TRAVAUX PRATIQUES

Après avoir lu l'article de l'usine digitale, **vous ferez la synthèse** de celui-ci, **en faisant ressortir les traitements sur les données à caractère personnel**

Source : https://www.usine-digitale.fr/article/la-protection-des-donnees-personnelles-face-aux-objets-connectes.N1087044

La protection des données personnelles face aux objets connectés

TRIBUNE La protection des données personnelles est primordiale pour garantir une adoption saine et pérenne des objets connectés par la société. Cette tribune de Me Isabelle Cantero et Me Eric A. Caprioli de la société d'avocats Caprioli & Associés étudie cette question sous son angle juridique.

PUBLIÉ LE 27 AVRIL 2021 À 09H30

LES EXPERTS DU NUMÉRIQUE, OBJETS CONNECTÉS, DONNÉES PERSONNELLES

TWITTERFACEBOOKLINKEDINFLIPBOARDEMAIL

La protection des données personnelles face aux objets connectés© jeferrb/Pixabay

Dans leur rapport sur les objets connectés, l'Institut de la souveraineté numérique et l'AFNIC soulignent "qu'*à mesure que ces technologies se diffuseront […], la protection des données issues des objets connectés deviendra un élément clé pour leur acceptabilité et constituera un facteur de différenciation et de confiance pour les technologies européennes*" (ISN et AFNIC, *Rapport Internet des Objets & Souveraineté Numérique*, 2021). Autrement dit, la protection des données personnelles est primordiale pour pérenniser le développement des objets connectés.

APPLICATION DU DROIT COMMUN DES DONNÉES PERSONNELLES

L'objet connecté est défini par la Commission d'enrichissement de la langue française comme un : *"objet qui est capable, outre sa fonction principale, d'envoyer ou de recevoir des informations par l'intermédiaire d'un réseau de télécommunication*". Il s'agit donc d'une nouvelle itération du réseau qui d'un point de vue juridique n'est pas réellement innovante. En effet, on applique le droit positif (en particulier, le RGPD et la Loi Informatique et Libertés modifiée) à l'objet connecté en fonction du traitement de données personnelles réalisé.

Ainsi, le professionnel détermine la finalité, la base légale (contrat, consentement, …), la durée de conservation, informe les personnes de leurs droits… sur le traitement de données. Concernant la base légale, on peut opter pour le contrat sous réserve que le traitement soit objectivement nécessaire à l'exécution de ce contrat. Lorsque le consentement est retenu comme base légale, il faut s'interroger sur

la formalisation du consentement liée à l'achat d'un simple objet dont la destination première n'est pas le recueil de données. Une difficulté pratique réside dans la pluralité de traitements que le produit est susceptible d'effectuer et donc dans l'encadrement juridique adéquat de cet ensemble.

De son côté, l'utilisateur peut faire valoir ses droits sur les données personnelles collectées. La démarche, lorsqu'elle est effectuée en ligne, est, par principe, encadrée par des conditions générales d'utilisation (CGU). Toutefois, ces CGU, parfois incompréhensibles ou peu accessibles pour les utilisateurs ne remplissent pas, pour certaines, les obligations d'information requises au titre de la protection des données personnelles.

Enfin, sans entrer dans les détails de la relation responsable de traitement / sous-traitance, on rappellera que le RGPD soumet cette relation à un certain nombre de nouvelles obligations. Ces obligations sont matérialisées par des engagements contractuels adaptés, notamment dans un contexte particulier post *Privacy Shield* pour les sociétés américaines.

OBJETS CONNECTÉS ET BIG DATA

En considérant les objets connectés comme des points d'entrée pour la collecte de données, on se retrouve avec des produits qui alimentent quotidiennement et de façon exponentielle le Big Data. Sur ce point, le CEPD a souligné "*qu'avec le nombre toujours croissant de capteurs déployés dans les véhicules connectés, il existe un risque très élevé de collecte excessive de données par rapport à ce qui est nécessaire pour atteindre l'objectif*" (CEPD, *Le*

traitement de données personnelles dans le contexte des véhicules connectés et des applications relatives à la mobilité, 2020).

Le sujet des objets connectés est donc étroitement imbriqué avec celui du Big Data. Ceci peut obliger les acteurs du marché des objets connectés de réaliser une analyse d'impact (AIPD) afin de prévenir et d'anticiper les risques juridiques et de conformité. En effet, l'AIPD est requise lorsqu'un traitement remplit au moins deux critères parmi une liste définie. Le critère "usage innovant" étant aisément rempli pour ce type de produit, reste le critère "collecte à large échelle" qui peut renvoyer au Big Data suivant les fonctionnalités des objets connectés.

Pour les objets connectés, comme pour le Big data, il s'agit de mettre en œuvre le principe d'*accountability*. Cela se traduit par un ensemble documentaire qui permet de déterminer les risques liés aux données personnelles traitées, d'élaborer une AIPD afin de prévoir les mesures techniques, organisationnelles et juridiques pour pallier les risques identifiés et d'en mesurer l'efficacité. L'*accountability* va de pair avec le principe de *privacy by design* qui vise la protection des données personnelles dès la conception des produits. En d'autres termes, il faut intégrer ce principe à tout moment du projet de l'objet connecté, du début à la fin, pour qu'il soit juridiquement viable.

SÉCURISATION DES DONNÉES PERSONNELLES

La sécurisation des données est l'autre facteur influençant la confiance des utilisateurs qu'ils soient particuliers ou professionnels. En effet, les acquéreurs d'objets connectés, bien que méfiants

quant à l'utilisation de leurs données par l'opérateur à qui ils permettent la collecte, le sont encore plus vis à vis des tiers et plus particulièrement lorsqu'il s'agit du piratage. La sécurité s'aborde, au premier chef, au niveau de l'objet lui-même. On se souvient de l'avertissement de la CNIL sur une gamme de jouets connectés mal sécurisés (appairage sans authentification, écoute des conversations, etc.).

D'autre part, la sécurité concerne la conservation des données. On retrouve, en cet endroit, la problématique, plus générale, liée au Big Data et au Cloud (hébergement des données). L'obligation de sécurité concernant les données à caractère personnel est prévue à l'article 32 du RGPD ; tout manquement étant passible de sanctions administratives dont une amende de 10.000.000 euros ou de 2% du CA mondial, conformément à l'article 83-4 du RGPD et/ou des sanctions pénales visées aux articles 226-16 à 226-24 du Code pénal. Au niveau du règlement européen, elle se traduit par une obligation de notification, pour les cas de violation des données, à l'autorité de contrôle ainsi qu'aux personnes concernées le cas échéant. À cet égard, le responsable de traitement peut s'inspirer des lignes directrices 01/2021 du CEPD qui envisagent différentes situations pratiques pour lesquelles cette notification est nécessaire.

Des objets connectés oui, mais sécurisés aux niveaux juridique et technique !

Eric A. Caprioli & Isabelle Cantero, avocats associés
Caprioli & Associés, société d'avocats membre du réseau JuriDefis