

## Protection des données à caractère personnel et voiture connectée

Gaelle Kermorgant, ALFRATEC, [gmkmorgant@gmail.com](mailto:gmkmorgant@gmail.com)

Si les acteurs de l'écosystème de la voiture connectée<sup>1</sup> ne veulent pas connaître la même mésaventure que la société *Genesis Toys*<sup>2</sup> qui vient d'être attaquée pour non-respect de la vie privée et de la sécurité des données personnelles par le Bureau Européen des Unions de Consommateurs (BEUC) ainsi que d'autres organisations de consommateurs américaines<sup>3</sup> dans divers Etats dont la France, ils doivent impérativement s'interroger sur leur politique de protection des données personnelles des utilisateurs de leurs produits.

Ceci apparait d'autant plus important que l'association l'Automobile club a publié en 2015 une étude relative à la voiture connectée soulignant qu'en France « *les français redoutent la divulgation de données personnelles (85%) l'usage commercial de leurs données (84%) et le piratage (84%)* »<sup>4</sup>.

Pour faire face à ce défi, il importe de comprendre ce que recouvre la notion de données à caractère personnel (« DCP »), puis de s'interroger sur l'organisation et la gestion de ces données dans l'entreprise.

Rappelons qu'en vertu du droit applicable dans l'Union européenne (« UE ») - qui est l'objet de cet article -, toute donnée permettant, directement ou indirectement, d'identifier une personne est une DCP<sup>5</sup>. Par exemple, dans une voiture connectée, le numéro VIN ou le numéro IP d'un ordinateur embarqué, sont des DCP.

Dès lors qu'une donnée est qualifiée de DCP, toute une batterie de mesures s'impose au responsable du traitement. Celles-ci peuvent être plus ou moins contraignantes eu égard à la sensibilité des données collectées. Ainsi, parmi les DCP qui peuvent être collectées dans la voiture connectée, certaines peuvent révéler des infractions au code de la route. Il s'agit principalement des données de géolocalisation et de vitesse. Or, en vertu de l'article 9 de la loi 1978, le traitement de DCP relatives aux infractions ne peut être mis en œuvre que par certaines personnes nommément désignées<sup>6</sup>. Dès lors, la collecte de ces données impose la mise en place de mesures de confidentialité et de sécurité accrues.

Une fois les DCP identifiées une recherche des risques rencontrés dans la gestion de ces DCP – ce que l'on appelle une analyse d'impact - s'impose pour identifier les solutions à adopter pour respecter la loi. Soulignons du reste que celle-ci sera obligatoire à compter du 25 mai 2018, dès lors que les technologies mises en œuvre présentent un risque pour le respect de la vie privée des personnes concernées<sup>7</sup>.

---

<sup>1</sup> Il s'agit notamment des constructeurs d'automobiles mais également des fournisseurs d'accès à internet, des fournisseurs de services liés au véhicule comme les assureurs et les réparateurs.

<sup>2</sup> Cette société vend notamment les deux jouets connectés *Mon amie Cayla* et le *robot i-Que*.

<sup>3</sup> <http://www.beuc.eu/press-media/news-events/eu-us-consumer-take-action-against-flawed-connected-toys>

<sup>4</sup> [http://mycarmydata.fr/wp-content/themes/shalashaska/assets/docs/sondage\\_min.pdf](http://mycarmydata.fr/wp-content/themes/shalashaska/assets/docs/sondage_min.pdf)

<sup>5</sup> Règlement (UE) 2016/679 du Parlement européen et du Conseil 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, et abrogeant la directive 95/46/CE, Article 4.

<sup>6</sup> Ceci est du reste rappelé également à l'Article 10 du Règlement (UE) 2016/679.

<sup>7</sup> Op.cit., Règlement (UE) 2016/679, section 3.

Lorsque cette analyse d'impact a été opérée, et conformément au principe de « *privacy by design* »<sup>8</sup>, chacun devra s'assurer que préalablement à la collecte de DCP, sont implémentées les mesures organisationnelles et techniques appropriées au traitement et aux objectifs du traitement.

