Objets connectés : les enjeux juridiques

Partie I – Penser la protection des données personnelles

LABEL CNIL FORMATION

Cette année, à l'occasion de conférences, de salons et d'échanges avec la presse ou encore d'interrogations de la part de notre clientèle, nous avons été amenés à traiter des enjeux juridiques des objets connectés à de nombreuses reprises.

Les objets connectés existent depuis quelques temps déjà, seule leur médiatisation est nouvelle. En revanche, il n'existe toujours pas de définition officielle. Plusieurs appellations se rapportent ainsi à ce phénomène : objets communicants, objets intelligents ou bien encore internet des objets (littéralement traduit de l'anglais « *Internet of Things* » ou IoT).

Chacun d'entre nous constate l'intérêt croissant du public (ou des publicitaires) pour les objets connectés. Il suffit pour cela de prendre le métro ou de se rendre dans les grandes surfaces. On entend et on lit que ces objets ont vocation à faire partie intégrante de nos vies et qu'il s'en crée un nouveau pratiquement tous les jours. Pour les promouvoir, les distributeurs s'adressent à l'individu (vie privé), au travailleur (environnement professionnel) et au citoyen (espace public). En témoignent également les encouragements de la part du Gouvernement aux startups qui créent et commercialisent ces objets.

Signe de l'intérêt croissant suscité par ces objets et de l'opportunité économique qu'ils représentent, le Président de la République inaugurait lui-même la Cité de l'objet connecté, à Angers, le 12 juin 2015.

Ces objets connectés sont bien souvent considérés comme étant la quatrième révolution de l'internet après l'internet lui-même, le e-commerce et l'apparition des réseaux sociaux. Chacune de ces « révolutions » a conduit à des changements importants dans la vie des internautes, dont certains ont donné lieu à de nouvelles

législations, notamment en vue de la protection du consommateur. Ainsi, pour toute entreprise qui souhaite se lancer dans l'aventure des objets connectés, il est vivement conseillé d'anticiper l'application du droit existant et à venir. Le respect des règles en vigueur permet en effet une crédibilité auprès des consommateurs et auprès des éventuels investisseurs.

Les objets connectés feront l'objet de beaucoup d'attention en cette fin d'année et pas seulement aux pieds des sapins. Il est en effet certain que ces objets sont porteurs de nombreux projets dans des domaines extrêmement variés. Les entreprises françaises l'ont d'ailleurs démontré en début d'année 2015 avec une présence très remarquée au Consumer Electronics Show de Las Vegas[1].

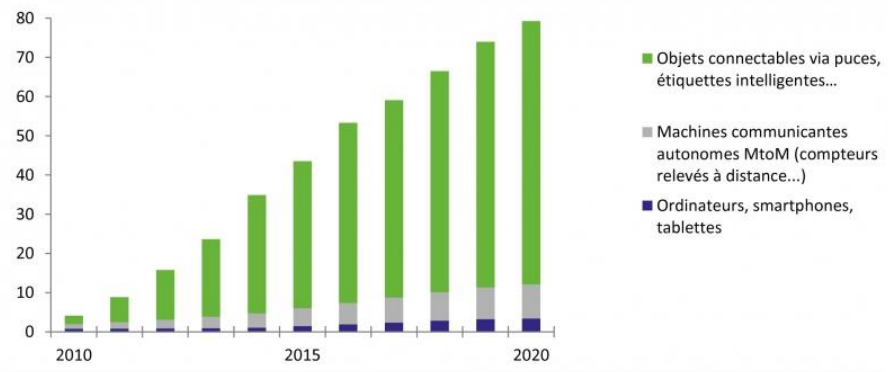
Nous vous souhaitons une bonne lecture, en espérant sincèrement que les lignes qui suivent pourront vous être utiles dans vos projets.

Garance Mathias
Avocat à la Cour

[1] France 24, *French Firms eye gadget market at Vegas Tech show*, 06/01/2015.

