PREISKEL & CO

LA SÉCURITE DE L'INTERNET DES OBJETS

SECURITY ISSUES WITH IOT PRODUCTS

CYBERSECURITE ET VIE PRIVEE : LES OBJETS CONNECTES SONT-ILS SECURISES ?

- Montres, téléviseurs, caméras de surveillance, vêtements, jouets, ampoules, moniteurs d'activité physique, assistants vocaux et même brosses à dents …. Les objets connectés se multiplient dans notre quotidien. Pourtant, ces objets ne sont pas sans risque ! Loin d'être des gadgets, ils sont désormais également des outils de travail utilisés dans des secteurs sensibles, comme ceux de la santé (robots chirurgiens) ou de la défense (drones).
- Parce qu'ils collectent et génèrent une grande quantité de données qui peuvent être stockées sur Internet, ils sont notamment porteurs de risques pour les données personnelles et la vie privée. Dans cet « internet des objets » (ou « IoT »), les failles de sécurité, accidentelles ou malveillantes, existent bel et bien. Les risques de sécurité posés par l'IoT devraient d'ailleurs se multiplier : d'après les travaux de l'IDATE DigiWorld, 35 milliards d'objets seront connectés à Internet d'ici à 2030 dans le monde.
- Les législateurs et les industriels ne peuvent laisser de côté la question de la sécurité de l'IoT, a fortiori à l'ère du RGPD. Quelles menaces font peser les objets connectés ? Que peuvent, ou doivent, faire les fabricants pour prévenir, gérer et corriger les failles de sécurité ? Quelles mesures sont prises par les pays dans le monde pour sécuriser l'IoT, établir un cadre de confiance et développer des bonnes pratiques ?

Les membres du réseau Lexing® dressent un tableau de la situation actuelle à travers le monde. Les pays suivants ont contribué à ce numéro : Afrique du Sud, Allemagne, Belgique, France, Grèce.

CYBERSECURITY AND PRIVACY: HOW SECURE ARE CONNECTED DEVICES?

- *Watches, TVs, CCTVs, clothes, toys, light bulbs, fitness trackers, virtual assistants and even toothbrushes. Connected devices are everywhere in our everyday life, but they could put you in danger! They are not just gadgets, they are now also business tools used in sensitive sectors, such as health (surgical robots) or defense (drones).*
- *Because they collect and generate a large amount of data that can be stored on the Internet, connected devices are a threat to personal data and privacy. In this "Internet of Things," (IoT) security breaches-— whether accidental or malicious — are real. The security risks posed by IoT are expected to increase: according to IDATE DigiWorld, there will be 35 billion connected devices worldwide by 2030.*
- *Legislators and manufacturers cannot ignore IoT security issues, especially in the GDPR era. What are the threats posed by connected devices? What can (or should) manufacturers do to prevent, manage and correct security breaches? What measures are being taken in various countries around the world to secure the IoT, build consumer trust and develop good practices?*

The Lexing® network members provide a snapshot of the current state of play worldwide. The following countries have contributed to this issue: Belgium, France, Germany, Greece, South Africa.

Lexing®

Lexing® est le premier réseau international d'avocats en droit du numérique et des technologies avancées. Créé sur une initiative d'Alain Bensoussan, Lexing® permet aux entreprises internationales de bénéficier de l'assistance d'avocats alliant la connaissance des technologies, des métiers et du droit qui leur sont applicables dans leur pays respectifs.

Lexing® is the first international lawyers' network for digital and emerging law. Created on an initiative of Alain Bensoussan, Lexing® allows multinationals to benefit from the assistance of seasoned lawyers worldwide who each combines unique expertise in technology and industry with a thorough knowledge of law in their respective country.

https://lexing.network

FREDERIC FORSTER

Vice-président du réseau Lexing® et Directeur du pôle Constructeurs Informatique, Télécoms et Electronique du cabinet Lexing Alain Bensoussan-Avocats

VP of Lexing® network Head of the IT and Telco division of Lexing Alain Bensoussan-Avocats

LEXING ALAIN BENSOUSSAN AVOCATS

L'internet des objets en Afrique du Sud

▪ L'Internet des objets (IoT) désigne l'intégration, dans des objets physiques, de puces électroniques et de capteurs, qui permettent de relier ces objets entre eux et à Internet, ces objets devenant alors des « objets connectés ». L'IoT est un phénomène mondial qui touche tous les pays, et l'Afrique du Sud, où un fournisseur a d'ores et déjà déployé un important réseau d'IoT à travers le territoire national (1), ne fait pas exception.

(1) How IoT is quietly taking over South Africa: https://mybroadband.co.za/news/internet-of-things/294358-how-iot-is-quietly-taking-over-south-africa.html

▪ Une question importante se pose : les réseaux de l'IoT sont-ils sécurisés ? La sécurité repose sur des aspects techniques mais aussi humains. Et c'est là que le bât blesse : l'humain est bien souvent le maillon faible de la sécurité des systèmes d'information. Or, l'IoT donne naissance à de nombreux nouveaux dispositifs - téléphones mobiles, vêtements, appareils industriels, etc. - qui servent d'intermédiaires, de passerelles entre les personnes physiques. Le plus grand risque pour la sécurité de l'IoT est précisément là, car aussi solides techniquement que pourraient être ces réseaux, les humains constituent autant de points de vulnérabilités exposant à des risques de fraude, d'hameçonnage ou d'attaques par ingénierie sociale.

▪ Le législateur a instauré des exigences générales en matière de sécurité de l'information qui s'appliquent indirectement à l'IoT, mais sont-elles suffisantes pour prévenir les incidents ?

