KPMG

Le RGPD, bouclier de la vie privée à l'ère des objets connectés

Comment le RGPD protège les utilisateurs d'objets connectés ?

Des objets connectés qui « sentent » le monde

Thermostats, télévisions, montres, volets roulants, pèse-personnes, voitures, colliers pour animaux, bracelets de « fitness » ou encore enceintes intelligentes, les objets connectés sont déjà largement présents dans nos vies et nous accompagnent au quotidien.
Selon une étude de l'ARCEP et de l'ADEME, la France comptait 244 millions d'objets connectés en 2022.

Un objet connecté se caractérise en premier lieu par sa capacité à « sentir » le monde physique qui l'entoure, grâce à des capteurs, comme des microphones, des caméras, des thermomètres, des capteurs de lumière, de géolocalistion ou de vibrations, etc.
L'objet peut également agir sur le monde physique via un écran, un haut-parleur, ou une commande envoyée à un moteur, une serrure, une vanne, etc.

Un objet connecté peut même, dans certains cas, agir de manière autonome, grâce à des moyens de calculs embarqués et des règles prédéfinies.

Et dans d'autres cas, il peut communiquer, avec un serveur mis en œuvre par le fabricant de l'objet dans le cloud, ou avec une application mobile, via différents types de connectivité (Wi-Fi, Bluetooth, Internet, etc.) Il peut ainsi envoyer des données collectées par les capteurs, et recevoir des commandes pour les actionneurs.
Des algorithmes fonctionnant sur un serveur dans le Cloud ou des intervenants humains (opérateurs, utilisateurs, etc.) analysent les données reçues et donnent des consignes à l'objet.
Par exemple, depuis son téléphone, un utilisateur peut, alors qu'il quitte son lieu de travail, prendre connaissance de la température qui règne dans son appartement, et donner une consigne pour déclencher le chauffage, et ainsi bénéficier d'une température adéquate quand il arrive chez lui;

Des objets connectés peuvent également communiquer entre eux, la donnée issue du capteur de l'un étant utilisée pour commander l'actionneur de l'autre.
Ainsi, un capteur de présence peut déclencher l'allumage d'une lampe.

D'énormes quantités de données personnelles collectées

Bien que les objets connectés soient utiles au quotidien, leur usage n'est pas sans conséquence, et il existe des risques liés à des usages mal intentionnés des données collectés par les objets.
Les milliards d'objets connectés utilisés dans le monde collectent en effet d'énormes quantités de données, qui sont transmises pour stockage, agrégation et analyse centralisée des données collectées sur les serveurs des fabricants.

Or, parmi ces masses de données se trouvent très souvent des données personnelles. Il s'agit en premier lieu de données liées aux propriétaires ou aux utilisateurs des objets, que l'on renseigne souvent au moment de l'installation de l'objet.
On doit aussi considérer des données qui n'ont pas été collectées à proprement dit, mais qui peuvent être déduites des données collectées.
Des algorithmes peuvent en effet permettre d'extraire des données collectées des données spécifiques sur, par exemple, les habitudes de vie ou l'état de santé de la personne concernée.
Ainsi, l'analyse des données d'une serrure connectée permet de savoir quand les occupants d'un appartement sont présents ou absents.
Les données de géolocalisation d'un véhicule permettent de savoir, avec une probabilité élevée, où son propriétaire se trouve.
L'analyse du rythme cardiaque provenant d'un bracelet de « fitness » connecté peut amener à identifier des pathologies.

Il peut également être possible de « désanonymiser » des jeux de données ne contenant pas les identités des personnes.

Ainsi, des données anonymisées de géolocalisation peuvent révéler l'adresse d'une personne, comme le montre une étude récente du LINC, le laboratoire d'innovation numérique de la CNIL.
Il suffit d'identifier l'emplacement où une personne passe la majorité de son temps.
Enfin, des données personnelles provenant de différents objets connectés et/ou d'autres sources peuvent être croisées afin d'en tirer des enseignements supplémentaires.
Prenons l'exemple d'un magasin qui collecte les données de géolocalisation de ses clients via une application installée sur les téléphones portables.
De telles données peuvent être croisées avec les données provenant du programme de fidélité pour proposer des offres personnalisées et maximiser la probabilité d'achat. En outre, les données collectées par les objets connectés permettent de réaliser des analyses sur des populations entières. Ainsi, pendant la crise du Covid19, Google publie des données sur le respect des mesures de confinement ville par ville, en se basant sur les données de géolocalisation remontées par les téléphones Android.