I. Les objets connectés et leur environnement

Même si tous les acteurs ne s'accordent pas sur les chiffres, la plupart s'entendent sur le fait que les prévisions en matière d'évolution des objets connectés sont importantes, voire exponentielles. France Stratégie a publié une note d'analyse en ce sens intitulée « Demain, l'Internet des objets » afin d'exposer les prévisions quant au nombre des objets connectés.



Source : http://www.strategie.gouv.fr/publications/demain-linternet-objets
Extrait de la note d'analyse « Demain, l'Internet des objets » publié le 12 janvier 2015

Cette croissance s'explique notamment par la grande diversité de secteurs pouvant être concernés par l'internet des objets. De la santé à l'écologie, en passant par l'habitat ou bien encore les assurances, les objets connectés sont partout.

A. Des objets qui communiquent

L'Internet des Objets fait référence à la possibilité pour les objets du quotidien de se connecter à Internet et de transmettre et recevoir des données. Par objet connecté, on désigne ainsi la domotique qui permet par exemple l'éclairage automatique de votre porche lorsque vous rentrez du travail ou encore les bracelets qui partagent avec vos amis le nombre de vos pas dans la journée ou votre temps de « *running* ».

L'appellation « *Internet des Objets* » sous-entend une certaine communication entre les objets connectés et leurs utilisateurs. On parle alors de la « *relation objet à personne* ».

Par ailleurs, ces objets connectés communiquent également entre eux. Dans ce cas, on utilise la formule « *relation objet à objet* ». À titre d'exemple, et dans le cadre d'objet lié à la santé, il est possible de mettre en avant le cas de la balance et d'une application installée sur le *smartphone* de l'utilisateur soucieux de son état physiologique.

Enfin, on entend également la formule « *Machine to Machine* », aussi connu sous l'appellation de M2M. Cette notion fait référence à l'utilisation d'un appareil (tel qu'un compteur par exemple) dont les données seront transmises par voie de communication fixe ou bien mobile vers une application. Celle-ci permettra alors à l'utilisateur de lire les informations qui auront été lues et analysées à l'issue d'une captation de données définie.

B. Un espace professionnel concerné

1. L'environnement professionnel impacté

Les objets connectés sont appelés à modifier l'environnement de travail. Tout comme cela a pu être le cas avec les ordinateurs portables ou les *smartphones*. De nouveaux modes de travail sont en effet apparus avec le développement de ces appareils comme le télétravail ou le BYOD.

Il n'est pas rare de voir des capteurs installés dans les locaux des entreprises et des administrations afin d'améliorer la sécurité ou faire des économies d'énergie. Par ailleurs et à titre d'illustration, les objets connectés peuvent permettre de contrôler l'accès aux locaux.

La pratique du *Wear Your Own Device* pourrait faire son entrée dans les entreprises. Il s'agit de la pratique qui consiste à porter les objets connectés sur soi. On peut ainsi facilement imaginer l'utilisation de montres connectées permettant d'accéder aux mails professionnels, des lunettes intelligentes ou encore d'autres objets selon le type d'activité concernée.

2. Les modes de travail impactés

L'environnement professionnel est impacté, tout comme les modes de travail. Ainsi, des casques de chantier connectés ont été créés, traitant des données et capables de repérer un circuit défectueux par exemple[2]. De même, on peut légitimement s'attendre à un recours de plus en plus important aux objets connectés dans le domaine médical[3].

On parle encore peu de l'Intranet des Objets. Néanmoins, il s'agit là d'une pratique qui peut être appelée à se développer, ne serait-ce que pour des questions de sécurité. Au sein d'une entreprise, la construction d'un réseau propre aux objets connectés pourrait constituer une nouvelle étape dans le cadre de la sécurisation de l'entreprise. Il conviendra alors d'encadrer l'utilisation de ce réseau et les pratiques de travail liées au développement de ces objets connectés.

