

## Bref aperçu de la jurisprudence récente en matière de protection des données

*Sébastien Fanti*

- A. Prolégomènes
- B. Arrêt du Tribunal fédéral du 8 septembre 2010 (ATF 136 II 508) dans l'affaire Logistep (surveillance d'internet par des sociétés privées)
- C. Arrêt du Tribunal fédéral du 8 septembre 2010 (ATF 136 II 508) dans l'affaire Logistep: la première audience judiciaire suisse twittée!
- D. Arrêt du Tribunal administratif fédéral (TAF) du 30 mars 2011 (A-7040/2009) dans l'affaire Google Streetview
- E. Délibération n° 2011-035 de la formation restreinte de la CNIL prononçant une sanction pécuniaire à l'encontre de la société Google Inc.
- F. Décision du 17 février 2011 de la commission cantonale de protection des données du Canton du Jura (tenue d'un fichier informatisé des automobilistes avertis par la police cantonale)
- G. Résumés d'arrêts divers du Tribunal fédéral
- H. Conclusions

### A. Prolégomènes

Les derniers développements jurisprudentiels survenus dans notre pays depuis l'année dernière auraient très certainement ravi Gérard Haas.<sup>1</sup> Les décisions intéressantes se succèdent à un rythme soutenu et engendrent des débats passionnés (inconnus jusqu'alors) et des guerres de procédure picrocholines. La protection des données devient un thème central en matière de nouvelles technologies, mais également dans tous les domaines de notre vie quotidienne et la prise de conscience des enjeux de la matière atteint désormais une rare acuité. Sauf, peut-être, chez les juristes. Peu conscients des bénéfices qui pourraient être retirés de procédures relativement simples à conduire sur le plan formel, ils négligent d'appréhender leurs dossiers à l'aune des nombreux droits octroyés tant par le droit fédéral que par les législations cantonales. Il n'est certes pas aisé de se baigner dans des eaux inconnues, qui peuvent s'avérer peu propices et anguleuses, dès lors que la technologie est souvent présente. Toutefois pour qui consacre ses énergies à appréhender la nomenclature de cette matière, les bonis sont multiples. C'est précisément le but de cette contribution, susciter l'envie d'en savoir plus.

---

<sup>1</sup> Pour qui „qui ne défend pas ses droits, mérite de les perdre“, *Gérard Haas/Marie-Pierre Fenoll*, Trousseau, Internet et la protection des données, Paris 2000.

## B. Arrêt du Tribunal fédéral du 8 septembre 2010 (ATF 136 II 508) dans l'affaire Logistep (surveillance d'internet par des sociétés privées)

Liminairement, il convient de préciser que cet arrêt est celui qui a suscité le plus grand nombre de commentaires de la doctrine dans le domaine de la protection des données.<sup>2</sup> Diverses questions de principe y ont été traitées et l'arrêt ne reflète que partiellement l'intensité des points de vue émis<sup>3</sup> lors des délibérations publiques par les Juges de la Ière Cour de droit public du Tribunal fédéral.

Dans la mesure où le soussigné a participé à la procédure comme mandataire et où son point de vue a déjà été exprimé y relativement,<sup>4</sup> aucun commentaire adventice ne sera émis.

Le 9 janvier 2008, le Préposé fédéral à la protection des données et à la transparence (abrégé ci-après le Préposé) a émis une recommandation<sup>5</sup> dans laquelle il sollicitait de la société Logistep SA que celle-ci mette fin à ses recherches dans les réseaux P2P (pair à pair), ce en raison, notamment, d'un défaut de base légale. Dite entreprise était mandatée par des titulaires de droit d'auteur pour rechercher dans les réseaux P2P les offres prétendument illicites de contenus protégés par le droit d'auteur, soit principalement des fichiers musicaux et vidéos.<sup>6</sup> Elle collectait les adresses IP<sup>7</sup> des utilisateurs des réseaux P2P proposant de tels contenus, puis les titulaires de droits d'auteur déposaient une plainte pénale aux fins d'obtenir l'identification

---

<sup>2</sup> À titre exemplatif et non exhaustif: *Lukas Bühlmann*, Logistep-Urteil: Bundesgericht qualifiziert IP-Adressen nicht grundsätzlich als Personendaten, Push-Service des arrêts, publié le 19 janvier 2011; *Andreas Glarner/Karin Rüfenacht*, (Pyrrhus-)sieg für den Datenschutz, Jusletter 20 décembre 2010; *David Rosenthal*, Wenn Datenschutz übertrieben wird oder: Hard cases make bad law, Jusletter 27 septembre 2010; *David Rosenthal*, „Logistep“: Offenbar ein Einzelfallentscheid, Digma 2011, 40–43; *Willi Egloff/Bertil Cottier*, Sammeln von IP-Adressen zwecks Bekämpfung von Urheberrechtsverletzungen gerechtfertigt, Medialex 2009, 143–149; *Lukas Morscher*, Aktuelle Entwicklungen im Technologie- und Kommunikationsrecht, ZBJV 2011, 177–211; *Philippe Meier*, Le droit de la protection des données, Berne 2011, 537.

<sup>3</sup> Un résumé de ces délibérations est disponible à cette adresse: <http://www3.unil.ch/wpmu/cinn/2010/11/proces-logistep-en-direct-du-tribunal-federal/>.

<sup>4</sup> *Sébastien Fanti*, Cybercriminalité, droit d'auteur et protection des données, Jusletter 31 mars 2008, 10 ss.

<sup>5</sup> Recommandation qui peut être consultée à cette adresse: [http://www.edoeb.admin.ch/dokumentation/00445/00508/index.html?lang=de&download=NHZLpZeg7t,lnp6I0NTU04212Z6ln1acy4Zn4Z2qZpnO2YUq2Z6gpJCDdX13fmym162epYbg2c\\_JjKbNoKSn6A](http://www.edoeb.admin.ch/dokumentation/00445/00508/index.html?lang=de&download=NHZLpZeg7t,lnp6I0NTU04212Z6ln1acy4Zn4Z2qZpnO2YUq2Z6gpJCDdX13fmym162epYbg2c_JjKbNoKSn6A).

<sup>6</sup> Même si le Préposé ne l'évoque pas dans sa recommandation, la société Logistep s'est principalement fait connaître en détectant les téléchargements illicites d'un jeu, cf. à cet égard l'Ordonnance de référé du 24 décembre 2007 du Tribunal de grande instance de Paris: [http://www.legalis.net/spip.php?page=jurisprudence-decision&id\\_article=2172](http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2172).

<sup>7</sup> L'adresse IP est un numéro qui permet d'établir la correspondance entre l'identifiant attribué lors de la connexion et l'identité de l'internaute.

des auteurs potentiels. Une action civile en dommages et intérêts concluait le processus judiciaire.

