

L'identification par radiofréquence et son impact sur la vie privée des consommateurs en droit européen et droit américain fédéral

Mémoire réalisé par
Adélie Fadeux

Promoteur
Paul Nihoul

Année académique 2013-2014
Master en droit

Plagiat et erreur méthodologique grave

Le plagiat entraîne l'application des articles 87 à 90 du règlement général des études et des examens de l'UCL.

Il y a lieu d'entendre par « plagiat », l'utilisation des idées et énonciations d'un tiers, fussent-elles paraphrasées et quelle qu'en soit l'ampleur, sans que leur source ne soit mentionnée explicitement et distinctement à l'endroit exact de l'utilisation.

La reproduction littérale du passage d'une oeuvre, même non soumise à droit d'auteur, requiert que l'extrait soit placé entre guillemets et que la citation soit immédiatement suivie de la référence exacte à la source consultée.*.

En outre, la reproduction littérale de passages d'une oeuvre sans les placer entre guillemets, quand bien même l'auteur et la source de cette oeuvre seraient mentionnés, constitue une erreur méthodologique grave pouvant entraîner l'échec.

* A ce sujet, voy. notamment <http://www.uclouvain.be/plagiat>.

Merci à Paul Nihoul, promoteur de la présente recherche, pour m'avoir éclairée lors de mes divers questionnements et appris que la rigueur est une vertu inexhaustible.

Merci à Yves Poulet, recteur de L'Université de Namur, professeur et chercheur, pour m'avoir transmis sa passion du droit et m'avoir inspirée dès ma première année sur les bancs de l'université et ce jusqu'à la dernière, par ses recherches au sein du CRIDS.

*Merci à toutes les personnes ayant contribué de loin ou de près à la réalisation de cette
recherche,
et en particulier à Camille, à ma sœur Virginie et à mes parents.*

« Lassée de jouer dans l'herbe du parc, Alice s'assoupit. À l'instant où elle s'endormait, son regard fut attiré par le passage d'un lapin blanc, habillé d'un costume trois pièces de marque et équipé d'une magnifique montre à gousset, qu'il consultait fébrilement. Le lapin s'inquiétait à voix haute : « Je ne vais jamais avoir suffisamment de temps ! ». Intriguée par ce manège et désireuse de lui apporter son aide, Alice décida d'accompagner le lapin...

Arrivée à quelques mètres de son automobile, celui-ci l'ouvrit grâce à une clé RFID. La fillette se permit alors de lui faire remarquer qu'ils gagneraient certainement du temps en prenant les transports en commun. « Qu'à cela ne tienne », répondit le lapin, et ils se dirigèrent vers le bus le plus proche. Une fois montés à bord et enregistrés sur le système par leurs cartes sans contact, les deux compères se dirigèrent vers un centre commercial. Le lapin savait en effet que le dernier album de son groupe préféré, les « Lièvres verts », était dans les bacs, et il souhaitait en acquérir un exemplaire numéroté. L'album dans la besace, ils quittèrent le magasin en jetant un regard à la montre, qui leur conseilla au passage, grâce aux informations de son lecteur RFID, de se rendre dans le magasin de vêtements du centre pour y acquérir le tee-shirt promotionnel des Lièvres verts, qui venait d'être livré, ainsi qu'un chapeau pour Alice, dont la puce implantée signalait un risque d'insolation. Les deux amis décidèrent de ne pas tenir compte de ces conseils. Ils savaient que leurs systèmes embarqués avaient tendance à les pousser à la consommation. En outre, le lapin avait promis à Alice un verre de jus de carottes ainsi qu'une copie de l'album des Lièvres verts, qu'elle ne connaissait pas.

Dans le terrier du lapin, la porte équipée d'un lecteur RFID s'ouvrit automatiquement. Le réfrigérateur fut moins coopératif et lui indiqua qu'il ne pouvait offrir à son invitée le jus promis, la date d'expiration contenue dans l'étiquette électronique de ce dernier étant expirée depuis deux heures. Ils se contentèrent donc d'un verre d'eau et Alice copia le disque du lapin avant de quitter celui-ci, qui devait maintenant recevoir le livreur de jus de carottes, appelé par l'ordinateur central du terrier. Elle ne savait pas, pauvre enfant, que son lecteur de disque refuserait, en l'absence de RFID valable, de lire cette copie... »

STEPHANIE LACOURT – Ubiquitous computing et Droit.

Introduction

Les sociétés dans lesquelles nous vivons ont toujours été dirigées par les personnes détenant le pouvoir... l'information !