C. L'espace public, terrain de jeu des objets connectés

L'espace public est également appelé à connaître divers changements avec l'arrivée des objets connectés, ce que recouvre notamment la notion de « smart city ». C'est en effet le cas des villes qui peuvent recourir au savoir-faire de certaines entreprises utilisant la technologie de l'Internet des Objets pour répondre aux enjeux relatifs à l'aménagement urbain ou bien encore aux défis énergétiques actuels. Il pourra s'agir par exemple de déterminer le trafic routier afin d'améliorer la circulation, la qualité de l'air, l'éclairage ou bien encore les questions de collecte de déchets pour limiter la pollution. L'objectif pourrait également être l'optimisation des services de la ville en tentant de faire des économies d'énergie, ce qui est largement mis en avant à l'occasion de la COP21[4].

La principale problématique juridique provient de l'intérêt des « smart cities », à savoir l'adaptation des services fournis par les « villes intelligentes » aux besoins de chacun des citoyens qui s'y promènent.

[2] http://hardware.daqri.com/smarthelmet/
[3] https://www.aruco.com/2015/08/medecine-connectee/

[4] Voir le site web spécialement créé pour l'événement : http://www.cop21.gouv.fr/fr

Plus précisément, ce n'est pas tant l'adaptation qui pose problème mais plus les moyens permettant d'atteindre cet objectif. Pour adapter un service, il faut connaître les attentes et les préférences de ses utilisateurs. Tout l'enjeu réside donc dans la protection des attentes et des préférences révélées par les citoyens.

Qui dit transmission de données, dit risque de fuite de données. Des accès non autorisés aux informations peuvent avoir lieu, des utilisations de données non consenties peuvent être réalisées, des attaques peuvent être facilitées sur d'autres systèmes, sans parler de l'atteinte au droit au respect de la vie privée ou au droit des données à caractère personnel.

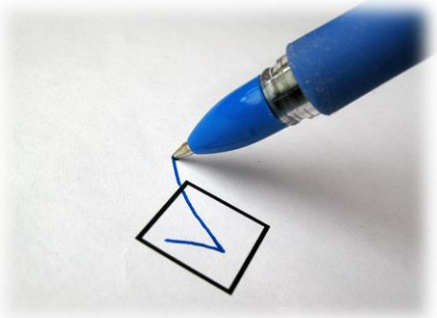
L'usage des objets connectés s'accompagne d'une augmentation significative du nombre de données à disposition des acteurs du marché parmi lesquelles les données à caractère personnel figurent en première place. La protection de ces dernières sera un enjeu prépondérant, à la fois technique et juridique.

II. Les droits des personnes à l'heure des objets connectés

A. Le consentement de l'utilisateur

L'une des premières interrogations en ce qui concerne la collecte des données à caractère personnel est bien entendu la question de la manière dont la collecte elle-même est opérée mais aussi le traitement suivi. Comment ces données sont-elles collectées ? Où sont-elles stockées ? L'utilisateur du moteur de recherche ou d'une application est-il conscient de la valeur commerciale de ses données ? A-t-il donné son accord exprès ?

Le consentement est fondamental en matière de collecte de données. Cette condition est souvent rappelée dans les différentes législations ayant trait aux données à caractère personnel.



La Directive 95/46/CE est la législation actuellement en vigueur à l'échelle de l'Union européenne. Bien qu'une proposition de Règlement sur la protection des données soit encore dans les rouages du processus législatif européen, c'est donc le texte de 1995 qui nous intéresse. Ainsi, l'article 2 de la Directive dispose que le « *consentement de la personne concernée* » signifie « *toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement* ». Le consentement est donc le maître mot et constitue la règle dans ce domaine.

L'article 8 de la Directive porte sur les catégories particulières de données, soit les données sensibles. Il est ainsi précisé que « *les États membres interdisent le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle* ». L'article 8-2 dispose que cette disposition ne s'applique pas lorsque « *la personne concernée a donné son consentement explicite à un tel traitement, sauf dans le cas où la législation de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut être levée par le consentement de la personne concernée* ».