Les exigences en matière de sécurité de l'information en Afrique du Sud

▪ La loi sud-africaine sur la protection des données n'est pas encore entrée en vigueur, mais lorsqu'elle sera pleinement effective, elle introduira une obligation générale de sécurité obligeant toute personne qui traite les données à caractère personnel de personnes concernées à prendre des « mesures techniques et organisationnelles appropriées et raisonnables » afin de protéger ces données contre tout accès non autorisé (2). Afin de satisfaire à cette exigence, les entreprises seront dès lors tenues d'identifier les risques pour les données à caractère personnel, d'envisager et de mettre en place des mesures de protection, de vérifier régulièrement leur bon fonctionnement et les mettre à jour au besoin (3).

(2) Pour un résumé de la législation sud-africaine sur la protection des données et des liens vers la législation pertinente, cf. : https://www.michalsons.com/focus-areas/privacy-and-data-protection/protection-of-personal-information-act-popia

(3) Pour plus de détails sur l'exigence relative à la sécurité de l'information cf. https://www.michalsons.com/focus-areas/information-technology-law/information-security-law

▪ En outre, la loi sud-africaine sur la protection des données exige des responsables du traitement qu'ils tiennent compte des pratiques et procédures pour la sécurité de l'information qui s'appliquent spécifiquement à leur secteur d'activité ou à leur profession. Autrement dit, les entreprises de certains secteurs d'activité, où sont couramment utilisés des dispositifs de l'IoT, se retrouvent assujetties à des obligations plus strictes. Tel est le cas notamment :

- du secteur bancaire : la loi sur les communications et les transactions électroniques oblige les banques à utiliser un système de paiement suffisamment sûr, compte tenu des normes technologiques acceptées et

(4) Section 43(5) du Electronic Communications and Transactions Act (« ECT Act ») : https://www.internet.org.za/ect_act.html#Information_to_be_provided

du type de transaction concerné (4) - les banques sud-africaines ont de plus en plus recours aux téléphones mobiles, cartes NFC (« Near Field Communication » ou communication en champ proche) et lecteurs biométriques dans le cadre de leurs systèmes de paiement ; et

- du secteur de la santé : la loi nationale sur la santé impose aux responsables des hôpitaux de mettre en place des mesures de contrôle destinées à empêcher l'accès non autorisé aux dossiers médicaux des patients et érige tout manquement en infraction pénale (5) – aujourd'hui, la plupart des hôpitaux sud-africains utilisent des appareils connectés de surveillance cardiaque, respiratoire ou autre des patients dans le cadre des soins.

(5) Section 17 du National Health Act: https://www.up.ac.za/media/s hared/12/ZP_Files/health-act.zp122778.pdf

▪ Malheureusement, il existe très peu de jurisprudence sur la sécurité de l'information en Afrique du Sud, et aucune concernant spécifiquement l'IoT.

La loi sud-africaine ne va pas assez loin

▪ Les erreurs humaines sont souvent à l'origine de failles dans la sécurité de l'information. Ces erreurs peuvent avoir des conséquences non négligeables sur l'économie, comme en témoigne l'actualité récente, car c'est bien une erreur humaine qui a causé la fuite massive de données « Master Deeds » (6) ou encore la cyberattaque dont a été victime la compagnie d'assurance Liberty (7).

(6) Data leak exposes personal records of nearly 1 million South Africans': https://www.timeslive.co.za/ne ws/sci-tech/2018-05-24-data- leak-exposes-personal-records- of-nearly-1-million-south- africans/

▪ Le facteur humain est donc une composante essentielle de la sécurité informatique. Par la création de nombreux nouveaux dispositifs susceptibles d'être détournés par les cybercriminels, notamment via des méthodes d'ingénierie sociale, l'IoT exacerbe les risques existants.

(7) Liberty hack attack': https://www.timeslive.co.za/ne ws/south-africa/2018-06-20-liberty-hack-attack-south-africans-should-be-terrified/

▪ De fait, bien qu'une exigence générale en matière de sécurité de l'information se profile à l'horizon et que des exigences sectorielles soient déjà en place, force est de constater qu'aucune ne traite suffisamment directement de l'IoT pour répondre aux menaces croissantes auxquelles sont exposés les objets connectés en Afrique du Sud.

DAVID LUYT

south-africa@lexing.network

The Internet of Things in South Africa

▪ *The Internet of Things (IoT) is the phenomenon of computer chips and sensors being embedded in everyday physical objects that connect them to each other and the Internet. It's transforming the world, and South Africa is no exception – with at least one provider having rolled out a major IoT network across the country. (1)*

▪ *However, how secure are these sort of networks? While they may be technically robust, the weak link in any information system from a security perspective is often the human element. The biggest security risk of IoT is exactly that – it results in lots of new devices that mediate communications between people, be they mobile phones, wearables or retail and industrial devices. This introduces many more vulnerabilities for fraud, phishing and other social engineering attacks.*

▪ *Legislators are imposing information security requirements that apply to IoT indirectly, but are they enough to prevent incidents?*

Information security requirements in South Africa

▪ *South African data protection law hasn't commenced fully yet, but when it does – it will have an umbrella information security requirement obliging anyone who processes the personal data of data subjects to implement "appropriate and reasonable technical and organisational measures" to protect it from unauthorised access. (2) Businesses will need to identify the risks to the personal data, identify potential safeguards, actually create those safeguards, check that they're working on an ongoing basis, and update them as necessary to satisfy this requirement. (3)*

▪ *South African data protection law also requires those responsible for processing personal data to consider prevailing information security practices and procedures that apply to their industry specifically or in terms of their professional rules and regulations. This obliges South African businesses to comply with more stringent information security obligations in specific industries where data subjects commonly use IoT devices, such as:*

