La nouvelle loi fédérale sur la protection des données à l'épreuve de l'Internet des Objets

Nicolas Capt et Fazil Kaan Sezen, le 17 mars 2021

L'Internet des Objets demeure un véritable enjeu en termes de protection des données.

Les citoyens sont confrontés à la prolifération exponentielle d'objets connectés prétendant à accéder à leur quotidien avec la promesse de le faciliter. Mais la présence d'une forme de voile technique sur leur fonctionnement intrinsèque les fait demeurer mystérieux et la multiplication effrénée de ces outils amène d'inévitables questionnements sur l'efficacité de la protection de notre sphère privée et intime.

Défini par l'Union Internationale des Télécommunications (UIT) comme une

> « *infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution* »,

l'Internet des Objets (IdO) s'inscrit *de facto* dans une réalité évolutive et permet une personnalisation à large échelle d'outils interconnectés de diverses natures et qualités.

Les promesses sont évidemment aussi nombreuses qu'alléchantes : la famille est en mesure de mener son ménage selon ses besoins effectifs (l'ère du réfrigérateur à court de soda et des lumières restées inutilement allumées est révolue), l'entreprise gagne en efficacité (les paramètres de production sont optimisés, de même que la relation client) et la société tout entière peut vivre exactement selon ses paramètres de préférences (la ville intelligente gère en temps réel lampadaires, poubelles électroniques et aide au stationnement). Dès lors qu'il est fait usage de paramètres objectivables et que des outils de mesures (capteurs, transmetteurs et récepteurs) peuvent être installés, toutes choses peuvent peu ou prou être (inter)connectées. Les possibilités d'application ne sont ainsi limitées que par l'imagination. De fait, il s'agit de transformer progressivement tous les objets en des ordinateurs programmables dans un scénario qui concrétise un rêve futuriste pour certains et confine au cauchemar totalitaire orwellien pour d'autres.

Une telle infrastructure informatique, ambitieuse dans son objectif de facilitation du quotidien, n'est évidemment pas sans soulever de sérieux questionnements liés à la sécurité des données, notamment du fait des particularités des objets composant le réseau. Chacun est, en effet, soumis à des contingences différentes : certains dispositifs, notamment ceux alimentés par batterie, n'auront pas un pouvoir de computation suffisant pour mettre en œuvre les mesures de sécurité dernier cri, par exemple. Ainsi, certains modes de sécurisation riment avec une consommation d'énergie importante. Ce n'est évidemment là qu'un exemple parmi d'innombrables autres.

En tout état, le réseau est sans nul doute compromis par l'existence de maillons faibles et la multiplication des points d'accès. L'avenir, à cet égard, s'annonce pour le moins sombre. Et ce n'est pas là un scénario catastrophiste futuriste conçu dans un laboratoire de prospective. En 2017, un aquarium intelligent qui avait pour vocation de contrôler et de réguler automatiquement la température et la propreté du bassin, de même que de pourvoir à l'alimentation de ses poissons, a permis une attaque informatique de grande ampleur contre un casino américain. La méthode : passer de l'aquarium à d'autres zones (plus sensibles) du réseau informatique auquel il était connecté. Plus récemment, un chercheur en cybersécurité a réussi à modifier temporairement – et en plein vol ! – la trajectoire de l'aéronef dans lequel il avait pris place, en accédant sans trop de difficulté au système informatique de guidage de l'avion, en passant primairement par le système de divertissement à bord (*Inflight Entertainment System*). Dans les deux cas, et sans entrer ici dans d'inutiles détails techniques, le problème était l'absence d'étanchéité du système sur lequel les objets connectés étaient branchés. Le cyber-meurtre et le cyberterrorisme, longtemps l'apanage un peu fantasque et baroque des auteurs de science-fiction, constituent désormais une réalité glaçante dont rien ne dit que nous serons en mesure de la contrer aisément.

