III - LES RÉPONSES JURIDIQUES

A - En matière de droit pénal

Le code pénal ne prévoit pas d'infraction spécifique aux Objets Connectés et il n'existe pas, de manière générale, de dispositions spécifiques à ces innovations. À ce jour, la notion même d'Objet Connecté n'est pas saisie par le droit en tant que telle. En effet, qualifiés d'« ovnis juridiques » par le ministère de l'Économie, ces objets n'ont ni définition juridique, ni statut. Nous ne sommes pas pour autant confrontés à un « vide juridique ». Le cadre juridique qui trouve à s'appliquer est varié et hétérogène et emprunte à divers domaines juridiques du droit commun : droit des contrats, droit des produits défectueux, droit de la responsabilité, etc.

CE QU'IL FAUT RETENIR

Outre le droit pénal, d'autres domaines du droit – droit à la protection des données à caractère personnel, droit relatif à la cyberdéfense – sont susceptibles d'encadrer la cybercriminalité visant les Objets Connectés et l'internet des objets. Les professionnels peuvent également envisager de sécuriser ces technologies par des moyens techniques, en permettant aux Objets Connectés et à l'internet des objets d'assurer leur propre sécurité.

Le droit pénal préexistant a également vocation à s'appliquer en matière de cybercriminalité dirigée vers l'IdO. En effet, certaines facettes de l'activité criminelle à venir pourront être sanctionnées par ce droit et certaines dispositions applicables aux attaques contre les systèmes informatiques pourront être exploitées.

L'article 323-2 du code pénal punit par exemple 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'IdO. Ce texte permettra également 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 actes cybercriminels pourront également être réprimés sur le fondement de l'article 323-3 du code pénal qui prévoit l'interdiction de 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'IdO pourra par exemple être sanctionnée sur ce fondement.

Pourra également être invoqué l'article 323-1 du code pénal qui prévoit l'interdiction de l'accès ou du maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données.

Dans certains cas donc, les attaquants ne feront que créer des façons inédites de réaliser les infractions préexistantes, et le droit pénal actuel apportera une réponse adéquate.

Cependant, les attaquants appréhendent et exploitent très vite les forces et faiblesses des nouvelles technologies et créent de nouvelles formes d'attaques. Un tel cadre peut donc s'avérer limité. L'encadrement par anticipation de l'ensemble des fraudes s'annonce difficile, tant les situations factuelles et les technologies seront variées. En fonction de l'ingéniosité des délinquants, de nouvelles infractions seront peut-être à définir et inventer. Il est vraisemblable que les nouvelles formes de criminalité trouveront une réponse législative classique en termes d'extension ou de diversification des incriminations ou d'aggravation des peines.

Outre le droit pénal, le droit applicable en matière de protection des données à caractère personnel ainsi que le droit relatif à la cyberdéfense viennent compléter le dispositif et renforcent les obligations incombant à certains acteurs en matière de sécurité des Objets Connectés.

B - L'accroissement progressif des obligations incombant à certains acteurs

1 - Le règlement sur la protection des données à caractère personnel

En matière de protection des données à caractère personnel, les obligations pesant sur le responsable du traitement ont été accrues. En effet, le règlement européen (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données, adopté par le Conseil le 27 avril 2016 et abrogeant la directive 95/46/CE du 24 octobre 1995 sur la protection des données, 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[4]. Il peut notamment s'agir de pseudonymisation et 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, soit en France à la Commission nationale de l'informatique et des libertés (CNIL)[5].

Les concepteurs d'Objets Connectés collectant des données à caractère personnel devront donc se soumettre à ces obligations accrues en matière de sécurité.

2 - La loi de programmation militaire et la directive NIS *(Network and Information Security)*

L'article 22 de la loi de programmation militaire (LPM)[6] prévoit l'adoption de mesures de renforcement de la sécurité des opérateurs d'importance vitale (OIV)[7]. Situés dans quatorze domaines stratégiques appartenant aux secteurs étatiques, de la protection des citoyens et de la vie économique et sociale de la nation tels que le transport, la défense, le nucléaire et l'énergie, ces OIV occupent une place essentielle dans le fonctionnement de la nation. L'État oblige donc ces entreprises à signaler à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) tout incident constaté sur leur système d'information. De même a-t-il donné à l'ANSSI le pouvoir de contrôler leurs systèmes informatiques et de leur imposer des mesures de sécurité. Les décrets d'application imposent également et notamment aux OIV de réaliser des contrôles, d'avoir un certain niveau d'équipement pour détecter les tentatives d'intrusion, ou encore de communiquer avec les victimes sur les attaques subies[8].

La transposition de la directive NIS 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 LPM 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, mais tous les opérateurs dits essentiels à l'économie. La directive s'appliquera ainsi 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, toute intrusion dans leur système informatique.

Les concepteurs d'Objets Connectés investissant ces domaines seront donc contraints par ces obligations.

IV - LES RÉPONSES TECHNIQUES

Outre l'aspect juridique, la cybersécurité de l'IdO peut également être envisagée d'un point de vue technique.

4 Règlement 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, art. 32.

5 Règl. (UE) 2016/679, art. 33.

6 L. n° 2013-1168 du 18 déc. 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, JO 19 déc.

7 Définis par l'art. R. 1332-1 c. défense, les OIV sont des organisations qui exercent des activités comprises dans un secteur d'importance vitale qui a « trait à la production et la distribution de biens ou de services indispensables (dès lors que ces activités sont difficilement substituables ou remplaçables) : satisfaction des besoins essentiels pour la vie des populations ; exercice de l'autorité de l'État ; fonctionnement de l'économie ; maintien du potentiel de défense ; ou sécurité de la Nation » « ou peut présenter un danger grave pour la population » (C. défense, art. R. 1332-2).

8 Décr. n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale ; Décr. n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de services de confiance pour les besoins de la sécurité nationale ; Décr. n° 2015-349 du 27 mars 2015 relatif à l'habilitation et à l'assermentation des agents de l'autorité nationale de sécurité des systèmes d'information.

Exigences sécuritaires dès la conception de ces objets

Comme indiqué précédemment, la difficulté dans ce domaine relève notamment du fait que chaque Objet Connecté représente une porte d'entrée pour l'attaquant, par le biais du « compte à privilège » qui contrôle et offre un accès au système d'information.

Les protections traditionnelles consistant à créer des défenses extérieures au réseau paraissent inadaptées face aux attaques perpétrées *via* ces comptes. C'est pour cette raison que certains professionnels préconisent, non pas d'utiliser à la marge les technologies de l'IdO, mais de sécuriser les activités grâce à ces technologies. Le colonel Éric Freyssinet propose à ce titre d'imaginer des « objets de confiance » qui effectueraient des sortes de « patrouilles numériques », sous le contrôle de ceux qui seraient chargés de sécuriser les systèmes ou même des services de police. Ces patrouilles obéiraient à des règles de transparence et de respect de la vie privée et seraient plus efficaces qu'une observation totalement extérieure telle qu'elle est réalisée aujourd'hui[9].

En d'autres termes, il conviendrait de prendre en compte les exigences sécuritaires dès la conception de ces objets. Dans l'idéal, il conviendrait peut-être même d'intégrer ces exigences sécuritaires techniques dès la conception de ces objets dans le droit positif...

[9] Ministère de l'Économie et des finances et du redressement productif, rapp. préc.