- *banking – where South African electronic communications and transactions law requires banks to use a sufficiently secure payment system, with reference to accepted technological standards and the type of transaction concerned (4) – South African banks increasingly rely on mobile phones, NFC cards and biometric readers as part of their payment systems; and*

- *healthcare – where relevant South African legislation requires the person in charge of a hospital to set up control measures to prevent unauthorised access to patients' health records and criminalises the failure to do so (5)*

(1) How IoT is quietly taking over South Africa': https://mybroadband.co.za/news/internet-of-things/294358-how-iot-is-quietly-taking-over-south-africa.html

(2) A summary of South African data protection law and links to relevant legislation: https://www.michalsons.com/focus-areas/privacy-and-data-protection/protection-of-personal-information-act-popia

(3) More detail on the information security requirement: https://www.michalsons.com/focus-areas/information-technology-law/information-security-law

(4) Section 43(5) of the ECT Act: https://www.internet.org.za/ect_act.html#Information_to_be_provided

(5) Section 17 of the National Health Act: https://www.up.ac.za/media/shared/12/ZP_Files/health-act.zp122778.pdf

– many modern South African hospitals use IoT patient cardiac, respiratory or other monitoring devices.

- *Unfortunately there is very little case law on information security in South Africa, and none specifically in the context of IoT.*

South African law doesn't do enough

- *Peoples' mistakes have long plagued information security in the South African business landscape, with human error (at least in part) causing both the 'masterdeeds' data leak (6) and Liberty attack (7) in recent years.*

- *IoT amplifies the existing risk of operational information security, such as what humans do when faced with social engineering attacks, in the South African business landscape by creating lots of new devices that cybercriminals can exploit to manipulate people.*

- *While there is a general information security requirement on the horizon and industry specific information security requirements in place, none of them deal with IoT directly enough to address the rising threat.*

(6) Data leak exposes personal records of nearly 1 million South Africans': https://www.timeslive.co.za/news/sci-tech/2018-05-24-data- leak-exposes-personal-records- of-nearly-1-million-south- africans/

(7) Liberty hack attack': https://www.timeslive.co.za/news/south-africa/2018-06-20-liberty-hack-attack-south- africans-should-be-terrified/

DAVID LUYT

south-africa@lexing.network

Les objets connectés et la sécurité

▪ Selon une étude de l'association allemande de l'industrie de l'Internet « eco » (« Verband der Internetwirtschaft e.V. »), le marché allemand de l'IoT devrait doubler ses revenus en cinq ans et bénéficier d'une croissance d'environ 19 % par an, pour atteindre près de 16,8 milliards d'euros en 2022. L'Allemagne compte en effet parmi les plus grands marchés de l'industrie 4.0 du monde (industrie automobile, construction de machines et d'installations, notamment) (1).

▪ Les appareils IoT soulèvent souvent des questions en matière de responsabilité et de sécurité informatique, mais également de protection des données. Au cours des dernières années, les spécialistes de la sécurité informatique ont montré à quel point il est facile d'accéder à certains objets pour en prendre le contrôle ou infiltrer le réseau auquel ils sont connectés (2).

Les objets connectés et les données personnelles

▪ Pour fonctionner, les objets connectés ont besoin d'être alimentés par une multitude de données, pouvant provenir de différentes sources.

▪ On peut de manière schématique les diviser en données relatives aux capteurs (données biométriques, caméras vidéo, microphones, etc.) et données relatives aux utilisateurs (données relatives aux comptes d'utilisateurs ou autres données qui peuvent être liées à une personne en particulier).

▪ La masse considérable de données à caractère personnel qui peuvent être, et seront très probablement, collectées par les objets connectés, menace gravement le principe de minimisation des données et, pour cette raison, de nombreux dispositifs connectés sont susceptibles d'être considérés comme contraires à la loi sur la protection des données. Les fabricants doivent donc s'atteler à chercher des moyens de rendre leurs produits conformes à ce principe fondamental de la protection des données. A cette fin, plusieurs solutions s'offrent à eux, telles que l'effacement anticipé des données personnelles, le remplacement d'un traitement de données dans le cloud par un traitement local (« Fog computing » ou informatique géodistribuée dite « en brouillard »), ou encore l'anonymisation et la pseudonymisation des données personnelles.

▪ Autre obstacle au respect de la législation sur la protection des données : l'obtention du consentement effectif de l'utilisateur. Même si l'utilisateur donne son consentement, ce consentement pourrait être considéré comme illicite dans la mesure où son champ d'application ne couvre pas tous les aspects de l'utilisation des données par l'objet connecté. Les systèmes IoT sont effectivement souvent très complexes et déroutants pour le consommateur moyen et il est donc nécessaire de s'assurer que les utilisateurs bénéficient d'une communication claire et complète sur les fonctionnalités de l'objet connecté.

▪ Avec le développement constant des objets connectés et l'importance grandissante de la protection des données, les exigences en matière de mesures techniques et organisationnelles ne cessent d'augmenter. Par exemple, les données très sensibles (telles que les données relatives à la santé issues des bracelets de fitness) exigent un niveau de sécurité informatique élevé. En tout état de cause, les principes de
protection des données dès la conception et par défaut doivent être respectés.