Dans cette optique, l'entreprise devra faire sienne un certain nombre de principes. Parmi eux se trouvent notamment ceux énumérés ci-après, dont nous illustrerons la mise en œuvre en nous fondant sur le Règlement (UE) 2015/758 qui organise le déploiement du système eCall dans l'UE.

- Le principe de limitation des finalités :

Les motifs de la collecte de DCP doivent être légitimes et indiquées de manière claire. De plus, une fois énoncées, ces finalités ne peuvent être modifiées sans respecter certaines règles, sous peine de violer le principe de licéité du traitement. Les données collectées ne peuvent être réutilisées pour une autre finalité que celle à laquelle l'utilisateur a consenti ou que celle définie par la loi<sup>9</sup>.

A titre d'illustration, le système eCall se présente clairement comme un instrument prévu pour uniquement réduire le nombre d'accidents mortels ainsi que la gravité des blessures provoquées par les accidents de la route, grâce à l'alerte précoce des services d'urgence<sup>10</sup>. Par ailleurs, l'article 6-3 du Règlement 2015/758 précise que les données collectées pour l'exécution du service eCall ne peuvent être transmises à d'autres fins. Par conséquent, ni le prestataire du *TPS eCall*<sup>11</sup>, ni le prestataire de services tiers, ni les opérateurs de télécommunication ne pourront stocker des données collectées dans le cadre de l'activation d'un appel d'urgence pour s'en servir, par exemple, dans le cadre d'un procès après un accident. Néanmoins, comme le note la parlementaire Sophia In't Veld "*In practice, abuse always occurred and gradually data would be used for new purposes. Insurance companies, personal injury lawyers, police, intelligence services would no doubt find the data very useful*"<sup>12</sup>.

- Le principe de minimisation des données :

Les DCP collectées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées<sup>13</sup>.

Si nous reprenons l'exemple du dispositif eCall, le nombre des informations collectées pour l'exécution du système a été strictement défini par le Comité européen de normalisation<sup>14</sup>. Les

---

<sup>8</sup> Op.cit., Règlement (UE) 2016/679, Article 25.

<sup>9</sup> Directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, Article 9.

<sup>10</sup> Règlement (UE) 2015/758 concernant les exigences en matière de réception par type pour le déploiement du système eCall embarqué fondé sur le service 112 et modifiant la directive 2007/46/CE, considérant 7.

<sup>11</sup> Op. cit, Règlement (UE) 2015/758, Article 3-10 : « *«eCall pris en charge par des services tiers» ou «TPS eCall», un appel d'urgence en provenance d'un véhicule vers un prestataire de services tiers, effectué soit automatiquement par l'activation de détecteurs embarqués, soit manuellement, qui transmet le MSD et établit une communication audio entre le véhicule et le prestataire de services tiers grâce à des réseaux publics de communications sans fil; »*

<sup>12</sup> Debate on the EU Parliament the 25th February 2014, « Deployment of the eCall in-vehicle system – Deployment of the interoperable EU-wide eCall

<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20140225+ITEM-013+DOC+XML+V0//EN&language=EN>

<sup>13</sup> Loi 78-17 relative à l'informatique, aux fichiers et aux libertés 1978, Article 6.

<sup>14</sup> CEN EN 15722 'Road transport and traffic telematics – Esafety – eCall minimum set of data'.

données qui sont communiquées au Centre de réception des appels d'urgence (« PSAP ») sont d'une part, les données dites obligatoires visant l'identification de l'appel (afin de le distinguer d'un appel depuis un téléphone portable), la géolocalisation du véhicule, la direction du voyage, l'heure de l'accident et si l'appel a été activé manuellement ou automatiquement. D'autre part, s'y ajoutent des données optionnelles que sont l'identification du véhicule, son type de motorisation et son carburant et le nombre de passagers avec une ceinture de sécurité attachée.