De l'avis du Préposé, cette pratique constituait une violation du secret des télécommunications,<sup>8</sup> dont le caractère est absolu en matière de droit privé. En agissant de la sorte, la société Logistep SA commettait un abus de droit, car elle usait de la procédure pénale dans le but de contourner le caractère absolu du secret en matière de droit privé. De surcroît, le traitement de données était opéré de manière totalement opaque pour les personnes concernées, dont les fournisseurs d'accès, ce qui est contraire à la loi. Diverses autorités de protection des données ou tribunaux ont émis des recommandations, respectivement des décisions similaires, ce qui démontre que si la problématique est commune, les réponses légales diffèrent. À titre exemplatif et non exhaustif:

- la décision du 28 février 2008 de la *Garante per la Protezione dei Dati Personali* (Autorité italienne chargée de la protection des données à caractère personnel);<sup>9</sup>
- la décision du Tribunal ordinaire de Rome (9ème section civile spécialisée en matière de propriété industrielle et intellectuelle) du 14 juillet 2007;<sup>10</sup>
- la décision du Landgericht de Bochum du 22 avril 2008;<sup>11</sup>
- la décision de l'Oberlandesgericht de Hamburg du 3 novembre 2010;<sup>12</sup>
- l'Ordonnance rendue le 25 juin 2007 par le Tribunal de grande instance de Paris;<sup>13</sup>
- l'Ordonnance de référé du 24 décembre 2007 du Tribunal de grande instance de Paris.<sup>14</sup>

La société Logistep SA ayant refusé de déférer à la recommandation du Préposé, le Tribunal administratif fédéral a été saisi le 13 mai 2008.<sup>15</sup> La plainte du Préposé a été rejetée par jugement du 27 mai 2009.<sup>16</sup> Le TAF a certes considéré que les adresses IP constituaient des

---

<sup>8</sup> Le secret des télécommunications est garanti par l'article 13 de la Constitution (ATF 126 I 50, consid. 6a; RVJ 2006, 327).

<sup>9</sup> Pour une analyse en français de cette décision par M. Amedeo Arena de l'Université de Naples: <http://merlin.obs.coe.int/iris/2008/7/article26.fr.html>.

<sup>10</sup> Disponible à cette adresse: [http://www.altroconsumo.it/20070724/1-ordinanza-del-tribunale-di-roma-Attach\\_s173003.pdf](http://www.altroconsumo.it/20070724/1-ordinanza-del-tribunale-di-roma-Attach_s173003.pdf).

<sup>11</sup> Disponible à cette adresse: <http://www.hrr-straftrecht.de/hrr/lg/08/2-qs-10-08.php>.

<sup>12</sup> Disponible à cette adresse: <http://www.landesrecht.hamburg.de/jportal/portal/page/bshaprod.psml; jsessionid=D0EE59E4F4B727BF37EAB3766448FAB8.jpj4?showdoccase=1&doc.id=KORE564602010&st=ent>.

<sup>13</sup> Disponible à cette adresse: <http://static.pcinpact.com/decision.pdf>.

<sup>14</sup> Disponible à cette adresse: [http://www.legalis.net/spip.php?page=jurisprudence-decision&id\\_article=2172](http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2172).

<sup>15</sup> Conformément à l'article 29 al. 4 LPD.

<sup>16</sup> Cf. 16<sup>ème</sup> rapport d'activités du Préposé 2008/2009, ch. 1.3.1.

données personnelles<sup>17</sup> (ce qui est une première en Suisse) dont le traitement par Logistep SA contrevenait au principe d'un traitement des données reconnaissable et à celui de la finalité, mais il a conclu en estimant que l'intérêt des titulaires de droits d'auteur devait l'emporter sur l'intérêt des personnes concernées à la protection des données.<sup>18</sup> Le Préposé a recouru devant le Tribunal fédéral, ce qui a engendré le jugement dont il est aujourd'hui question. À ce stade de l'analyse, il convient de relever que près de 16 mois se sont écoulés entre la recommandation du Préposé (9 janvier 2008) et le prononcé du TAF (27 mai 2009), ce qui n'est pas admissible dans un domaine tel que celui de la protection des données, quelques clics s'avérant suffisants à transférer un fichier issu d'une collecte de données dans un autre hémisphère. Dans ces conditions se pose légitimement la question d'une règle de procédure imposant une décision dans un délai très bref, les mesures provisionnelles demeurant réservées.

Le Tribunal fédéral s'est prononcé dans cette affaire lors de délibérations publiques qui ont eu lieu le 8 septembre 2010 et ont suscité un grand intérêt également hors du cénacle juridique. *In limine litis*, il paraît opportun de relever que la décision a été prise à trois voix contre deux, ce qui témoigne dès lors, du fait que les opinions les plus diverses ont leur raison d'être, que le sujet est inédit et qu'il implique tous les principes fondamentaux du droit de la protection des données.

Comme à l'accoutumée, en cas de violation alléguée par le Préposé de la LPD, la stratégie de défense consiste à tenter, liminairement, de se soustraire à l'application de la loi. Le cas d'espèce ne fait pas exception à la règle, de sorte que le Tribunal fédéral a dû examiner si des données personnelles au sens de l'article 3 let. a LPD étaient récoltées par Logistep SA. Le Tribunal fédéral retient, à cet égard, qu'en cas de communication de données, il suffit que le destinataire soit en mesure d'identifier les personnes concernées (selon le texte légal qu'elles soient identifiées ou identifiables) pour que les données puissent être qualifiées de données personnelles (ce qui est en l'occurrence le cas) et que la LPD trouve application à l'intégralité du traitement de données. Relativement à la question de savoir si l'adresse IP est ou non une donnée personnelle, question résolue pour la première fois dans notre pays,<sup>19</sup> la Haute Cour émet l'avis suivant: il n'est pas possible de constater de manière abstraite si des adresses IP

---

<sup>17</sup> „IP-Adressen sind folglich entgegen der Ansicht der Beklagten als Personendate im Sinne des DSG anzusehen“; le TAF n'est toutefois pas d'avis qu'il s'agit de données sensibles au sens de l'article 3 let. c LPD.

<sup>18</sup> L'existence de faits justificatifs au sens de l'article 13 LPD a donc été retenue.

<sup>19</sup> Cf. à cet égard, *Claude Mouradian*, La position du Tribunal fédéral suisse sur le statut de l'adresse IP, *Juriscom.net*, publié le 24 février 2011: <http://www.juriscom.net/actu/visu.php?ID=1294>; cet article met en évidence les appréhensions différentes de cette question selon les pays.

(notamment les adresses IP dynamiques) sont ou non des données personnelles.<sup>20</sup> Chaque cas doit donc être analysé *in concreto* et pour lui-même. Les adresses IP doivent en toute hypothèse être considérées comme des données personnelles lorsqu'une forte probabilité d'identifier la personne en question existe. La structure de fonctionnement de la société Logistep SA reposait et avait pour but l'identification des personnes concernées, ce qui permet de conclure que les adresses IP récoltées sont des données personnelles protégées par la loi.

Le Tribunal fédéral a également considéré que l'activité déployée par la société Logistep SA comportait une atteinte importante à la sphère privée des utilisateurs concernés que l'État se devait de protéger.<sup>21</sup> La société Logistep SA ayant violé le principe de finalité (art. 4 al. 3 LPD) et l'exigence légale de reconnaissabilité (art. 4 al. 4 LPD), il convenait de déterminer si l'un des motifs justificatifs de l'article 13 LPD pouvait trouver application, qu'il s'agisse de dite société ou des détenteurs de droits d'auteur. Le Tribunal fédéral précise que si la justification du traitement de données personnelles en violation des principes figurant aux articles 4, 5 al. 1 et 7 al. 1 LPD ne peut certes être, de manière générale, exclue, les motifs justificatifs doivent être admis concrètement avec une grande réserve. Lors de cette analyse de l'existence de motifs justificatifs au sens de l'article 13 LPD, le fait que la recommandation du Préposé soit émise dans l'intérêt public (pour défendre un grand nombre de personnes) doit être pris en considération. Une telle recommandation produit, de surcroît, un effet indirect à l'égard de toutes les personnes qui procèdent selon la même méthode. L'intérêt d'une lutte efficace contre les violations des droits d'auteur ne permet pas, en l'espèce, de contrebalancer les atteintes à la personnalité et les incertitudes liées au procédé litigieux adopté s'agissant du traitement de données adopté. Il n'y donc pas de prépondérance d'intérêt (art. 13 al. 2 LPD) pour la société Logistep SA ou pour les détenteurs des droits d'auteur, ce qui conduit à nier l'existence de motifs justificatifs au traitement de données illicite.