(1) https://www.eco.de/presse/s tudie-von-eco-und-adl-industrial-iot-umsaetze-~~wachsen-bis-2022-jaehr~~lich-rund-19-prozent/

(2) Par exemple : https://www.golem.de/news/smart-home-wenn-die-lampe-zum-trojaner-wird- 1901-138712-2.html

▪ Au niveau européen, la directive sur la responsabilité du fait des produits, dans la mesure où elle ne couvre que les biens physiques, entraîne un certain flou juridique. La Commission européenne mène d'ailleurs actuellement une grande étude visant à évaluer si les règles et le fonctionnement général de cette directive restent appropriés à la lumière de l'évolution technologique, et notamment de l'internet des objets. (3)

▪ Pour aller plus loin sur les questions de responsabilité liées à la fabrication des objets connectés, il convient donc de se tourner vers la législation allemande sur la responsabilité du fait des produits. La loi sur la responsabilité du fait des produits prévoit que le fabricant est responsable sans faute du dommage causé par un défaut de son produit dès lors que ce dernier affecte la vie, l'intégrité corporelle, la santé ou les biens d'une personne. Ce texte couvre les biens meubles, y compris les logiciels intégrés (certains considèrent également les logiciels dits indépendants comme un produit au sens de cette loi), et est donc applicable à la plupart des objets connectés. Le fabricant peut éviter de voir sa responsabilité engagée s'il peut prouver que le dommage ne pouvait pas être évité malgré l'utilisation de mesures de protection conformes à l'état de l'art. En outre, dans certains cas, la responsabilité des fabricants peut être réduite s'ils se conforment à la norme DIN 27072 (4) (Technologies de l'information - Dispositifs compatibles avec l'IoT - Exigences minimales de sécurité de l'information) ainsi qu'au référentiel d'exigences relatif à la sécurité des systèmes informatiques élaboré par l'agence allemande de cybersécurité (BSI). (5)

▪ L'identification des fabricants des différentes parties de l'objet connecté va devenir une réelle problématique juridique dans le domaine de la responsabilité du fait des produits. Pour ce faire, il serait souhaitable que les fabricants décrivent leur apport respectif aussi précisément que possible afin de permettre, le cas échéant, une séparation claire des responsabilités.

▪ Par ailleurs, dans le cadre de la législation sur la responsabilité du fait des produits, le fabricant est, entre autres, soumis à une obligation de surveillance de ses produits. Or, cette obligation peut entrer en conflit avec ses autres obligations découlant de la législation sur la protection des données. Il sera alors nécessaire de déterminer, au cas par cas, si et dans quelle mesure l'obligation spécifique de surveillance des produits justifie l'utilisation des données personnelles.

▪ Actuellement, en cas de dommages causés par un objet connecté, les utilisateurs ne peuvent être tenus responsables que s'ils sont en faute, ce qui dans la pratique est rare en raison de la complexité et de l'imprévisibilité des systèmes informatiques modernes, qui amoindrissent le niveau de l'obligation de contrôle pesant sur l'utilisateur. La possibilité d'un transfert contractuel des risques et des responsabilités sur les consommateurs semble peu envisageable. Le consommateur moyen n'est généralement pas conscient des risques potentiels qu'il s'engage à assumer au moment où il souscrit au contrat d'achat pour l'objet connecté.

▪ Enfin, lorsque les vendeurs d'objets connectés ne sont pas eux-mêmes fabricants de ces produits, les droits de garantie traditionnels entrent également en jeu. La mise en œuvre de ces droits peut, par exemple, résulter d'un manque de sécurité informatique ou d'une défaillance du système.

(3) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0002&from=EN, p. 43ff.

(4) https://www.din.de/de/din-und-seine-partner/presse/mitteilungen/din-spec-27072-mehr-sicherheit-im-smart-home-330088

(5) https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2016/Cyber-Angriffe_durch_IoT-Botnetze_25102016.html

SUSANNE KLEIN
&
ADRIAN VORNWALD

germany@lexing.network

▪ *According to a study by eco ("Verband der Internetwirtschaft e.V."), the German IoT market will generate revenues of around 16.8 billion euros in 2022. This would mean a doubling within five years and a growth of around 19 % per year. Germany is among the world's largest industry 4.0 markets (especially in the automotive industry, but also in mechanical and plant engineering).(1)*

(1) https://www.eco.de/presse/studie-von-eco-und-adl-industrial-iot-umsaetze-wachsen-bis-2022-jaehrlich-rund-19-prozent/

▪ *IoT-devices often raise questions of liability and IT-security, as well as questions of data protection. In recent years, IT security specialists showed how easily they can access some of those devices to gain control over them or infiltrate the network the devices are connected to. (2)*

(2) E.g.: https://www.golem.de/news/smart-home-wenn-die-lampe-zum-trojaner-wird-1901-138712-2.html

Data protection

▪ *IoT products generally offer a broad variety of sources for personal data.*

▪ *They can roughly be divided into sensor data (biometric data, video cameras, microphones, etc.) and user data (data related to user accounts or other data that can somehow be related to an individual person).*

▪ *Due to the sheer mass of personal data that can and most likely will be collected by IoT products, the principle of data economy is critically endangered. Therefore, many devices might be considered inadmissible according to data protection law. To prevent this, manufacturers should seek ways to make their products compliant with this fundamental data protection principle. Possible methods to achieve this could be the early deletion of the personal data, the preference of a local data processing over cloud processing (Fog Computing should be preferred over Cloud solutions) and anonymization and pseudonymization of personal data.*

▪ *Another obstacle to compliance with data protection law could be the obtaining of effective user consents. Even if consent is given, it can still be deemed unlawful as its scope does not cover every aspect of the data use of the IoT product. This is caused by the fact that IoT systems are often very complex and confusing for the average consumer. Thus it is necessary that a clear and comprehensible communication of the functionality of the IoT device is guaranteed.*

▪ *With the constant further development of IoT products and their increasing data protection relevance, the demands placed on the technical and organizational measures are also increasing. For example, IT security must be ensured to a particularly high degree for very sensitive data (e.g. health-relevant data from fitness wristbands). As always, the principles of "privacy by design" and "privacy by default" must be observed.*

Liability

▪ *The European Product Liability Directive is currently a legal grey area, since it only covers physical goods. It is currently under a broad evaluation by the European Commission whether its rules and overall functioning remain appropriate for new technologies such as IoT products.(3)*

(3) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0002&from=EN, p. 43ff.