On notera alors que le consentement doit être explicite. Ainsi, une simple navigation sur un site Internet ou la simple utilisation de l'objet connecté ne peut être considérée

comme un consentement, même implicite. La Commission des clauses abusives a ainsi pu le rappeler lors d'une recommandation relative aux réseaux sociaux en novembre 2014[5].

La question du consentement prend un relief particulier en présence d'un objet connecté dès lors qu'il se traduit par l'acceptation des conditions générales d'utilisation. Le consentement sera-t-il considéré comme éclairé lors que l'on sait que ces conditions générales sont peu lues ?

B. Les droits d'accès, de rectification et de retrait de l'utilisateur

L'utilisateur de moteurs de recherches, de réseaux sociaux, d'applications mais aussi d'objets connectés doit être conscient de la valeur des données qu'il transmet aux différents responsables de traitement.
Il est ainsi désormais commun de dire que l'utilisateur est lui-même le prix des services rendus par les applications[6].

L'un des droits qui en résulte et qu'il convient de préciser ici est celui de l'accès aux données. Celui-ci consiste, concrètement, en la possibilité pour un utilisateur de demander au responsable de traitement s'il possède ou non des informations le concernant et de les lui communiquer[7]. Il suffit alors de demander aux responsables de traitement une copie des données qu'il a en sa possession, en les faisant parvenir au demandeur dans un format accessible et lisible par ce dernier. La finalité de ce droit est donc la possibilité de vérifier l'exactitude des informations en possession des sociétés ou administrations visées.

Vient alors la possibilité d'exercer un autre droit complémentaire : celui du droit à la rectification. Celui-ci permet donc d'éviter la transmission d'informations erronées sur l'utilisateur ou bien encore de retirer certaines informations si l'utilisateur le souhaite. On parle alors de droit de retrait. Ces droits sont d'ailleurs assez mis en avant actuellement du fait de la grande attention portée au droit à l'oubli ou au déréférencement en Europe. On peut alors rappeler la décision de la Cour de justice de l'Union européenne en date du 13 mai 2014[8], décision dont le retentissement a été international.

A ces droits, s'ajoute un principe que chaque responsable de traitement doit intégrer dans ses politiques de traitement de données à caractère personnel, soit la proportionnalité ou la pertinence des données collectées, notamment eu égard à leur caractère sensible.

C. Proportionnalité

Les entreprises devraient limiter la collecte et la conservation des données des utilisateurs au strict minimum. Il s'agit également de supprimer les données dont elles n'ont plus besoin pour fournir le service aux utilisateurs.

Le principe de minimisation des données inquiète certains acteurs, quant au frein éventuel à l'utilisation innovante des données. Les entreprises et administrations doivent toutefois limiter la collecte et la conservation des données de leurs consommateurs aux volumes et catégories nécessaires à l'exercice de leurs

[5] Recommandation n°2014-02 de la Commission des clauses abusives. Voir notre article sur « la Commission des clauses abusives, les données personnelles et les réseaux sociaux » du 17 novembre 2014. www.avocats-mathias.com
[6] http://www.internetactu.net/2012/02/27/quand-vous-ne-voyez-pas-le-service-cest-que-vous-etes-le-produit/

[7] Article 39 de la loi du 6 janvier 1978 modifiée
[8] CJUE, Google Spain SL, Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González, 13 mai 2014

acticités. En effet, la mise en œuvre de ce principe de minimisation est intéressante à deux titres. D'une part, un grand volume de données représente une cible bien plus intéressante pour les cyberdélinquants et/ou cybercriminels. D'autre part, si une entreprise collecte et conserve d'importants volumes de données, le risque inhérent est que ces données soient un jour utilisées pour une finalité différente de celle pour laquelle elles ont été recueillies.

Focus sur la géolocalisation

La directive du 12 Juillet 2002 définit en son article 2.c les « données de localisation » comme « toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur de communications électroniques accessible au public ».

Or, de nombreux objets connectés permettent de savoir où se situe exactement son utilisateur. Si ces données viennent à être détournées, elles pourraient être très utiles à certaines personnes malveillantes.