À ce stade, reste que beaucoup d'applications IdO sont déployées au sein de circuits plus ou moins clos qui comptent sur la confiance des participants et l'abondance de ressources, comme dans les entreprises ou les institutions publiques. Le déploiement généralisé de solutions IdO dépend de l'avancée technique, tant en matière d'infrastructure que de sécurité. S'y ajoute la contrainte usuelle d'une limitation des coûts.

L'adéquation de la législation sur la protection des données est particulièrement importante dans le cadre des technologies IdO, étant donné que ces dernières génèrent et collectent, en masse, des données parfois sensibles et ceci en quantités massives, lesdites données étant ensuite soumises au joug algorithmique. En tant que tel, l'IdO pose simultanément l'entièreté des questions essentielles en matière de protection des données (sécurité, profilage, traite-

ment automatisé, interopérabilité et portabilité des données). Sans oublier les principes de responsabilité et de transparence.

L'exemple des robots empathiques, ces compagnons matériels ou dématérialisés auxquels il est possible de se confier et qui sont destinés en première intention aux personnes fragiles (personnes âgées, enfants, personnes souffrant d'un handicap, etc.) apparaît ici particulièrement pertinent. Des exigences accrues de sécurité, d'anonymat et de transparence dans la collecte et le traitement de données s'imposent pour de tels dispositifs, au risque de permettre, à défaut, une collecte à bas bruit et une exploitation ultérieure de données sensibles particulièrement intimes.

La nLPD du 25 septembre 2020 avait pour objectif principal d'inscrire – juridiquement et politiquement – la Suisse dans les nouvelles exigences européennes telles que déduites du (haut) standard continental que constitue désormais le Règlement Général sur la Protection des Données. Plusieurs obligations concrétisant des principes européens se retrouvent ainsi de façon quasi inchangée dans la nLPD (*privacy by design*, portabilité des données, etc.). Cela étant, dans le contexte de l'IdO, c'est bien la reconnaissance légale des procédures de certification qui retient avant tout l'attention.

La certification et la standardisation permettent d'uniformiser les procédés techniques et sont mises à jour selon les évolutions métier. Elles font partie intégrante de la responsabilité du développeur et jouent un rôle important dans le *branding* des produits. Des produits critiques tels que les robots empathiques développeront sans doute leurs propres standards et certificats. De façon plus générale, on notera que c'est une chose qu'un réseau IdO soit développé par une entreprise dans son ensemble, mais que c'en est indéniablement une autre de relier plusieurs outils distincts, chacun développé par une entreprise indépendante, avec des risques éminemment accrus. Seule la standardisation permettra l'interopérabilité, la sécurité et la portabilité des données de divers objets indépendamment développés, sachant toutefois que, selon toute vraisemblance, nombre d'entreprises seront réticentes à procéder de la sorte pour des raisons de concurrence.

Dans un futur proche, il faudra ainsi porter un regard attentif à la standardisation en matière d'IdO, laquelle favorisera sans doute l'adoption et la prise en main de ces technologies par des développeurs indépendants. Cela aurait d'ailleurs comme vertu de maintenir en vie la concurrence ainsi que ses bénéfices avérés pour les consommateurs. Certains standards concernant l'interopérabilité ont été publiés au cours de l'année passée, d'autres sont en développement. Les standards ISO/IEC relatifs aux systèmes de sécurité dans le contexte des

IdO seront en principe publiés en 2022.

En conclusion, la protection des données demeurera sans doute au cœur d'un débat central de l'ère cyber faisant intervenir le besoin de sécurité des citoyens, la course économique des entreprises pour l'adoption généralisée de leurs produits et les failles conceptuelles dans le développement de certains produits. Pour les citoyens, il semble qu'une certaine circonspection soit de mise, pour l'heure à tout le moins. Si prudence est mère de sûreté dans le monde analogique, elle l'est à plus forte raison dans un monde numérique où les échanges de données sont le plus souvent parfaitement invisibles à l'utilisateur.

Proposition de citation : Nicolas Capt / Fazil Kaan Sezen, La nouvelle loi fédérale sur la protection des données à l'épreuve de l'Internet des Objets, 17 mars 2021 *in* www.swissprivacy.law/63

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.