▪ *For liability issues related to the manufacture of IoT products, a closer look at the German Product Liability Act is required. It states that the manufacturer is liable*

without fault if the defect in a product kills someone, injures their body or health or damages an item. The Product Liability Act covers movable items including embedded software (some voices also consider independent software itself a product in the sense of this law). It is therefore applicable to most IoT products. The manufacturer may be able to evade liability if he can prove that the damage could not have been prevented despite using state of the art protection measures. Moreover, manufactures may be able to limit their liability in certain areas if they comply with DIN 27072 (4) (Information Technology - IoT capable devices - Minimum requirements for Information security) and the BSI catalogue on security requirements for IT systems. (5)

- *An upcoming problem in the area of product liability is the distinction of manufactures of different parts of the IoT product. In order to improve this situation, it could be advisable for manufacturers to describe their respective service as precisely as possible in order to allow a clear separation of responsibilities.*

- *In the context of product liability, the manufacturer must, among other things, comply with product monitoring obligations. These may conflict with data protection law and require a precise examination of whether the specific product monitoring obligation in each case can justify the use of personal data.*

- *IoT users can currently only be held liable if they are at fault. Due to the complexity and unpredictability of modern IT systems and therefore very low control obligations for the user, this case will hardly arise. The possibility of a contractual shift of risks and liabilities to consumers seems unlikely as well. The average consumer will regularly not be aware of the potential risks he or she assumes with his or her acceptance.*

- *In the case of sellers of IoT Products who are not themselves manufacturers the general warranty claims must be taken into account, which may, for example, result from a lack of IT security or a system failure.*

(4) https://www.din.de/de/din-und-seine-partner/presse/mitteilungen/din-spec-27072-mehr-sicherheit-im-smart-home-330088

(5) https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2016/Cyber-Angriffe_durch_IoT-Botnetze_25102016.html

SUSANNE KLEIN
&
ADRIAN VORNWALD

germany@lexing.network

▪ Thermostat réglable par smartphone, caméra de surveillance IP, montre intelligente, tous ces biens de consommation ont un point commun : ce sont des objets connectés, c'est-à-dire des ustensiles courants qui nous fournissent, en temps réel, de l'information, destinées à gérer les environnements (urbains, professionnels, etc.) et à améliorer notre qualité de vie. Selon les dernières estimations, ces machines seront cinq fois plus présentes dans notre quotidien en 2020.

▪ Parmi les enjeux amenés par cet « internet des objets » (IoT), figure sans surprise leur sécurité : les risques de cyberattaques augmentent proportionnellement au nombre de terminaux liés au réseau.

▪ En Belgique, ce risque est notamment allégé par deux nouvelles lois, adoptées sous l'impulsion européenne : la loi du 30 juillet 2018 et la loi du 7 avril 2019. La première, qui met en œuvre certains principes du Règlement général sur la Protection des Données (RGPD), impose au responsable de traitement de prévoir des mesures techniques destinées à assurer la sécurité des données traitées. Quant à la seconde, il s'agit de la récente loi belge qui transpose la directive européenne relative à la sécurité des réseaux et des systèmes d'information (dite directive NIS). Cet instrument législatif impose aux fournisseurs de services numériques européens, dont les prestataires actifs dans le domaine du *cloud* (1), de mettre en place des mesures techniques et organisationnelles destinées à gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information. Les objets connectés, dont les informations sont stockées dans le *cloud*, gagnent ainsi en sécurité.

▪ Par ailleurs, la question de la sécurité physique des usagers d'objets connectés mérite d'être posée. Prenons l'exemple d'un véhicule autonome qui cause un dommage à un tiers. Contre qui ce tiers peut-il agir et sur quelle base ? En l'absence de règle particulière en droit belge, il y a lieu de mobiliser les règles du droit de la responsabilité civile actuellement applicables, et notamment la loi du 25 février 1991 relative à la responsabilité du fait des produits défectueux. Dans ce cadre, la victime devra prouver le défaut du produit (c'est-à-dire son manque de sécurité), le dommage qu'elle a subi et le lien causal unissant les deux.

▪ Bien qu'il existe des règles applicables aux objets connectés dans l'arsenal législatif belge, on regrette qu'elles ne soient pas particulières à ceux-ci. En effet, afin d'encadrer au mieux les enjeux amenés par cette nouvelle technologie, il convient que l'évolution de la loi soit à l'image de l'(a) (r) évolution que traverse actuellement l'environnement numérique.

(1) Ainsi que ceux actifs dans les domaines des moteurs de recherches et de places de marché en ligne

Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel

Loi du 25 février 1991 relative à la responsabilité du fait des produits défectueux

Loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique

PAULINE LIMBREE

belgium@lexing.network

▪ *Adjustable thermostat with smartphones, IP surveillance cameras, intelligent watch, these consumer goods have one thing in common: they are connected objects, everyday utensils that provide us, in real time, information to manage our environments (urban, professional, etc.) and to improve our quality of life. According to the last estimates, there will be five times more of these machines in our daily lives in 2020.*

▪ *Amongst the key issues emerging from this Internet of Things (IoT), no surprise, safety and cyber-security lead the way: the risks of cyberattacks increase in proportion to the equipment connected to the network.*

▪ *In Belgium, two new acts adopted under European initiatives mitigate the risks: the act of 30 July 2018 and the act of 7 April 2019. The first one, which provides certain principles of the General Data Protection Regulation (GDPR), imposes on the controller to provide technical measures to ensure the security of the data processed. As for the second one, it is the new Belgian act that implements the directive concerning measures for a high common level of security of network and information systems (called the NIS directive). That legislative instrument imposes on digital service providers, including the providers of the cloud computing (1), to set up technical and organizational measures to manage risks to the security of network and information systems. The IoT becomes safer this way.*