Il convient également de relever, dans un but prospectif, que le Tribunal fédéral a évoqué les difficultés que le procédé utilisé pouvait générer du point de vue de la loi sur l'investigation secrète<sup>22</sup> et du principe de proportionnalité, sans examiner plus avant ces questions, en raison de la violation constatée de la LPD. Cette référence à la LFIS doit orienter la réflexion s'agissant de la légalité de preuves obtenues par des privés par „infiltration“ des réseaux sociaux

---

<sup>20</sup> Pour ceux qui auraient de la peine à appréhender les différentes formes d'adresses IP, voici un autre exemple tiré de la vie réelle: le pêcheur qui remonte ses filets ignore si ceux-ci recèlent des espèces protégées ou non; la pêche aux adresses IP est identique quant à son résultat.

<sup>21</sup> Pour la petite histoire, l'un des membres de la Cour a confié après l'issue des délibérations publiques avoir été influencé négativement par le fait que la société Logistep SA n'a pas autorisé les journalistes qui réalisaient un reportage sur l'activité litigieuse à accéder aux ordinateurs, respectivement à l'infrastructure technique et ce, même sans caméras. Le manque de transparence a donc joué un rôle important.

<sup>22</sup> LFIS (RS 312.8).

notamment.<sup>23</sup> Finalement, le Tribunal fédéral a expressément laissé en suspens la question de l'utilisation par les autorités de poursuite pénale des données recueillies par Logistep SA. Il faudra donc attendre une éventuelle procédure pour savoir si l'illicéité du traitement de données a eu pour conséquence la constatation de l'illicéité du moyen de preuve.

Et nunc, quid? Le Tribunal fédéral a clairement manifesté son insatisfaction relativement à la situation légale prévalant actuellement en matière de protection des droits d'auteur. Il ne s'agissait nullement, dans cette affaire, de donner précellence à la protection des données par rapport à la protection du droit d'auteur, mais d'appliquer le droit dans sa teneur actuelle. Le Tribunal fédéral a tenu à le signifier formellement pour éviter toute interprétation erronée ou orientée de sa décision. Dans son rapport d'activité 2010,<sup>24</sup> il a adressé une véritable invitation au législateur à prendre les mesures nécessaires afin de garantir une protection adéquate des droits d'auteur congruente aux technologies les plus récentes. A notre connaissance, le Parlement n'envisage pas, à ce jour, de modifier la loi fédérale sur le droit d'auteur.<sup>25</sup> Comme le relève avec pertinence la SUIISA dans son rapport annuel 2010,<sup>26</sup> il n'est donc *de facto* plus possible de prouver qu'une infraction au droit d'auteur a été commise sur Internet, et, *a fortiori* de demander réparation. L'issue de cette situation manichéenne pourrait intervenir si la Suisse ratifie<sup>27</sup> le récent Accord ACRC (Accord commercial relatif à la contrefaçon)<sup>28</sup> signé le 1<sup>er</sup> octobre 2011 à Tokyo, lequel introduit l'obligation de prévoir des mesures efficaces pour lutter contre les infractions à la propriété intellectuelle dans un environnement numérique.<sup>29</sup> Elle serait sur le point de le faire à l'heure où ces lignes sont écrites.<sup>30</sup> À l'aune des nombreux griefs émis

---

<sup>23</sup> Est-il licite de créer un faux profil sur Facebook pour, après s'être fait accepter, de ce fait comme ami, récolter des informations qui seront produites à titre de preuve dans une procédure ultérieure?

<sup>24</sup> Rapport de gestion 2010 du Tribunal fédéral (disponible à cette adresse: [http://www.bger.ch/fr/gb2010\\_bger\\_d.pdf](http://www.bger.ch/fr/gb2010_bger_d.pdf)), 17 au § intitulé „Indications à l'intention du législateur“, lequel aurait également pu s'intituler invitation au législateur, tant les sujets abordés nécessitent une diligente et efficiente intervention.

<sup>25</sup> Il convient de signaler à cet égard une initiative isolée de la Conseillère aux États Géraldine Savary qui a lancé un postulat le 19 mars 2010, postulat intitulé „La Suisse a-t-elle besoin d'une loi contre le téléchargement illégal de musique“.

<sup>26</sup> Rapport annuel 2010 SUIISA, 22, disponible à cette adresse: [http://www.suisa.ch/fileadmin/user\\_upload/Downloads/Publikationen/SUIISA-Rapport-Annuel.pdf](http://www.suisa.ch/fileadmin/user_upload/Downloads/Publikationen/SUIISA-Rapport-Annuel.pdf).

<sup>27</sup> Selon un article du Monde du 5 octobre 2011, huit pays ont signé ce traité (USA, Australie, Canada, Corée du Sud, Japon, Maroc, Nouvelle-Zélande et Singapour) et trois autres acteurs seraient sur le point de le signer dont la Suisse. La Suisse est l'un des initiateurs de l'ACRC.

<sup>28</sup> Il s'agit d'un traité international multilatéral concernant les droits de propriété intellectuelle; pour de plus amples informations, cf. la page wikipédia y consacrée: [http://fr.wikipedia.org/wiki/Accord\\_commercial\\_anti-contrefa%C3%A7on#Dispositions\\_principales](http://fr.wikipedia.org/wiki/Accord_commercial_anti-contrefa%C3%A7on#Dispositions_principales).

<sup>29</sup> Pour en savoir plus, *Denis Barrelet/Stéphane Werly*, Droit de la communication, Berne 2011, n. 554, 163.

<sup>30</sup> [http://www.lemonde.fr/technologies/article/2011/10/05/le-traite-acta-officiellement-signé-par-huit-pays\\_1582756\\_651865.html](http://www.lemonde.fr/technologies/article/2011/10/05/le-traite-acta-officiellement-signé-par-huit-pays_1582756_651865.html).

par les défenseurs de la vie privée,<sup>31</sup> ainsi que des problèmes inhérents à la ratification et à l'application de tels textes, le législateur serait bien inspiré de se saisir par anticipation d'un problème pour lequel tous s'accordent à dire qu'une solution doit rapidement être trouvée, solution respectueuse des droits de chacun.