Des risques multiples pour la vie privée

Un fabricant d'objets peut donc avoir la possibilité, sur le plan technique, de réaliser des analyses lui permettant d'inférer de nouvelles catégories de données personnelles, parfois sensibles, telles que les adresses physiques, les états de santé, les pratiques religieuses, les opinons politiques, les habitudes de consommation, les revenus des ménages, les fréquentations, etc.
La grande puissance de calcul dont disposent les serveurs permet d'effectuer des analyses très poussées, allant bien au-delà de ce que l'on croit capable d'un objet connecté.
La tentation peut exister de monétiser ces données, en les revendant à d'autres organisations. Ainsi, un fabricant d'objets connectés destinés à surveiller le sommeil des utilisateurs pourrait créer un algorithme lui permettant d'identifier les insomniaques, et revendre les données à un producteur de somnifère. Le fait que les données soient a priori anonymisées ne représente pas une garantie absolue.
Il faut aussi réaliser que, contrairement à des applications web ou mobile à qui nous fournissons des données (post de réseaux sociaux, « like », etc.), la collecte de données par des objets connectés se fait souvent de façon invisible pour les utilisateurs des objets via les capteurs.

Des objets connectés peu sécurisés

On vient de voir que l'utilisation d'objets connectés implique des risques liés à des collectes ou des traitements de données personnelles abusifs. Mais d'autres scénarios de risques existent. Ils sont rendus possibles par le niveau de sécurité, la plupart du temps faible, des objets eux-mêmes.

Les objets connectés sont souvent livrés avec des identifiants d'utilisateurs et des mots de passe par défaut qui sont connus car inscrits dans les documentations des produits ou dans des bases de données spécialisées disponibles sur Internet.
Ces mots de passe sont rarement modifiés car leurs utilisateurs ne savent pas qu'ils doivent le faire ou n'en voient pas l'utilité. Ainsi, il est fréquemment possible de se connecter à des objets comme des caméras connectées avec un mot de passe comme « admin » ou « password » ou « default ».

Une autre lacune couramment rencontrée est la non-application des mises à jour fournies par les fabricants. De tels correctifs sont publiées par les fabricants et permettent de remédier aux failles de sécurité découvertes au fil du temps dans les objets connectés.
Mais elles sont rarement appliquées car les propriétaires et utilisateurs des objets ne sont pas au courant de leur existence, ne savent pas comment les appliquer, ou n'en voient pas la nécessité.

En outre, les objets connectés utilisent souvent des technologies, des architectures, des protocoles de communication et des mécanismes de sécurité variés.

Une maison intelligente peut ainsi comprendre une grande variété d'appareils provenant de divers constructeurs, tels que des thermostats intelligents, des caméras de sécurité et des assistants domestiques, chacun ayant son propre hardware, ses propres logiciels et ses propres protocoles de communication.
Cette hétérogénéité rend difficile établissement de règles de sécurité générales.

Enfin, les utilisateurs sont souvent tentés de rendre l'objet accessible depuis Internet, afin de pouvoir le commander à distance.
C'est pratique et tentant, mais cela entraine un accroissement considérable de la surface d'exposition et donc de la vulnérabilité de l'objet.
Mot de passe facilement devinable, fail les de sécurité non corrigées et exposition sur Internet peuvent donc être exploités par des personnes mal intentionnées pour s'introduire sur des objets connectés.
L'intrus peut alors prendre connaissance des données collectées par l'objet, comme des enregistrements vidéo ou sonores.
Il peut également, selon les cas, agir sur les capteurs, par exemple en diffusant des messages sonores par le biais d'un haut-parleur, ou en déverrouillant une porte protégée par une serrure connectée.

Par ailleurs, ces vulnérabilités des objets connectés en font des cibles prisées par les botnets, ces réseaux de systèmes compromis qui sont utilisés pour réaliser différents types de malversations (déni de service, spam, etc.).

Des réglementations pour l'instant parcellaires

Bien que les objets connectés soient aujourd'hui omniprésents, et en dépit des risques spécifiques et non négligeables liés à leur essor de ces objets, il n'existe pas, pour le moment, une réglementation spécifique portant sur ce type de technologie.
La Californie a été pionnière en votant en 2018 une loi qui exige des fabricants d'objets connectés un certain nombre de mesures de sécurité, comme l'absence de mots de passe par défaut. L'Europe a édicté des réglementations sectorielles incluant des exigences de cybersécurité sur des objets connectés. Ainsi en est-il des règlements MDR (Medical Device Regulation) et GSR (General Safety Regulation) portant respectivement sur les dispositifs médicaux et sur les véhicules routiers. Mais le futur règlement Cyber Resilience Act, qui portera notamment sur la sécurité des objets connectés, est en cours de discussion et ne rentrera pas en application avant plusieurs années.

Par ailleurs, les objets connectés sont conçus dans un pays, fabriqués dans un deuxième, vendus et utilisés dans un troisième et les données collectées sont envoyées dans un serveur localisé dans un quatrième pays. Il en résulte une difficulté accrue à identifier les différentes juridictions à considérer, les éventuelles réglementations à respecter et les régulateurs à satisfaire.