▪ *Furthermore, the question of the physical security of the IoT user must be put forward. Take the example of a smart car which injures a third party. What legal action does this third party have? Lacking a special rule in Belgium law, we should apply the general rules on civil liability, including the Law of 25 February 1991 on the liability for detective goods. In this context, the victim should prove that the product was defective due to its cybersecurity flaws.*

▪ *Although rules apply on IoT in the Belgian legislation, it is unfortunate that they are not related to these objects. Indeed, to better manage the issues related to this new technology, the legislative changes must be the image of the numeric changes.*

(1) Ainsi que ceux actifs dans les domaines des moteurs de recherches et de places de marché en ligne

Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel

Loi du 25 février 1991 relative à la responsabilité du fait des produits défectueux

Loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique

PAULINE LIMBREE

belgium@lexing.network

▪ Les objets connectés continuent inexorablement leur développement et irriguent non seulement les activités personnelles mais aussi les activités professionnelles.

▪ Dans ce contexte, le respect des impératifs de sécurité devient naturellement incontournable, qu'il s'agisse de la sécurité des accès physiques à ces objets, mais aussi de leur sécurité d'accès logique qui, si elle n'est pas – ou mal – prise en compte peut contaminer l'ensemble de l'écosystème technique auquel ils sont connectés.

▪ Si le travail normatif peine quelque peu à faire émerger un référentiel commun et universel, la réglementation contient déjà un certain nombre de pistes de résolution de ces problématiques sécuritaires, notamment au travers des dispositions du règlement européen 2016/679 relatif à la protection des données à caractère personnel (RGPD) (1).

▪ Entré en application il y a un an, le RGPD renforce, en effet, les obligations en matière de confidentialité et de sécurité (fiabilité de la collecte, des traitements, des flux de données, sûreté contre les intrusions et les vols ou la corruption d'information…).

(1) Règlement (UE) 2016/679 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 (règlement général sur la protection des données).

▪ Si l'obligation de sécurité des données n'est pas nouvelle, le RGPD impose de se conformer à de nouveaux principes et obligations inconnus de bon nombre d'entreprises jusqu'alors.

▪ Ainsi, l'analyse d'impact relative à la protection des données doit être réalisée lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées (2). Cet outil doit permettre aux entreprises de maîtriser les risques identifiés.

(2) RGPD, Art. 35

▪ Par ailleurs, la révélation des failles de données est devenue obligatoire dans la quasi-totalité des cas, tant auprès de l'Autorité de contrôle, telle que la Cnil, qu'auprès des personnes dont les données ont été concernées par ces failles, dès lors qu'il existe un risque avéré ou potentiel d'altération de leurs données à caractère personnel.

▪ Enfin, des mesures de précautions doivent impérativement être prises à l'occasion de la réalisation de flux de données, et ce à plus forte raison lorsque des données d'une particulière sensibilité sont concernées (informations médicales, biométriques, de géolocalisation, relative aux infractions…).

▪ Au regard de ces obligations renforcées, la mise en œuvre par les entreprises de chantiers techniques et juridiques est indispensable, ce d'autant plus que les premières sanctions prononcées par la Cnil sous l'empire du RGPD semblent marquer une nouvelle ère plus répressive.

FREDERIC FORSTER

france
@lexing.network

- *The rise of connected devices is inexorable; they have already become an integral part of our personal and business environments and permeated our everyday life.*

- *Considering their increasing importance, complying with security requirements is essential. The security of the physical and logical access to these devices must be ensured insofar as if these devices are not (or not sufficiently) secure, they can contaminate the entire technical ecosystem to which they are connected.*

- *While standards organizations have some difficulty in developing a common and universal reference framework, some laws and regulations already contain a number of ways of addressing these security issues, including the European Regulation 2016/679 on the protection of personal data (GDPR) (1).*

(1) Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

- *The GDPR, which came into force a year ago, strengthens confidentiality and security obligations (reliability of data collection, processing, transfers, security against intrusion, theft or compromising, etc.) for personal data.*

- *The data security obligation is not new, but the GDPR requires compliance with principles and obligations that were unknown to many companies until now.*

- *For example, a data protection impact assessment must be carried out when the processing of personal data is likely to result in a high risk to the rights and freedoms of data subjects (2). A DPIA is designed to help companies identify risks and control them.*

(2) GDPR, Art. 35

- *In addition, the disclosure of data breaches has become mandatory in almost all cases not only to the Supervisory Authority (such as the CNIL), but also to the data subjects whose data have been affected by these breaches, where there is a proven or potential risk of alteration of their personal data.*

- *It is also essential to take precautionary measures when carrying out data transfers, and be extra careful when particularly sensitive data (such as medical data, biometric data, location data, data on criminal convictions and offences) are concerned.*

- *In view of these increased obligations, companies need more than ever to implement appropriate technical and legal measures, especially since the first penalties imposed by the CNIL under the GDPR seem to mark a new, more repressive era.*