### **C. Arrêt du Tribunal fédéral du 8 septembre 2010 (ATF 136 II 508) dans l'affaire Logistep: la première audience judiciaire suisse twittée!**

Pour la première fois, le Tribunal fédéral s'est déterminé formellement sur l'utilisation de Twitter<sup>32</sup> durant les séances publiques, dans le cadre de l'affaire Logistep, sans toutefois que cela ne transparaisse à la lecture de cet arrêt.<sup>33</sup> Après plusieurs échanges de correspondance, exclusivement avec le Secrétariat général du Tribunal fédéral, le point de vue suivant a été émis: „À ce jour, le Tribunal fédéral n'a pas réglé expressément la question relative à l'utilisation d'appareils électroniques dans les salles d'audience. Jusqu'ici, les ordinateurs et téléphones portables ont été tolérés, pour autant qu'ils soient utilisés dans le but de rédiger un texte et qu'ils ne dérangent pas le bon déroulement de la séance. Il est toutefois nécessaire de préciser que les prises de vue ou de son sont formellement interdites, cette réserve étant nécessaire compte tenu de la multifonctionnalité de ces appareils. Aussi longtemps que ces conditions seront respectées et que le juge qui préside l'audience n'ordonne pas le contraire, rien ne s'oppose à l'utilisation de ‚Twitter‘. Nous nous réservons toutefois de régler expressément cette question à l'avenir, sur la base des expériences qui seront faites [...]“

À l'issue des délibérations publiques du 8 septembre 2010, il est apparu que la position communiquée par le Secrétariat général du Tribunal fédéral n'était pas partagée par l'ensemble des magistrats composant la Cour, voire même n'aurait pas été celle de la Cour, si celle-ci avait dû se prononcer. Une incertitude demeure donc relativement à l'avenir de l'utilisation de Twitter lors des audiences publiques des Tribunaux, en sus de la possibilité pour le Juge président les débats de proscrire de telles communications. Le Tribunal fédéral réserve

---

<sup>31</sup> Pour les griefs émis en Suisse par la Déclaration de Berne et alliance sud, cf.: [http://www.evb.ch/cm\\_data/1011\\_Mmo\\_ACTA\\_DB\\_\\_AS\\_Final.pdf](http://www.evb.ch/cm_data/1011_Mmo_ACTA_DB__AS_Final.pdf).

<sup>32</sup> Il s'agit d'un réseau social et de microblogage qui permet à l'utilisateur d'envoyer gratuitement des messages brefs (140 caractères), appelés „tweets“ („gazouillis“), par internet, par messagerie instantanée ou par SMS.

<sup>33</sup> Pour une présentation exhaustive de la procédure ayant conduit à ce que le Tribunal fédéral accepte que l'audience soit twittée, cf. *Sébastien Fanti*, De l'utilisation de Twitter lors des audiences publiques des tribunaux, *Medialex* 2011, 1–4; *Sébastien Fanti*, *Gazette du Palais*, n° 203–204, *Droit des technologies avancées*, 26–28.

également une réglementation ultérieure sur la base des expériences réalisées. Les garde-fous sont donc ancrés.

Il s'agit sans nul doute des prémices d'une inéluctable fulgurance dans la transmission en temps réel du contenu des audiences des tribunaux. Les défenseurs de la transparence avaient pronostiqué le „You Tube next?“. L'actualité récente a toutefois démontré que des supports pluriels pouvaient s'avérer de redoutables vecteurs de transparence. L'application „Michael Jackson Doctor Trial“, oeuvre de la chaîne de télévision Fox (disponible pour iPhone, iPad et les téléphones équipés du système d'exploitation Android, de même que les BlackBerry), occupait la 29<sup>ème</sup> place de tous les classements d'applications payantes confondus. Elle permet de suivre en direct le procès du médecin de feu le roi de la pop poursuivi pour homicide involontaire et propose, en sus, des analyses d'experts. Force est donc de constater que l'intérêt pour la science juridique, certes teinté de voyeurisme, ne pourra se satisfaire de supports classiques de compte-rendu. La transparence raisonnable doit donc être concrétisée dans les plus brefs délais, sous peine de voir la technologie s'imposer. L'impulsion devrait, de ce point de vue, et pour éviter des solutions différenciées, provenir du Tribunal fédéral qui a déjà ouvert la voie avec la sagesse et la clairvoyance qui le caractérisent.

#### **D. Arrêt du Tribunal administratif fédéral (TAF) du 30 mars 2011 (A-7040/2009) dans l'affaire Google Streetview<sup>34</sup>**

Cette affaire a également donné lieu à nombre de publications,<sup>35</sup> qui témoignent de l'intérêt croissant pour les problématiques juridiques liées aux technologies avancées. De nombreuses autorités de protection des données ont également été saisies dans le monde ce qui a engendré l'ouverture de procédures dans, à tous le moins, 12 pays dans le monde,<sup>36</sup> avec des fortunes

---

<sup>34</sup> L'arrêt est disponible à cette adresse: <http://www.bvger.ch/aktuell/index.html?lang=fr>.

<sup>35</sup> À titre exemplatif et non exhaustif: *Peter Studer*, Der Datenschutzbeauftragte klagt Google wegen Street View beim Bundesverwaltungsgericht ein: Angemessen oder übertrieben? Jusletter 23 novembre 2009; *Thomas Müller*, Lex helvetica gilt auch für die amerikanische Firma Google Inc., Jusletter 18 avril 2011; *Lukas Morscher*, Aktuelle Entwicklungen im Technologie- und Kommunikationsrecht, ZBJV 2011, 177–221; *Philippe Meier*, À l'impossible nul n'est tenu ... sauf Google?, Quelques réflexions sur l'arrêt Google Street View du Tribunal administratif fédéral (TAF) du 30 mars 2011, Medialex 2011, 69–71; *Hanspeter Thür*, Aktuelle Fragen rund um den Datenschutz, BJM 2010, 225–239.

<sup>36</sup> Pour un état de lieux non exhaustif de ces procédures, cf.: [http://fr.jurispedia.org/index.php/Google\\_street\\_view\\_et\\_donn%C3%A9es\\_personnelles](http://fr.jurispedia.org/index.php/Google_street_view_et_donn%C3%A9es_personnelles).



diverses<sup>37</sup> pour le géant de Mountainview. Dans la majorité des cas, un constat de violation des normes en matière de protection des données a été émis.

Google Street View est un service qui permet de naviguer virtuellement dans les rues des grandes villes. Il utilise une technologie qui permet de fournir une vue de la rue à 360 degrés en n'importe quel point de cette rue.<sup>38</sup> Une voiture équipée de caméras (d'une hauteur de 2.75 m) circule dans les rues en prenant des images qu'un logiciel assemble pour donner l'impression de continuité. Ce service a été intégré à Google Earth dès avril 2008. Ce service a été mis en ligne à la mi-août 2009 en Suisse et il comporte plus de 20 millions d'images. Depuis, tant le Préposé que Google Suisse ont reçu nombre d'annonces concernant l'insuffisance ou l'absence de floutage des visages et des plaques d'immatriculation.<sup>39</sup>

Il convient de préciser que le Préposé avait émis un certain nombre de conditions préalables, tel que la possibilité d'annoncer online les insuffisances de floutage ou de demander l'effacement des images. Ces annonces sont d'ordinaire traitées dans les 24 à 48 heures. De surcroît, Google a communiqué à l'avance les lieux où les prises de vue étaient planifiées.

Après différentes vérifications, le Préposé a constaté la présence d'images problématiques et insuffisamment anonymisées et il en a fait état publiquement le 21 août 2009 déjà.<sup>40</sup> Il s'agissait notamment d'images prises dans des rues privées, d'images de jardins... Les informations données par Google étaient également lacunaires et imprécises. Le Préposé a alors informé Google qui a proposé différentes mesures d'amélioration, dont l'implémentation d'une nouvelle version du logiciel destinée à améliorer le floutage. Google a par contre refusé un traitement manuel des données. Celles-ci sont apparues insuffisantes au Préposé, raison pour laquelle il a émis une recommandation le 11 septembre 2009 (art. 29 al. 3 LPD).<sup>41</sup>

---

<sup>37</sup> La recommandation 05/2010 du 15 décembre 2010 de la Commission de la protection de la vie privée (Belgique) en matière de Mobile Mapping est disponible à cette adresse: [http://www.privacycommission.be/fr/docs/Commission/2010/recommandation\\_05\\_2010.pdf](http://www.privacycommission.be/fr/docs/Commission/2010/recommandation_05_2010.pdf); le rapport des conclusions émis par le Commissariat à la protection de la vie privée du Canada en vertu de la LPRPDE n° 2010-001 relativement à la collecte de données Wi-Fi par Google Inc. est disponible à cette adresse: [http://www.priv.gc.ca/cf-dc/2011/2011\\_001\\_0520\\_f.cfm](http://www.priv.gc.ca/cf-dc/2011/2011_001_0520_f.cfm); la position de la France est exposée ci-après au § V.