Des objets connectés très souvent concernés par le RGPD

Le Règlement pour la Protection des Données Personnelles s'applique dès que des données personnelles de personnes physiques résidant en Europe sont collectées et traitées. Il suffit donc qu'une personne porte sur elle un objet connecté (bracelet de fitness), soit transportée par un objet connecté (voiture), utilise des objets connectés dans son domicile (thermostat) ou voit simplement ses données captées par un objet (caméra de surveillance sur la voie publique) pour que la règlementation européenne s'applique.
Bien sûr, il existe des cas où des objets connectés ne sont pas concernés par le RGPD car ils ne collectent pas des données personnelles. On peut, par exemple, penser à des balises de géolocalisation placées sur du bétail, ou des objets connectés utilisés dans le monde industriel, pour par exemple surveiller une chaine de production. Mais étant donné le caractère très étendu de la notion de données personnelles (« […] toute donnée qui permet d'identifier directement ou indirectement une personne physique […] » article 4.1 du RGPD), la majeure partie des objets connectés utilisés en Europe doit être considérée comme relevant du RGPD, de même que les serveurs et applications mobiles associées. En outre, la règlementation s'applique quelle que soit la nationalité ou la localisation des entreprises concernées.

Des principes très utiles pour la protection des données personnelles collectées par les objets connectés

Le RGPD représente un cadre exigeant qui vise à réduire les risques engendrés par la collecte des données personnelles. Il édicte plusieurs principes qui se révèlent très utiles pour maîtriser les risques sur la vie privée des personnes liées aux objets connectés.

Ainsi, le principe du « by design » exige des fabricants d'objets qu'ils analysent, dès la phase de conception de l'objet, les risques pour les personnes et qu'ils prennent les mesures nécessaires pour réduire ces risques.

Le principe de minimisation énonce que les données personnelles collectées doivent être limitées au strict nécessaire pour atteindre les objectifs spécifiés dans la finalité du traitement, ce qui permet ainsi de réduire les risques liés à la collecte massive de données.

De même, le principe de finalité déterminée énonce que les données personnelles ne doivent être collectées que pour des objectifs spécifiques, explicites et légitimes, et ne doivent pas être traitées ultérieurement de manière incompatible avec ces objectifs.
Ce principe permet donc de contrôler les analyses réalisées par les fabricants sur les données transmises sur les serveurs. Ainsi, dans l'exemple précédemment cité, le RGPD interdirait de revendre les données des insomniaques à des fabricants de somnifères.
Le principe de transparence demande que les personnes dont les données sont collectées (propriétaires des objets, opérateurs, utilisateurs, mais aussi toutes personnes « captées » par l'objet) soient informées des finalités et des modalités du traitement.
Cette exigence de transparence se révèle particulièrement utile dans le cas d'objets connectés qui collectent des données personnelles de manière discrète, voire invisible, car il permet aux personnes de savoir quelles données sont collectées sur eux. De même, les personnes peuvent savoir quels traitements sont réalisés sur les serveurs à partir des données collectées.

Enfin, le RGPD impose aux responsables de traitements de mettre en œuvre des mesures techniques et organisationnelles appropriées pour maîtriser les risques liés à la confidentialité, l'intégrité et la disponibilité des données personnelles.
La règlementation ne liste pas de manière précise les mesures de sécurité à mettre en place pour couvrir les risques.
Il appartient au responsable de traitement de se reporter à des référentiels de sécurisation spécialisés pour les objets connectés pour identifier et sélectionner de telles mesures.
Les règlementations à venir seront sans doute plus explicites, mais les principales mesures sont d'ores et déjà connues (suppression des mots de passe par défaut, utilisation de mécanisme d'authentification à deux facteurs, publication des correctifs de sécurité, simplification des procédures d'application des correctifs, réduction de la surface d'exposition, chiffrement des flux de communication, etc.).

Le RGPD, un cadre efficace pour la maîtrise des risques liés aux objets connectés

Les objets connectés peuvent faciliter et améliorer l'existence de ceux qui les utilisent, mais ils génèrent également des risques importants pour la vie privée des individus.
Les quantités considérables de données personnelles traitées par ces technologies peuvent être exposées à des abus par des acteurs indélicats ou malveillants. En l'absence de réglementation spécifique aux objets connectés, le RGPD constitue un cadre éprouvé qui permet le développement des nouvelles technologies tout en assurant la protection des personnes dont les données sont collectées. Son application peut certes se révéler plus complexe qu'un traitement de données dans un système d'information classique, mais ses principes peuvent aider les responsables d'un projet d'objet connecté à prendre les bonnes décisions, et in fine mettre sur le marché un produit performant et respectueux des droits des personnes.


▸RS:/0211 SEARCH...A01
▸RS:/0211 SEARCH...A01
▸TR/01ON ▸TR/01▸03
▸TR/01ON ▸TR/01▸03
▸TR/01▸03
▸TR/01▸03
▸SEARCH▸TR/01▸03
▸SEARCH▸TR/01▸03
▸SEARCH▸TR/01▸03
▸SEARCH▸TR/01▸03
▸RS:/011
▸RS:/011
▸RS:/0211TR /ON
▸RS:/0211TR /ON

Contacts

KPMG France
Tour EQHO
2 avenue Gambetta
92066 Paris La Défense Cedex
France

Linda Valero
Manager Advisory, Cybersecurité
& Privacy, Connected Tech
0626894906
lindavalero@kpmg.fr

Charlène Lecuyer
Consultante Advisory, Connected Tech
0628020201
charlenelecuyer@kpmg.fr

www.kpmg.fr