- Le principe de limitation de la conservation des DCP :

La durée de conservation ne doit pas excéder celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

Ainsi il est indiqué que les données enregistrées pour l'exécution du dispositif eCall ne peuvent être conservées plus longtemps que nécessaire à leur transmission aux secours d'urgence : les données collectées doivent être « *automatiquement et constamment effacées* »<sup>15</sup>. Néanmoins, conformément au principe de proportionnalité<sup>16</sup> et en vue d'assurer la finalité de la collecte des données de géolocalisation, il a été décidé également que les données communiquées au PSAP dans ce domaine se limiteraient à ne retenir que les trois dernières positions du véhicule émetteur de l'appel afin de le localiser précisément<sup>17</sup>.

- Le principe de sécurité des données :

Ce principe vise avant tout à prévenir tout acte malveillant.

En ce qui concerne le dispositif eCall, le Règlement 2015/758 exige que le véhicule ne puisse être constamment traçable. En effet, la communication avec le réseau de télécommunication ne se produit que lorsque le système est activé<sup>18</sup>. De plus, est requis que « *Les technologies renforçant la protection de la vie privée (soient) intégrées dans le système eCall embarqué fondé sur le numéro 112 afin d'offrir aux utilisateurs le niveau de protection de la vie privée approprié, ainsi que les garanties nécessaires pour prévenir la surveillance et les utilisations abusives* »<sup>19</sup>.

- Le principe de licéité du traitement :

La collecte et le traitement de DCP ne peuvent avoir lieu que sous certaines réserves qui sont dans la plupart des cas le consentement de la personne concernée. Dans cette situation, la personne concernée doit pouvoir refuser la collecte/le traitement de ces DCP.

L'autorisation du traitement des données peut aussi ne pas être le consentement de l'intéressé mais la conséquence d'une loi<sup>20</sup>.

- Le droit à l'information de l'intéressé. Soulignons que ce droit sera considérablement renforcé à compter de mai 2018 avec l'application du Règlement 2016/679<sup>21</sup>.

Cette liste non exhaustive de principes, doit être prise en compte dès la conception de la voiture connectée. A compter du 25 mai 2016, leur non-respect pourra coûter une amende pouvant

<sup>15</sup> Op.cit., Règlement (UE) 2015/758, Article 6-5.

<sup>16</sup> Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, article 6-1-c.

<sup>17</sup> Op.cit., Règlement (UE) 2015/758, Article 6-5.

<sup>18</sup> Ibid, Considérant 21 et Articles 6-4 et 6-9-g.

Voir notamment : <https://ec.europa.eu/digital-single-market/en/news/ecall-%E2%80%93-do-you-have-any-concerns-your-privacy-you-shouldnt...>

<sup>19</sup> Op. cit., Règlement (UE) 2015/758, Article 6-7.

<sup>20</sup> Exemple : le système eCall est obligatoire à compter du 31 mars 2018.

<sup>21</sup> Voir notamment son article 12.

atteindre la somme la plus élevée entre 20 millions d'euros et 4% du chiffre d'affaires total annuel<sup>22</sup>.

Ces quelques principes contraignants soulignent combien l'approche européenne est très protectrice de la vie privée. Nous pouvons donc nous demander si elle n'est pas de nature à retarder l'arrivée de nouveaux produits en limitant l'accès et le traitement de DCP<sup>23</sup>.

Selon Sophie Nerbonne, directrice de la direction de la conformité de la CNIL, si les utilisateurs comprennent que leurs données sont protégées lorsque les produits/services sont conformes à la loi européenne, ils auront confiance dans l'utilisation de ces dits produits/services et seront donc plus enclin à les acheter. Le respect de la loi européenne devrait donc être compris comme un instrument commercial.