<sup>38</sup> Cette technologie est intitulée Mobile Mapping. Il s'agit de la technologie par laquelle un véhicule équipé de caméras et/ou d'un scanner peut enregistrer numériquement toutes les données d'une route spécifique, notamment par la prise de photos à 360 degrés.

<sup>39</sup> Le Préposé a publié dès le 18 août 2009, soit quelques jours après la mise en service de Google Street View sur son site web une demande type d'anonymisation de données disponible à cette adresse: <http://www.edoeb.admin.ch/dokumentation/00503/01583/index.html?lang=fr>.

<sup>40</sup> Par le biais d'une information aux médias intitulée „Google Street View doit être retiré d'internet“, cf.: <http://www.edoeb.admin.ch/dokumentation/00438/00465/01676/01678/index.html?lang=fr>.

<sup>41</sup> Cf. l'annonce de la recommandation: <http://www.edoeb.admin.ch/dokumentation/00438/00465/01676/01681/index.html?lang=fr>; la recommandation étant disponible à cette adresse: <http://www.edoeb.admin.ch/dokumentation/00445/00508/index.html?lang=de>.

La société Google n'ayant pas obtempéré, le Tribunal administratif fédéral a été saisi par requête du 11 novembre 2009 du Préposé fédéral à la protection des données.<sup>42</sup> Il exigeait, en substance, que les visages et les plaques d'immatriculation soient rendus méconnaissables, que l'anonymat des personnes photographiées à proximité d'installations sensibles soit garanti, que les photographies d'espaces privés ou prises à partir de rues privées soient retirées de Google Street View et que les villes et villages soient informés préalablement de l'intention de les photographier et de la mise en ligne.<sup>43</sup>

Le Préposé a requis du président de la cour du Tribunal administratif fédéral des mesures provisionnelles, ainsi que le lui permet l'article 33 al. 2 LPD.<sup>44</sup> Cette question a été débattue entre les parties qui sont, finalement, parvenues à un accord au terme duquel:

- Google s'engage à ne publier sur Internet aucune nouvelle image prise en Suisse pour Street View, ni dans le cadre de son service en ligne Street View, ni dans le cadre d'aucun autre de ses produits, et ce jusqu'à ce que le Tribunal administratif fédéral ait statué et que l'arrêt soit entré en force.
- Google s'engage à se soumettre à l'arrêt que le Tribunal administratif fédéral rendra dans cette affaire et à l'appliquer pour toutes les photographies prises en Suisse pour Street View, si et dans la mesure où le jugement devait l'exiger.<sup>45</sup>
- Google reste autorisé à poursuivre ses prises de vues en Suisse, à ses risques toutefois, eu égard à l'issue à venir de la procédure judiciaire en cours. Conformément au ch. 1 ci-dessus, les images concernées ne seront pas mises en ligne et, jusqu'à ce que le Tribunal administratif fédéral ait statué, resteront au sein du groupe Google et pourront être utilisées uniquement à des fins ou dans le cadre de produits ne se rapportant pas à des personnes.
- Google annoncera en ligne et au plus tard une semaine à l'avance (au lieu d'un mois précédemment) les districts ou environs de villes où elle envisage de procéder à des prises de vues sur le domaine public.

---

<sup>42</sup> La plainte du Préposé est disponible à cette adresse: <http://www.edoeb.admin.ch/dokumentation/00651/01596/index.html?lang=de>.

<sup>43</sup> Les exigences du Préposé sont disponibles en résumé ici: <http://www.edoeb.admin.ch/dokumentation/00438/00465/01676/01681/index.html?lang=fr>.

<sup>44</sup> Dont la teneur est la suivante: „si le Préposé constate à l'issue de l'enquête qu'il a menée en application de l'article 27 al. 2 ou de l'article 29 al. 1 que la personne concernée risque de subir un préjudice difficilement réparable, il peut requérir des mesures provisionnelles du président de la cour du Tribunal administratif fédéral qui est compétent en matière de protection des données. Les articles 79 à 84 de la loi fédérale du 4 décembre 1947 de la procédure civile fédérale s'appliquent par analogie à la procédure.“

<sup>45</sup> Le libellé du chiffre 2 est pour le moins singulier. Prendre l'engagement de se soumettre à un arrêt susceptible de recours au Tribunal fédéral est pour le moins sibyllin même s'il ne s'agit que de mesures provisionnelles.

- Le PFPDT considère que les objectifs visés par les mesures provisionnelles qu'il avait demandé au Tribunal administratif fédéral de prendre sont atteints, ce qui l'amène à retirer la demande en question.
- L'accord conclu ne préjuge en rien les positions défendues par les parties dans le cadre de la procédure en cours.

Le TAF a rendu son arrêt le 30 mars 2011 et il a partiellement admis l'action engagée par le PFPDT contre Google Inc. et Google Switzerland GmbH (abrégés ci-après Google) concernant Google Street View.<sup>46</sup> Le traitement des données a été considéré par le TAF comme attentatoire à la personnalité: chacun(e) a droit à sa propre image, qui fait partie du droit de la personnalité; en l'occurrence, nonobstant le fait que les images fassent apparaître des personnes comme des éléments secondaires destinés à animer un paysage, un voisinage ou un événement, le droit à l'autodétermination en matière d'information s'applique également et il convient de procéder à un examen des intérêts en jeu. Les intérêts en jeu sont les suivants: le droit au respect de la vie privée et le droit à sa propre image à examiner à l'aune des intérêts purement économiques avancés par Google. Dans ce cadre, le TAF met en exergue le fait qu'il ne s'agit pas d'interdire entièrement Google Street View, mais simplement de ne publier sur Internet que des images rendues méconnaissables ou de ne pouvoir en disposer sans avoir obtenu l'assentiment des personnes concernées.

Google fait valoir un intérêt économique dans l'exploitation de Google Street View, notamment celui qui consiste à renforcer sa position dans le domaine des applications cartographiques en ligne et à pénétrer sur de nouveaux marchés via des applications, comme des systèmes de navigation. S'y ajoute la vente d'espaces publicitaires. Le TAF retient toutefois que lorsque Google évoque l'intérêt des particuliers, entreprises et communes à utiliser ce service en ligne, c'est en réalité de ses propres intérêts financiers dont il s'agit. C'est donc dans le but d'une réussite économique que Google est prêt à accepter une éventuelle atteinte aux droits de la personnalité de nombreuses personnes. Il serait au demeurant possible d'éviter ces atteintes moyennant un surplus de coûts pour Google puisque les images devraient être rendues encore plus méconnaissables au moyen d'un procédé en partie manuel. Cet effort supplémentaire ne serait pas de nature à remettre en cause la viabilité économique du service, une répercussion des coûts sur les utilisateurs étant également possible.