Les industriels doivent donc assurer la sécurité du produit dès la conception. De plus, conformément à l'article 226-17 du Code pénal, le non-respect de l'obligation de sécurité imposée à tout traitement de données à caractère personnel est sanctionné de 5 ans d'emprisonnement et de 300 000 € d'amende. Lorsque c'est une personne morale qui est en cause, l'amende peut être multipliée par 5 et atteindre jusqu'à 1 500 000 €.

Dès lors, il est fortement conseillé aux entreprises d'étudier leurs politiques de collecte et de traitement des données à caractère personnel de leur clientèle, ainsi que leurs besoins d'en connaître dans l'exécution de leurs prestations. Puis, à la suite de cette étude, les responsables de traitement seront en mesure de fixer des limites raisonnables à la collecte des données clients et décider de :

- Ne pas collecter de données ;
- Collecter uniquement et seulement les catégories de données nécessaires au fonctionnement du produit ou du service ;
- Collecter des données moins sensibles ;
- Anonymiser les données qu'ils collectent ;
- Etc.

Ces différents droits sont d'autant plus importants que les données peuvent parfois faire l'objet de transferts vers l'Espace Économique Européen (EEE), voire d'autres États qui n'ont pas forcément le même niveau d'exigence en ce qui concerne leur protection.

III. Le partage des données collectées

A. Le transfert des données par les objets connectés

L'internationalisation des échanges est également à prendre en compte. Internet a accentué les échanges de données de part et d'autre de la planète.

Le principe est celui de l'interdiction du transfert des données en dehors de l'EEE composé de l'Union européenne, du Lichtenstein, de l'Islande et de la Norvège, lorsque le niveau de protection n'est pas adéquat. Certains pays sont toutefois reconnus comme ayant un niveau adéquat de protection des données personnelles des citoyens européens. Les Etats-Unis, avec le *Safe Harbor*, étaient considérés comme tels.

Attardons-nous sur le *Safe Harbor* qui fait actuellement l'objet de négociations à la suite des révélations liées à l'affaire Snowden et de l'arrêt rendu par la Cour de Justice de l'Union Européenne, le 6 octobre 2015[9]. La Cour a en effet invalidé la décision par laquelle la Commission européenne avait constaté que les Etats-Unis assurent un niveau de protection suffisant des données à caractère personnel des citoyens européens.

La Cour a rappelé que « *l'Union est une Union de droit dans laquelle tout acte de ses institutions est soumis au contrôle de la conformité avec, notamment, les traités, les principes généraux du droit ainsi que les droits fondamentaux (…). Les décisions de la Commission (…) ne sauraient donc échapper à un tel contrôle*. ». La Cour a également reconnu que « *le niveau de protection assuré par un pays tiers est susceptible d'évoluer.* ». Dès lors, « *il incombe à la Commission (…) de vérifier de manière périodique si la constatation relative au niveau de protection adéquat assuré par le pays tiers en cause est toujours justifié en fait et en droit.* ». Et la Cour d'ajouter qu'une « telle vérification s'impose, en tout état de cause, lorsque des indices font naître un doute à cet égard. »[10].

A la suite de cette décision, les transferts de données vers les Etats-Unis ne sont plus considérés comme réalisés vers un pays offrant une « *protection adéquate des données personnelles* ». Les entreprises seraient ainsi dans l'obligation de procéder à des demandes d'autorisation auprès de la CNIL[11]. Toutefois, la demande risque d'être forte. Restent les clauses contractuelles types[12], ce qui impliquerait une renégociation des contrats en cours. Pour un même groupe, en cas de transfert de données entre les filiales, les Binding Corporate Rules[13] peuvent être mises en œuvre.

Le Groupe de l'article 29 s'est réuni le 15 octobre afin de tirer les conséquences de l'arrêt rendu par la Cour de justice de l'Union européenne le 6 octobre dernier invalidant la décision de la Commission européenne instaurant la sphère de sécurité. Les institutions européennes et les autorités américaines sont invitées à trouver des solutions avant la fin du mois de janvier 2016. A défaut, les autorités de protection pourraient procéder à des actions répressives coordonnées[14].