FREDERIC FORSTER

france
@lexing.network

- Une définition de l'IoT L'Agence européenne de la cyber-sécurité (ENISA) définit l'Internet des objets (IoT) comme « un écosystème cybernétique et physique de capteurs et d'actionneurs interconnectés, permettant une prise de décision intelligente » (1). Etroitement lié aux systèmes cyber-physiques, l'IoT est utilisé dans les infrastructures intelligentes, telles que l'industrie 4.0, les réseaux et les transports intelligents… La sécurisation des systèmes IoT présente un certain nombre de défis techniques et juridiques particuliers, compte tenu de la diversité et du grand nombre de dispositifs qui peuvent se connecter à l'IoT, allant de l'électronique grand public aux véhicules, en passant par les dispositifs médicaux et les infrastructures industrielles. Pouvant afficher un taux de croissance annuelle de 31 % (2), le nombre de dispositifs IoT est aujourd'hui estimé à environ 20 milliards. Ce chiffre pourrait atteindre 34 milliards en 2020.
- Les menaces liées à l'IoT. Les attaques par déni de service (DDoS) (comme celle causée par le logiciel malveillant « Mirai ») et les attaques par rançongiciel sont les menaces les plus fréquemment associées à l'IoT. Garantir la confidentialité et l'intégrité des données est essentiel. Les pirates informatiques tirent parti des vulnérabilités actuelles de l'IoT, telles que la faiblesse des mots de passe, l'insécurité des mécanismes par défaut, des services et interfaces, ou encore l'absence de mécanismes de mise à jour sécurisés. (3)
- Le rôle de l'ENISA. Chargée de soutenir l'élaboration de la politique et du droit de l'UE en matière de sécurité des réseaux et de l'information, l'ENISA a également pour mission de soutenir les États membres dans leurs efforts pour développer et améliorer la prévention, la détection et l'analyse des problèmes et incidents de sécurité des réseaux et de l'information et la capacité d'y faire face. L'Agence a publié plusieurs études, documents et rapports relatifs à la sécurité de l'IoT et des infrastructures intelligentes. Elle a récemment diffusé une étude sur les bonnes pratiques pour la sécurité de l'IoT dans le contexte de la fabrication intelligente, qui traite des défis en matière de sécurité et de confidentialité associés au développement de systèmes et de services industriels, accéléré par l'introduction des innovations de l'IoT (4). L'ENISA a également mis au point un outil interactif en ligne destiné à guider les opérateurs et les industries de l'IoT et des infrastructures intelligentes dans leur appréhension des risques (5).
- La technologie 5G. L'IoT devrait bénéficier de manière significative des innovations de la 5G. Cette cinquième génération de communications mobiles offre en effet de multiples avantages pour les objets connectés : ultra haut débit, latence ultra-faible, réductions des coûts, économies d'énergie et capacité système accrue.
- Le cas de la Grèce. La Grèce prépare le déploiement de réseaux 5G, notamment en établissant le cadre réglementaire nécessaire à l'octroi de licences expérimentales aux opérateurs afin qu'ils puissent tester cette technologie. L'autorité grecque de régulation des télécommunications (EETT) a d'ores et déjà pris des mesures et lancé la consultation publique sur la modification des règles encadrant sur l'utilisation du spectre radioélectrique afin de libérer des fréquences pour l'Internet des objets (6).

REFERENCES

(1) https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot

(2) https://en.wikipedia.org/wiki/Internet_of_things

(3) OWASP Internet of Things Project, https://www.owasp.org/images/1/1c/OWASP-IoT-Top-10-2018-final.pdf

(4) "Industry 4.0 - Cybersecurity Challenges and Recommendations", ENISA, May 20, 2019, Catalogue number: TP-03-19-407-EN-N ISBN: 978-92-9204-293-6 DOI: 10.2824/143986, https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations/at_download/fullReport

(5)(5) https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool

(6) "Review of Frequency Bands for the Deployment of 5G Networks", EETT, October 2018, https://www.eett.gr/opencms/export/sites/default/admin/downloads/News/Rpt_5G_Deployment_engl.pdf

GEORGE A. BALLAS
&
THEODORE KONSTANTAKOPOULOS

greece@lexing.network

- IoT; a definition. The European Union Agency for Network and Information Security (ENISA), defines the Internet of Things (IoT) as "a cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decision making" (1). IoT being tightly bound to cyber-physical systems, is an enabler of Smart Infrastructures, such as Industry 4.0, smart grid, smart transport. Securing IoT systems presents a number of unique technical and legal challenges, considering the diversity and vast number of devices that may connect to the IoT, ranging from consumer electronics of everyday use, to vehicles, medical devices and industry infrastructure. The number of IoT devices increased 31% year-over-year (2); today, IoT devices are estimated at around 20 billion, and this figure is expected to reach 34 billion by 2020.

- Common IoT threats. Common IoT threats include denial of service (DDoS) attacks (like the one caused by the Mirai malware), ransomware attacks, etc. Ensuring data privacy and integrity is also an important challenge to deal with. Hackers will take advantage of current IoT vulnerabilities, e.g. weak passwords and insecure default mechanisms, insecure services and interfaces, lack of secure update mechanisms, etc. (3)

- The role of ENISA. ENISA supports the development of EU network and information security policy and law; also supports Member States in their efforts to develop and improve the prevention, detection and analysis of and the capability to respond to network and information security problems and incidents. In this context, ENISA has published various studies, papers and reports on security of IoT and Smart Infrastructures. Relevant is the very recent study on "Good Practices for Security of IoT in the context of Smart Manufacturing", which focuses on addressing the security and privacy challenges related to the evolution of industrial systems and services precipitated by the introduction of IoT innovations (4). Notably, ENISA has also developed an interactive web-based online tool aimed at guiding IoT operators and industries of IoT and Smart Infrastructure when conducting risk assessments (5).

- 5G technology. 5G, the next-generation mobile network, is expected to significantly benefit IoT innovation, providing superfast bandwidth speeds, ultra-low latency, cost reductions, energy savings and higher system capacity.

- Greece. From a regulatory perspective, Greece is now preparing for the deployment of 5G networks, e.g. establishing a regulatory framework for trial licenses of 5G networks; relevant are initiatives taken by the telecoms Regulator, the Hellenic Telecommunications and Post Commission (EETT), including the public consultation on the amendment of the Regulatory Framework for the Use of the Radio Frequency Spectrum for Internet of Things (IoT) applications (6).