En définitive, même si l'on doit reconnaître que le fait de renoncer à des coûts supplémentaires et celui de proposer gratuitement Google Street View constituent des intérêts à poursuivre un but lucratif, l'intérêt des personnes concernées à leur propre image prévaut. La conclusion est

---

<sup>46</sup> La conclusion n° 4 de la plainte du Préposé a été rejetée: „Google Inc. sowie die Google Schweiz GmbH stellen sicher, dass die von Privatstrassen aus gemachten Aufnahmen aus dem Dienst Google Street View entfernt werden, sofern keine Einwilligung für die Aufnahmen vorliegt.“

donc que l'intérêt du public à prendre connaissance de l'image de l'événement ou que l'intérêt économique de Google ne peut en aucun cas prévaloir sur le droit à sa propre image, puisqu'il est possible et adéquat de rendre les images méconnaissables partiellement, voire totalement.

En conséquence, selon cet arrêt, Google doit veiller à ce que tous les visages et plaques de contrôle soient rendus méconnaissables avant la publication des images sur Internet. En ce qui concerne les installations sensibles (hôpitaux, prisons, maisons de protection de la femme, etc.), l'anonymat des personnes doit être garanti. Google devra également informer une semaine avant ses prises de vue non seulement sur Internet, mais également dans les médias locaux. S'agissant des lieux privés (jardins, cours intérieures de maison) les images de Google Street View ne devront pas montrer davantage que ce que peut voir un passant normal.

Cet arrêt a fait l'objet d'un recours auprès du Tribunal fédéral qui devrait prochainement se prononcer, à l'aune du temps qui lui a été nécessaire pour rendre son jugement dans l'affaire Logistep.

Il convient de constater (comme par ailleurs dans l'affaire Logistep), que le TAF a rendu sa décision 16 mois après avoir été saisi par le Préposé (soit le 30 mars 2011 alors que la plainte a été déposée le 11 novembre 2009). Un tel délai pour rendre un jugement, nonobstant l'accord intervenu relativement aux mesures provisionnelles requises et la complexité du cas, n'est pas acceptable. La comparaison avec les décisions rendues dans d'autres pays permet de constater qu'il est possible de trancher de tels cas dans un délai de 6 mois, dès la question des mesures provisionnelles réglée. La plainte du Préposé a, comme l'a relevé le Tribunal fédéral dans son arrêt Logistep, un effet préventif pour tous ceux qui pratiquent le même traitement de données que la défenderesse. Le signal qui doit en conséquence être donné est celui d'un traitement diligent et rapide des violations alléguées de la LPD. À défaut, les acteurs du domaine des technologies avancées ne nourriront à brève échéance plus aucune crainte relativement aux risques en cas d'insoumission à une recommandation du Préposé. C'est donc le Préposé lui-même qui pourrait être affaibli par ces atermoiements, que rien ne justifie.<sup>47</sup>

L'un des points cruciaux, rarement évoqués dans cette affaire a trait au fait que la société Google Switzerland Sàrl répond désormais légalement en Suisse, nonobstant ses dénégations réitérées visant à orienter les procédures vers la société Google Inc. (absence de qualité pour défendre alléguée).<sup>48</sup> Si le Tribunal fédéral devait soutenir également ce point de vue, les procédures à l'encontre de Google Switzerland Sàrl pourraient se multiplier. Le TAF a, à cet

---

<sup>47</sup> Il convient, à cet égard, de relever la promptitude avec laquelle le Préposé a émis sa recommandation, puis a déposé sa plainte.

<sup>48</sup> Notamment dans le cadre de la procédure ayant abouti à l'arrêt de la Cour civile du Tribunal cantonal jurassien du 12 février 2011 (Albert Tanneur Institut & Co Sàrl/Google Inc.). La consultation de l'arrêt peut se faire à cette adresse: <http://www.jura.ch/JUST/Instances-judiciaires/Tribunal-cantonal/Jurisprudence-recente.html>.

égard, fait preuve de clairvoyance, tant il paraît douteux que la société Google Switzerland Sàrl soit littéralement coupée de son cordon ombilical (le moteur de recherche et les serveurs qui l'hébergent), respectivement que seule la société Google Inc. dispose réellement des données collectées. De plus, rien ne permet de vérifier les allégations de Google que l'autorité et les tribunaux devraient donc croire sur parole. Google Switzerland Sàrl soutient également ne pas exploiter le moteur de recherche Google. Or, il apparaît exactement le contraire à la lecture du but figurant dans ses statuts publiés au Registre du Commerce de Zurich.<sup>49</sup> De surcroît, Google Inc. détient la seule part sociale de Google Switzerland Sàrl.<sup>50</sup> Ces deux sociétés sont donc intimement liées, tant du point de vue technique et que du point de vue juridique. La conclusion à laquelle parvient le TAF à cet égard est donc en adéquation avec la réalité juridique.

Les critiques principales relatives à cet arrêt ont trait à la pesée des intérêts opérée, ainsi qu'au statut légal des images réalisées. S'agissant précisément de ces images, force est de constater que leur statut doit être appréhendé à l'aune du but poursuivi qui est en définitive un but commercial. D'autre part, une image peut aujourd'hui, de par l'évolution des technologies, être rapidement modifiée, diffusée, dupliquée, etc. Nous en avons une excellente illustration avec l'histoire, largement reprise par les médias,<sup>51</sup> d'une Maserati parquée devant l'hôtel de police de Lausanne. Tout le monde s'interroge: „Que faisait Christian Constantin le Président du FC Sion devant ce commissariat à Lausanne?“. En réalité, nonobstant les affirmations des journalistes, il ne s'agissait pas de Christian Constantin que l'on pouvait apercevoir au moyen du service Google Street View, mais d'un tiers qui s'est finalement reconnu et dont l'identité a pu être établie. Cet exemple anodin démontre que les images récoltées par Google, même si elles ont pu l'être dans un contexte accessoire ou accidentel et sur la voie publique ont eu pour conséquence de générer des interrogatoires sur le pourquoi de la présence d'une personnalité devant un commissariat. Il n'est guère agréable de devoir justifier d'une telle présence et la personne concernée pourrait très clairement subir un dommage de ce fait, ce d'autant qu'une erreur est possible comme ce fut le cas en l'espèce. En définitive, le simple quidam que l'on peut

---

<sup>49</sup> „Die Gesellschaft bezweckt die Herstellung und Entwicklung von computergestützten Technologieprogrammen, Produkten, Dienstleistungen und Anwendungen sowie die Entwicklung und den Verkauf von Produkten respektive die Erbringung von Dienstleistungen für den Internetgebrauch insbesondere im Bereich der **Internetsuche**, der Internetprogramme, -produkte, und -anwendungen, hauptsächlich in der Schweiz. Die Gesellschaft kann Patente, Handelsmarken und technische und industrielle Kenntnisse erwerben, verwalten und übertragen. Die Gesellschaft kann sich an anderen kommerziellen und industriellen Unternehmungen beteiligen und im In- und Ausland Zweigniederlassungen und Tochtergesellschaften errichten. Die Gesellschaft ist berechtigt, im In- und Ausland Grundeigentum zu erwerben, zu belasten, zu veräußern und zu verwalten. Die Gesellschaft kann im Übrigen alle Geschäfte tätigen, die geeignet sind, die Erreichung des Gesellschaftszweckes zu fördern.“

<sup>50</sup> À hauteur de 400'000 francs.

<sup>51</sup> [http://www.nzz.ch/nachrichten/digital/was\\_macht\\_christian\\_constantin\\_bei\\_der\\_polizei\\_1.10178941.html](http://www.nzz.ch/nachrichten/digital/was_macht_christian_constantin_bei_der_polizei_1.10178941.html).

identifier au moyen d'un tel service et qui n'a de surcroît rien demandé à personne est en droit de considérer qu'il est victime d'une atteinte à ses droits de la personnalité. L'image représente donc désormais dans notre société un risque accru dont il convient de tenir compte.