Pour conforter cette position et lutter contre la distorsion de concurrence est affirmée l'application du droit européen dès lors qu'il y a traitement de données personnelles dans le cadre des activités d'un établissement situé sur le territoire de l'Union ou faisant usage d'un équipement situé sur le territoire d'un Etat membre<sup>24</sup> ou, à compter de mai 2018, offrant des « biens ou des services aux personnes concernées dans l'UE », ou contrôlant un comportement de ces personnes qui se déroule dans l'UE<sup>25</sup>. Cet effet extraterritorial affirmé pose la question de son efficacité. Comme souligné par Cedric Ryngaert « *where data controllers have no establishment or assets in, or other links with the EU, such enforcement is difficult* »<sup>26</sup>. De plus, certaines autorités de contrôle ont peu de moyens humains et financiers pour effectuer les vérifications adéquates.

Ceci soulève la question de la mobilité de la voiture connectée et encore plus de celle des données. En vertu de la loi européenne, une information de l'utilisateur est requise avant tout traitement de données personnelles. Or, force est de constater que ni lors de l'achat ni lors de la location d'une voiture connectée, l'utilisateur est alerté sur les modalités du traitement de ses données personnelles dès qu'il franchit une frontière. Il pourrait donc être utile qu'une norme soit adoptée afin que la voiture puisse informer son conducteur de la loi applicable dès le franchissement d'une frontière. L'utilisateur devrait alors pouvoir interroger la voiture pour connaître les règles en matière de traitement de ses données personnelles. Cette mesure ne fait pas obstacle à la nécessité d'informer également les utilisateurs dans le contrat, mais eu égard au nombre d'informations communiquées à l'utilisateur au moment de contracter, il semble que les développements technologiques pourraient utilement soutenir la règle juridique d'information préalable de la personne concernée.

En raison du caractère mobile des voitures connectées et des données mais également pour la favoriser la compétitivité des produits/services proposés sur le sol européen, il apparaît que le challenge des prochaines années se déplacera vers la scène internationale. Il faudra sans doute

---

<sup>22</sup> Op.cit., Règlement (UE) 2016/679, Article 83.

<sup>23</sup> C'est du reste ce qu'a semblé dire Angela Merkel en novembre 2016 lors du sommet sur les techniques de l'information qui s'est tenu à Saarbrücken ; Voir : <http://www.dw.com/en/merkel-calls-for-loosening-of-restrictive-german-data-protection-laws/a-36431222>

<sup>24</sup> Op.cit., Directive 95/46/EC, Article 4-1-a and 4-1-c.

<sup>25</sup> Op.cit., Règlement (UE) 2016/679, Article 3-2.

<sup>26</sup> Cedric Ryngaert Symposium issue on extraterritoriality and EU data protection, International Data Privacy Law, 2015, vol(5), n°4, page 223.

du temps et des efforts pour trouver un compromis quant à la portée du concept de protection de la vie privée et aux moyens de le protéger au niveau international. Néanmoins, cela semble le prix à payer pour que les développements des voitures connectées soient un succès et apportent innovation en Europe.

## **Gaëlle KERMORGANT**

Après des études à Aix-en-Provence, Rennes, Paris et Edimbourg, Gaëlle a acquis pendant près de vingt années son expérience comme juriste dans les secteurs de la chimie, de l'assurance et en relation avec les institutions européennes.



Titulaire d'un CAPA (certificat d'aptitude à la profession d'avocat) et de trois masters en droits (LLM), elle a une grande expérience en matière de droit de la concurrence, des contrats, de la consommation et de la distribution. Elle a également développé des compétences juridiques en technologies de l'information, en propriété intellectuelle et dans le domaine de l'intelligence artificielle et des véhicules autonomes/connectés.

Gaëlle a déjà communiqué à plusieurs reprises sur les thèmes de la voiture autonome en Allemagne et en France (CESA 2014, Paris ; AMAA 2015, Berlin).

Gaëlle est aujourd'hui membre de l'association du droit des robots, collaboratrice d'une PME de consulting, ALFRATEC et ouvrira dans les prochaines semaines son cabinet d'avocat.