En dernier lieu, il n'est pas exclu que la CNIL préfère l'option de l'autorisation unique[15]. En effet, certains fichiers ou traitements de données personnelles sensibles ou à risques, qui visent une même finalité et des catégories de données et de destinataires identiques, sont autorisés par la CNIL au travers de décisions-cadre, appelées autorisations uniques. Si un traitement est conforme à l'une de ces autorisations, l'organisme peut effectuer une déclaration de conformité.

B. La sécurité des objets connectés et des données collectées

Les objets connectés tendent à devenir, s'ils ne le sont pas déjà, des objets du quotidien alimentés par les données des utilisateurs. Qu'il s'agisse d'une montre connectée ou d'un dispositif domotique, le défaut de sécurité des objets connectés est, par suite, susceptible d'avoir une forte répercussion sur la vie privée des personnes.

[9] http://www.cnil.fr/linstitution/actualite/article/article/invalidation-du-safe-harbor-par-la-cour-de-justice-de-lunion-europeenne-une-decision-cl/
[10] http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117fr.pdf
[11] http://www.cnil.fr/vos-obligations/declarer-a-la-cnil/mode-demploi/comment-declarer/la-demande-dautorisation/
[12] http://www.cnil.fr/vos-obligations/transfert-de-donnees-hors-ue/contrats-types-de-la-commission-europeenne/
[13] http://www.cnil.fr/vos-obligations/transfert-de-donnees-hors-ue/les-bcr/
[14] http://www.avocats-mathias.com/donnees-personnelles/safe-harbor-g29
[15] http://www.cnil.fr/documentation/deliberations/autorisations-uniques/

Des exemples de détournement d'objets connectés sont déjà recensés. La société californienne Proofpoint[16] annonçait déjà en 2014 avoir découvert que des tiers étaient parvenus à pénétrer les systèmes d'information de divers objets connectés au sein du domicile de personnes, tels que des télévisions connectées, des consoles de jeux vidéo, et un réfrigérateur. Plus de 750.000 courriers électroniques malicieux avaient été envoyés, entre le 23 décembre et le 6 janvier, essentiellement à des entreprises et des individus à travers le monde[17].

On peut également citer le cas de l'ampoule Lifx connectée au réseau wi-fi du bureau ou du domicile et contrôlée grâce à un smartphone. Elle peut notamment être allumée ou éteinte à distance, ses couleurs peuvent varier au rythme de la musique ou simplement par l'intermédiaire d'une application installée sur le téléphone. En 2014, en raison d'une faille de sécurité corrigée depuis, il était possible, en étant à moins de 30 mètres d'une ampoule, d'intercepter les identifiants au réseau wi-fi[18].

L'avis du Groupe de l'article 29 du 16 septembre 2014 souligne que sécuriser les objets n'est pas suffisant puisque les données sont susceptibles d'être communiquées par des tiers. La sécurité des infrastructures de stockage des données et les réseaux de communications doit également être assurée.

Pour rappel, le responsable du traitement doit, en effet, prendre toutes les mesures « *au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.* » en vertu de l'article 34 de la loi du 6 janvier 1978 modifiée. En cas de manquement, le responsable de traitement risque notamment une sanction financière pouvant aller jusqu'à 150 000€. Si ces sanctions sont bien souvent jugées peu dissuasives, il ne faut pas oublier qu'une publication de la sanction porterait atteinte à l'image de l'entreprise ou de l'administration. Par ailleurs, des sanctions pénales sont également encourues[19].

De plus, en cas de recours à la sous-traitance, un audit de sécurité devra être effectué préalablement et au cours de la relation de sous-traitance. Il conviendra également que le responsable de traitement soit vigilent si le sous-traitant fait lui-même appel à un prestataire secondaire. Pour rappel, dans le cadre de la fuite de données à laquelle un opérateur de téléphonie historique a été confronté, la Cnil avait mis en avant le défaut d'audit de sécurité auprès du prestataire secondaire[20].