En ce qui concerne finalement la pesée des intérêts en présence et la quasi-obligation de résultat s'agissant du floutage des images, il est certes permis de s'interroger. Toutefois, à l'aune des chiffres présentés par la firme de Google elle-même, on perçoit immédiatement que si le pourcentage d'images non floutées est faible, cela représente toutefois une atteinte potentielle aux droits de plusieurs milliers de personnes qui n'ont, une fois encore, rien sollicité. À admettre un taux d'échec qui, même s'il est infime, lèserait un si grand nombre, on créerait une inégalité de traitement entre des images pour lesquelles un consentement est régulièrement et formellement requis (pour les photos des enfants dans un cadre scolaire ou associatif) et des images littéralement spoliées. Cela augure d'une évolution qui deviendrait rapidement incontrôlable. Finalement, le fait de refuser, alors que cela est parfaitement possible, une anonymisation „manuelle“ démontre une nouvelle fois que le but est économique. De telles démarches ont un coût que Google n'est pas disposé à assumer. Pourtant, personne ne doute du fait que ces images vont être valorisées d'une manière ou d'une autre (par l'intégration par exemple à un logiciel GPS) et qu'elles vont en définitive rapporter beaucoup d'argent à Google. Cela justifie dès lors de se montrer strict, s'agissant de l'application du principe de proportionnalité. Le Tribunal fédéral osera-t-il, dans ces circonstances, ouvrir une boîte de pandore dont il ne peut ignorer qu'elle générera, *de facto*, une multiplication d'ingérences dans la sphère privée du citoyen par le biais de services dont l'intrusivité croissante ne cesse de générer craintes et débats? Cet arrêt est sans nul doute le plus attendu et il influera durablement sur le développement des technologies avancées dans notre pays.

#### **E. Délibération n° 2011-035 de la formation restreinte de la CNIL prononçant une sanction pécuniaire à l'encontre de la société Google Inc.<sup>52</sup>**

La Commission nationale de l'informatique et des libertés (abrégé ci-après CNIL) est le pendant français du Préposé à la protection des données et à la transparence. Elle a été instituée par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée en 2004,<sup>53</sup> qui la qualifie d'autorité administrative indépendante.

---

<sup>52</sup> La délibération est disponible à cette adresse: [http://www.cnil.fr/fileadmin/documents/La\\_CNIL/actualite/D2011-035.pdf](http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/D2011-035.pdf).

<sup>53</sup> Dont la teneur est consultable à cette adresse: <http://www.cnil.fr/en-savoir-plus/textes-fondateurs/loi78-17/>.

La société Google procède depuis plusieurs années à la collecte massive de données techniques sur les réseaux Wi-Fi, aux fins d'offrir des services de géolocalisation (notamment les services Google Maps, Street View et Latitude). La CNIL a mené une série de contrôles sur place afin de vérifier la conformité de ces traitements à la loi „informatique et libertés“. Ces contrôles ont révélé divers manquements comme la collecte de données Wi-Fi à l'insu des personnes concernées et la captation de données dite „de contenu“ (identifiants, mots de passe, données de connexion, échanges de courriels). La CNIL a donc mis en demeure la société Google, en mai 2010, de régulariser sa situation.

Estimant qu'il n'avait pas été répondu à ses demandes dans les délais impartis, la formation contentieuse de la CNIL a prononcé à l'encontre de la société, le 17 mars 2011, une amende de 100 000 €

Des contrôles effectués fin 2009 et début 2010 ont permis à la CNIL de constater que les véhicules déployés sur le territoire français capturaient et enregistraient non seulement des photographies, mais aussi des données transitant par les réseaux sans fil Wi-Fi de particuliers, et ce à l'insu des personnes concernées. Il s'avère que c'est précisément cette collecte de dizaines de milliers de points d'accès Wi-Fi par le biais des „Google cars“ qui a permis à la société de développer une base de données de géolocalisation extrêmement performante, et d'acquérir ainsi une position dominante dans le secteur des services de géolocalisation. En avril 2010, Google a déclaré dans la presse internationale ne collecter aucune donnée de contenu de communications à l'occasion de la circulation de ses véhicules. Revenant sur ses déclarations initiales, la société a reconnu deux semaines plus tard par voie de presse qu'elle avait effectivement enregistré de telles données.

Compte tenu de la gravité des faits et du risque d'atteinte à la vie privée des utilisateurs des réseaux Wi-Fi concernés, la CNIL a mis en demeure la société, le 26 mai 2010, de cesser toute collecte de données à l'insu des personnes et de lui fournir une copie de l'intégralité des données de contenu captées sur le territoire national. Google ayant communiqué ces données de contenu, la CNIL a ainsi été la première autorité au monde à pouvoir les analyser. L'analyse menée sur ces données par la CNIL a permis de constater que Google avait enregistré, outre des données techniques (identifiants SIID et adresses MAC des points d'accès Wi-Fi), de nombreuses données concernant des particuliers, identifiés ou identifiables (données de connexion à des sites web, mots de passe de messagerie, adresses de courrier électronique, échanges de courriels révélant notamment des informations sensibles sur l'orientation sexuelle ou la santé des personnes).

Dans sa décision du 17 mars 2011, la formation contentieuse de la CNIL relève que Google a pris l'engagement de cesser la collecte de données Wi-Fi par ses „Google cars“ et de supprimer les données de contenu enregistrées selon elle par erreur. En revanche, elle constate qu'elle n'a

pas renoncé à utiliser les données identifiant les points d'accès Wi-Fi de particuliers à leur insu. En effet, cette collecte n'est aujourd'hui plus réalisée par les „Google cars“, mais s'opère directement par le biais des terminaux mobiles des utilisateurs se connectant au service de géolocalisation Latitude (smartphones, etc.), et ce à leur insu. La CNIL considère que ce défaut d'information constitue une collecte déloyale au sens de la loi, qui était déjà à l'œuvre avec les „Google cars“.

La formation contentieuse estime en outre que les réponses apportées par la société Google à la suite de la mise en demeure sont insuffisantes, celle-ci ne lui ayant toujours pas fourni les éléments du programme informatique ayant conduit à la collecte des données Wi-Fi, contrairement à sa demande en ce sens. Enfin, elle reproche à Google de contester l'application de la loi française au service Latitude, et d'avoir ainsi refusé de le déclarer à la CNIL malgré deux demandes en ce sens. Dans ces conditions, compte tenu des manquements constatés et de leur gravité, ainsi que des avantages économiques que retire la société Google de ces manquements, la formation contentieuse de la CNIL a décidé de prononcer à son encontre une sanction pécuniaire de 100 000 € (la sanction pécuniaire maximale étant de 300 000 €).