REFERENCES

(1) https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot

(2) https://en.wikipedia.org/wiki/Internet_of_things

(3) OWASP Internet of Things Project, https://www.owasp.org/images/1/1c/OWASP-IoT-Top-10-2018-final.pdf

(4) "Industry 4.0 - Cybersecurity Challenges and Recommendations", ENISA, May 20, 2019, Catalogue number: TP-03-19-407-EN-N ISBN: 978-92-9204-293-6 DOI: 10.2824/143986, https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations/at_download/fullReport

(5) https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool

(6) "Review of Frequency Bands for the Deployment of 5G Networks", EETT, October 2018, https://www.eett.gr/opencms/export/sites/default/admin/downloads/News/Rpt_5G_Deployment_engl.pdf

GEORGE A. BALLAS
&
THEODORE KONSTANTAKOPOULOS

greece@lexing.network

LEXING NETWORK

PAYS / COUNTRY	CABINET / FIRM	CONTACT	TELEPHONE	EMAIL
Afrique du Sud *South Africa*	Michalsons	John Giles	+27 (0) 21 300 1070	south-africa@lexing.network
Allemagne *Germany*	Beiten Burkhardt	Andreas Lober	+49 69 756095-0	germany@lexing.network
Australie *Australia*	Madgwicks Lawyers	Dudley Kneller	+61 3 9242 4744	australia@lexing.network
Belgique *Belgium*	Lexing Belgium	Jean-François Henrotte	+32 4 229 20 10	belgium@lexing.network
Canada *Canada*	Langlois avocats, S.E.N.C.R.L.	Jean-François De Rico	+1 (418) 650 7000	canada@lexing.network
Chine *China*	Jade & Fountain PRC Lawyers	Jun Yang	+86 21 6235 1488	china@lexing.network
Costa Rica *Costa Rica*	Lexing Costa Rica	Gabriel Lizama	+506 2253-1726	costa-rica@lexing.network
Côte d'Ivoire *Ivory Coast*	Imboua Kouao Tella & Associés	Annick Imboua-Niava	+ 225 22 44 74 00	ic@lexing.network
Espagne *Spain*	Lexing Spain	Marc Gallardo	+ 34 93 476 40 48	spain@lexing.network
États-Unis *USA*	Greenberg Traurig	Françoise Gilbert	+1 650-804 1235	usa@lexing.network
France *France*	Alain Bensoussan-Avocats Lexing	Alain Bensoussan	+33 1 82 73 05 05	france@lexing.network
Grèce *Greece*	Ballas, Pelecanos & Associates L.P.C.	George A. Ballas	+ 30 210 36 25 943	greece@lexing.network
Hongrie *Hungary*	OPL - Orbán & Perlaki	Miklos Orban	+36 1 244 8377	hungary@lexing.network
Inde *India*	Poovayya and Co	Siddhartha George	+91 80 4115 6777	india@lexing.network
Israël *Israel*	Appelfeld & Co	Ilanit Appelfeld	+ 972 3 60 98 099	israel@lexing.network
Italie *Italy*	Studio Legale Zallone	Raffaele Zallone	+ 39 (0) 229 01 35 83	italy@lexing.network
Japon *Japan*	Hayabusa Asuka Law Office	Koki Tada	+81 3 3595 7070	japan@lexing.network
Liban *Lebanon*	Kouatly & Associates	Rayan Kouatly	+ 961 175 17 77	lebanon@lexing.network
Maroc *Morocco*	Fayçal Elkhatib et Associés S.C.P.A	Hatim Elkhatib	+212 5 39 94 05 25	morocco@lexing.network
Mexique *Mexico*	Carpio, Ochoa & Martínez Abogados	Enrique Ochoa De Gonzälez Argüelles	+ 52 55 25 91 1070	mexico@lexing.network
Norvège *Norway*	Advokatfirmaet Føyen Torkildsen AS	Arve Føyen	+47 21 93 10 00	norway@lexing.network
Nouvelle-Calédonie *New Caledonia*	Cabinet Franck Royanez	Franck Royanez	+ 687 24 24 48	nc@lexing.network
Pologne *Poland*	Traple Konarski Podrecki i Wspólnicy	Xawery Konarski	(+48) 12 426 05 30	poland@lexing.network
Portugal *Portugal*	Alves Pereira & Teixeira de Sousa	João P. Alves Pereira	+ 351 21 370 01 90	portugal@lexing.network
République tchèque *Czech Republic*	Rowan Legal	Josef Donát Michal Nulíček	+420 224 216 212	czechrepublic@lexing.network
Royaume-Uni *United Kingdom*	Preiskel & Co LLP	Danny Preiskel	+ 44 (0) 20 7332 5640	uk@lexing.network
Sénégal *Senegal*	SCP Faye & Diallo	Mamadou Seye	:(+221) 33 823 60 60	senegal@lexing.network
Slovaquie *Slovakia*	Rowan Legal	Josef Donát Michal Nulíček	+420 224 216 212	slovakia@lexing.network
Suisse *Switzerland*	Sébastien Fanti	Sébastien Fanti	+ 41 (0) 27 322 15 15	switzerland@lexing.network

La JTIT est éditée par Alain Bensoussan Selas, société d'exercice libéral par actions simplifiée, 58 boulevard Gouvion-Saint-Cyr, 75017 Paris, président : Alain Bensoussan. Directeur de la publication : Alain Bensoussan - Responsable de la rédaction : Isabelle Pottier Diffusée uniquement par voie électronique - gratuit- ISSN 1634-0701

Abonnement à partir du site : https://www.alain-bensoussan.com/outils/abonnement-petit-dejeuner-debat/