Toutes ces questions démontrent l'intérêt à porter aux différents contrats et l'importance d'être accompagné par des professionnels du droit spécialisés en droit des données à caractère personnel.

[16] http://investors.proofpoint.com/releasedetail.cfm?releaseid=819799
[17] http://www.economist.com/news/science-and-technology/21594955-when-internet-things-misbehaves-spam-fridge
[18] http://thehackernews.com/2014/07/smart-led-lightbulbs-can-be-hacked-too.html
[19] Article 226-17 du Code pénal « Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. ».
[20] Délibération de la formation restreinte n°2014-298 du 7 août 2014 prononçant un avertissement à l'encontre de la société ORANGE.

C. Penser la conformité en amont

En ce qui concerne la protection des données à caractère personnel, trois grands principes sont désormais bien souvent mis en avant et sont repris dans la proposition de règlement européen sur les données.

Tout d'abord, le principe de responsabilité, plus connu sous son appellation anglophone « *accountability* ». Celui-ci « *consiste en l'obligation pour le RSSI de prouver aux autorités de contrôle chargées de la protection des données personnelles ou encore aux personnes concernées par les traitements que son entreprise respecte la législation en vigueur. Il s'agit donc d'assurer une traçabilité et une transparence au sein de l'entreprise. Le RSSI devra ainsi adopter des règles internes et mettre en œuvre les mesures appropriées pour garantir que le traitement des données à caractère personnel est effectué dans le respect du règlement*[21] ».

Le principe de « *privacy by design* » permet d'assurer la conformité à la législation en la matière de protection des données dès la création d'une société, ou de tout service interne à celle-ci ou bien encore de tout service ou produit, ayant rapport avec le traitement des données. Ce concept a pour particularité de s'effectuer *a priori*, soit au moment même de la conception des technologies, des infrastructures et des pratiques de la société.

Il est en effet conseillé aux entreprises qui fabriquent des objets connectés et les distribuent de mettre en œuvre des éléments de sécurité raisonnable dans leurs produits et ce, de manière anticipée. Bien entendu, pour déterminer ce niveau de sécurité raisonnable, plusieurs critères seront pris en compte, parmi lesquels le volume et le caractère sensible des données collectées ainsi que les coûts prévisionnels des indemnités à verser en cas de failles de sécurité.

C'est pourquoi les entreprises sont encouragées à « penser » la sécurité dès la conception du produit et non après son lancement. En application du principe de « *privacy by design* », les entreprises devraient :

- ✓ Mettre en place des mesures de gestion des risques liés aux atteintes à la vie privée de leur clientèle et à la sécurité de leurs produits ;
- ✓ Réduire le volume des données qu'elles collectent et conservent ;
- ✓ Tester leurs mesures de sécurité avant de lancer leurs produits.

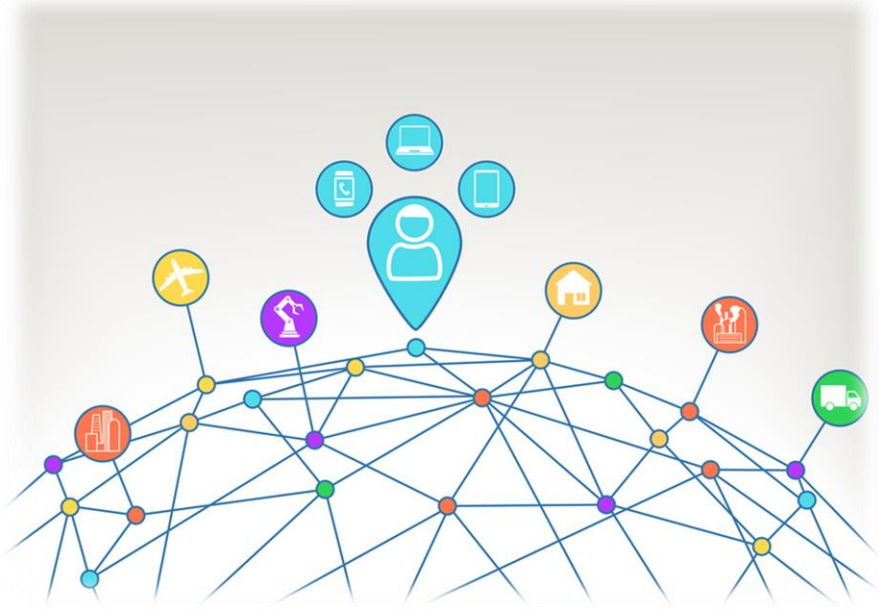
Par ailleurs, dans le respect des politiques internes, il est pertinent de prévoir une sensibilisation des salariés aux bonnes pratiques en matière de sécurité de l'information et de s'assurer que les enjeux de sécurité sont traités dans les sphères de responsabilité appropriées au sein de la structure.