En vertu de l'article 34 LPD, une telle sanction serait également possible en Suisse, étant précisé que le montant de l'amende est limité à 10'000 francs. Hormis cette différence de traitement, inhérente à des normes moins sévères dans notre pays, force est de constater que les constatations réalisées par la CNIL permettent de soutenir que des données sensibles, au sens également de notre droit helvétique, sont collectées. Ce qu'il y a de plus inquiétant encore, c'est qu'une nouvelle fois, nonobstant les engagements pris, Google est en contradiction avec ses propres déclarations. La confiance est rompue et cette attitude a pour conséquence manifeste de générer une nécessité de contrôle accru des activités de cette entreprise, avec le risque d'introduction à terme d'une règle d'autorisation préalable d'exploitation, lorsque comme en l'espèce, les données d'un grand nombre de personnes sont collectées et traitées. Cette décision doit exhorter à la prudence, dans la mesure où les données spoliées sont extrêmement sensibles (santé, préférences sexuelles, etc.) et que la masse d'informations détenues par Google permettra (si elle ne le permet pas déjà) de dresser des profils de personnalité très précis. C'est dans le but de signifier à Google que de tels comportements sont intolérables et inqualifiables que la CNIL a infligé une amende qualifiée de record. La firme de Mountainview n'a pas contesté cette amende.



**F. Décision du 17 février 2011 de la commission cantonale de protection des données du Canton du Jura (tenue d'un fichier informatisé des automobilistes avertis par la police cantonale)**

Durant l'automne 2010, divers médias se sont fait l'écho de l'existence d'un fichier constitué par la Police cantonale jurassienne, recensant les conducteurs de véhicules à qui un simple avertissement verbal aurait été signifié en raison de la commission d'une infraction, laquelle conduit d'ordinaire au prononcé d'une amende d'ordre. Ce fichier serait utilisé par les agents de police pour vérifier si un conducteur a déjà fait l'objet d'un avertissement et d'autre part par la hiérarchie pour vérifier si les objectifs assignés aux agents ont été respectés (montant global d'amendes à prononcer). Finalement, les agents auraient été instruits sur la base d'un catalogue des amendes d'ordre: amende obligatoire (couleur rouge), amende selon les circonstances (couleur bleue) et avertissement (couleur verte).

La Commission cantonale de la protection des données a ouvert une enquête le 9 novembre 2010. L'instruction a permis d'établir qu'au 26 novembre 2010, 2700 avertissements environ avaient été décernés depuis 2004.

L'existence d'une base de données informatique de la Police cantonale dans laquelle sont enregistrés les avertissements verbaux signifiés aux automobilistes qui contreviennent aux règles de la circulation routière a été établie. Il s'agit du journal de la police, c'est-à-dire la main courante informatique dans laquelle sont mentionnées toutes les activités de la police.

Les données collectées (événement; nom et prénom de l'automobiliste; date de naissance; domicile; adresse; marque et couleur du véhicule et numéro d'immatriculation) sont des données à caractère personnel qui dans la mesure où elles sont traitées dans le cadre d'une procédure pénale même simplifiée, constituent des données sensibles.

La loi sur les amendes d'ordre ne fait pas état d'un avertissement qui pourrait être décerné au contrevenant à la place d'une amende d'ordre. De surcroît, l'amende d'ordre (qui constitue une peine, cf. arrêt CEDH Zolotoukhine c/Russie) est totalement anonyme et ne fait l'objet d'aucune inscription dans un registre quelconque y. c. le casier judiciaire. Lorsqu'elle est payée, toute trace est effacée.

Il résulte du principe absolu de l'anonymat des amendes d'ordre et de l'absence de toute base légale que l'inscription d'une amende d'ordre infligée à un automobiliste dans un registre ou une base de données quelconque est interdite.

S'agissant des avertissements, la procédure simplifiée ne prévoit pas dans le système de la loi sur les amendes d'ordre, la possibilité d'exempter de toute sanction un conducteur ayant commis une infraction routière. Il est toutefois toléré qu'aucune suite ne soit donnée à la commission d'une infraction si peu grave qu'elle constitue un cas bagatelle.

Ainsi, nonobstant le fait que la démarche n'est pas incongrue, il apparaît que l'inscription des avertissements dans une base de données de la police (journal de police) est contraire au principe d'anonymat ancré dans la loi sur les amendes d'ordre. L'accomplissement d'aucune tâche légale n'implique que des données à caractère personnel permettant d'identifier les automobilistes avertis soient répertoriées dans les dossiers de la police. Ces inscriptions doivent donc être considérées comme un traitement illicite de données personnelles. Les avertissements doivent conséquemment être effacés.

### **G. Résumés d'arrêts divers du Tribunal fédéral**

- Arrêt du Tribunal fédéral 1C\_111/2010 du 29 avril 2010: le droit fédéral (art. 365 ss CP et LPD) ne prévoit pas que les inscriptions au casier judiciaire fassent systématiquement l'objet d'une notification d'office à la personne concernée. La protection juridique est assurée par l'accès au fichier, qui peut avoir lieu en tout temps (art. 370 CP, art. 26 ordonnance VOSTRA et art. 25 LPD) et par le droit de rectification (art. 26 al. 4 VOSTRA et 25 LPD).
- Arrêt du Tribunal fédéral 2C\_230/2010 du 12 avril 2011: l'obligation d'annonce imposée aux prostituées et aux tenanciers d'établissements n'est pas disproportionnée en tant que telle, ce d'autant que le législateur cantonal s'est abstenu de soumettre l'activité de ces entreprises au régime plus strict de l'autorisation préalable. L'annonce des personnes qui s'adonnent occasionnellement à la prostitution est quant à elle nécessaire en raison de leur vulnérabilité souvent accrue due à leur inexpérience et à la possible absence d'affiliation aux associations d'entraide. Les obligations d'annonce précitées ne violent donc pas l'article 13 Cst.
- Dans un arrêt du 18 octobre 2011, la deuxième section de la Cour européenne des droits de l'homme<sup>54</sup> a retenu que la Suisse avait violé l'article 8 CEDH (droit au respect de la vie privée et familiale) en relation avec le classement durant 5 ans d'une ressortissante française comme « prostituée » dans la base de données informatique de la police de Genève (affaire *Khelili c. Suisse*, requête n° 16188/07). La mémorisation, dans le dossier de police, d'une donnée à caractère personnel, prétendument erronée, viole le respect de la vie privée et le maintien de la mention « prostituée » pendant des années n'était ni justifié, ni nécessaire dans une société démocratique. La Suisse devra verser à Mme Khelili 15'000 euros

---

<sup>54</sup> Disponible à cette adresse : <http://s.conjur.com.br/dl/decisao-corte-europeia-direitos-humanos33.pdf>

pour dommage moral, ce qui à l'aune du droit interne et de la jurisprudence helvétique constitue un montant tout à fait singulier de par son importance. Il devrait inciter à la prudence tous les maîtres de fichier.

## **H. Conclusions**

On ne peut que se réjouir de la multiplication des décisions qui témoignent d'un intérêt grandissant pour les questions de défense de la sphère personnelle.

Le délai nécessaire à la prise de décision entrave toutefois le développement de l'économie numérique, dont la Suisse est l'un des fers de lance. Les décisions doivent être prises avec plus de célérité et elles doivent permettre aux acteurs d'en retirer des enseignements transposables dans la pratique.

De ce point de vue, les jugements rendus évoquent trop fréquemment des problématiques sans les résoudre. Les délibérations publiques permettent de constater que les juges ont appréhendé certains aspects sous-jacents des litiges (comme c'est le cas dans l'affaire Logistep de l'application de la loi sur l'investigation secrète), mais qu'ils ne souhaitent pas les traiter. C'est précisément ce qui permettrait aux entreprises d'adapter leurs pratiques et d'éviter ainsi des procès inutiles.

Le rôle de la justice est également prospectif et prophylactique, surtout dans un domaine tel que celui des technologies avancées où la fulgurance est la règle de sorte qu'en toute hypothèse les juristes sont en décalage, si ce n'est à la traîne.