En outre, les entreprises ne devraient retenir que des cocontractants (sous-traitants, fournisseurs, prestataires, partenaires, etc.) capables de maintenir un niveau raisonnable de sécurité. Il est nécessaire de rappeler que les contrats signés entre les entreprises et leurs cocontractants doivent prévoir des mécanismes de surveillance et de transparence concrets et suffisants.

De même, lorsque les entreprises repèrent des failles importantes dans leurs solutions, elles doivent immédiatement mettre en place des mesures de sécurité, à différents niveaux et en profondeur.

[21] Garance Mathias, Solutions IT N°1 en Juin 2014.

Enfin, il est essentiel que les entreprises mettent en œuvre des mesures de contrôle pour limiter l'accès aux données à caractère personnel d'un utilisateur.



Quant au principe de « *privacy by default* », il est très proche du « *privacy by design* » mais se différencie par le fait qu'il laisse une marge de manœuvre à l'utilisateur. Le « *privacy by default* » est tout particulièrement intéressant dans le cadre de l'utilisation d'objets connectés et du développement des applications. Les paramètres par défaut font donc en sorte que la plus grande protection des données possible soit garantie. Il reviendra alors à l'utilisateur de modifier les paramètres s'il le souhaite. Cela peut être le cas en matière de localisation par exemple mais il faudra alors veiller à ce qu'il y ait une notification sur les dangers liés à ces changements.

Des bonnes pratiques devront donc être mises en place, la rédaction de certains écrit devra être assurée, notamment au niveau interne de l'entreprise ou de l'administration (politiques de respect de la vie privée, politiques contractuelles avec les sous-traitants, principe du besoin d'en connaître, etc.). Par ailleurs, pour l'*accountability,* le RSSI devra veiller à faire réaliser une analyse d'impact relative à la protection des données préalablement à la mise en œuvre de traitements à risque, comme prévu par l'article 33 du projet de Règlement. Il devra également s'assurer de l'acceptation expresse, en toute conscience, du risque résiduel par ses supérieurs hiérarchique.

IV. Conclusion

Que retenir des problématiques énoncées ? Il faudra que les entreprises qui se lancent dans l'aventure des objets connectés, s'assurent de la conformité de leurs procédures, de leurs règlements et de leurs contrats avec la législation en vigueur (notamment leurs conditions générales d'utilisation). Ces précautions sont nécessaires en cas de contentieux mais également pour s'assurer de la protection des données des utilisateurs, le respect du droit à la vie privée étant une liberté fondamentale.

Les objets connectés constituent un véritable défi pour les entreprises, administrations ainsi que pour les particuliers (bien que pas forcément conscients) qui seront plus ou moins attachés à leur utilisation. Afin d'éviter les abus et protéger au mieux les utilisateurs de l'Internet des Objets, certains travaux législatifs sont en négociations. Nous avons déjà pu les évoquer plus haut, il s'agit de travaux à la fois au niveau européen, mais également au niveau national.

Les enjeux juridiques des objets connectés vont bien au-delà de la problématique des données à caractère personnel. Vous aurez l'occasion de nous lire à ce sujet dans la deuxième partie de ce Livre Blanc, à paraître prochainement.