Aujourd'hui, l'information la plus complète nous concernant ne se situe plus dans les bases de données de l'Etat mais bien dans celles des commerciaux se trouvant à la tête d'une multinationale ayant pour principal objectif le traitement des données personnelles. Prenons par exemple le cas de ChoicePoint, entreprise qui dispose de plus de 17 billions d'archives concernant les citoyens et les entreprises américaines. Ces données concernent des personnes individualisées. Certes, l'individu moyen a généralement conscience qu'un tel traitement de données le concernant est mis en place : il répond à des questionnaires lorsqu'il sollicite un crédit à la banque, lorsqu'il effectue un achat sur internet, lorsqu'il commande une carte de fidélité, etc. Ces données sont collectées de plus en plus *via* les nouvelles technologies : l'internet, notre smartphone, etc. Cependant, nous ne sommes pas conscients de tous les moyens de collecte dont disposent les entreprises de traitement.

Connaissez-vous la *RFID* ? La *NFC* ?

Ces deux nouvelles technologies de l'information et de la communication sont relatives à l'identification par radiofréquence. Ce sont de petites étiquettes contenant une puce électronique disposées sur la plupart des produits que nous achetons en magasins, sur nos billets de banque, sur notre carte de crédit, ou même insérées dans nos animaux ; et qui divulguent diverses informations à des lecteurs eux-mêmes situés un peu n'importe où : au coin de la rue, à la sortie d'un magasin, à l'entrée du bâtiment de notre lieu de travail. C'est ce qu'on appelle plus communément l'intelligence ambiante ou l'intelligence des objets : ceux-ci n'ont plus besoin de l'intervention de l'homme pour communiquer entre eux.

L'identification par radiofréquence n'est pourtant pas une technologie si nouvelle puisqu'elle a été créée lors de la seconde guerre mondiale afin d'identifier si l'avion qui entrait sur le territoire était un avion ami ou ennemi. Ses possibilités d'application augmentent cependant de manière exponentielle depuis quelques années. Lors d'une conférence sur *The Internet of Things*, organisée par la *Federal Trade Commission* des Etats-Unis, une intervenante a mentionné une étude réalisée par Cisco dans laquelle il était exposé qu'en 2008, il existait plus d'objets connectés entre eux que de personnes sur terre, qu'en 2015, 25 billions d'objets devraient être connectés et qu'ils seraient 50 billions en 2020.

Comprendre cette technologie et les enjeux qu'elle recouvre paraît alors essentiel afin que nous gardions un minimum de contrôle quant à la divulgation des données nous concernant.

Tel est l'objectif de la présente recherche.

Nous tenterons tout d'abord de définir ce qu'est l'identification par radiofréquence tout en expliquant son fonctionnement et ses diverses applications.

Ensuite, nous tenterons d'établir de façon plus au moins exhaustive au vu de la technologie actuelle, les risques que représente l'identification par radiofréquence ainsi que les liens entre ces problématiques et la vie privée, non pas comme droit mais comme valeur.

Enfin, nous analyserons les différentes solutions proposées aux risques inhérents à l'identification par radiofréquence par deux régimes juridiques : celui du droit de l'Union européenne et celui du droit américain fédéral ; afin d'en comparer les éléments essentiels, d'en expliquer les disparités et d'en ressortir une solution meilleure puisque la comparaison de points de vue enrichit inévitablement l'aboutissement d'une recherche.

Titre 1^{er}. Qu'est-ce que l'identification par radiofréquence ?

Afin de tenter de définir ce qu'est l'identification par radiofréquence, il est au préalable nécessaire d'expliquer le processus d'identification mais également d'en présenter les diverses applications.

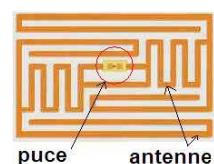
Chapitre 1^{er}. Explication du processus d'identification par radiofréquence

L'identification par radiofréquence est une nouvelle technologie qui permet une identification sans contact¹, c'est-à-dire qu'une personne ou un objet sur lequel est apposée une étiquette d'identification, qui se situe à une distance plus ou moins longue d'un lecteur d'étiquettes, peut être identifié individuellement par celui-ci. Plusieurs questions se sont alors posées : Quel est le fonctionnement d'une telle technologie ? Ce fonctionnement diffère-t-il selon l'application ? Qu'entend-on par la notion d'identification ?

Section 1^{ère}. Le mécanisme

Le mécanisme est simple à première vue. Pour générer une identification par radiofréquence, il est nécessaire de disposer d'une étiquette d'identification et d'un lecteur d'étiquettes.

Une étiquette d'identification peut se présenter entre autres, sous la forme d'une étiquette de supermarché, d'un fil pas plus épais qu'un cheveu, d'un boîtier pas plus grand qu'un smartphone, d'un grain de riz,... Il en existe même de taille plus petite qu'un grain de sel !² Celle-ci contient une antenne et une puce électronique dans laquelle est intégrée une mémoire³. L'étiquette d'identification n'est donc pas une puce d'identification car l'étiquette contient une antenne capable de communiquer avec le lecteur sans contact. Les puces d'identification nécessitent un contact physique avec le lecteur : une carte SIS a besoin d'être insérée dans le lecteur afin de communiquer votre identité à la pharmacie par exemple ; alors qu'une étiquette



¹ A. BENSOUSSAN, *Informatique et libertés*, Levallois, Editions Francis Lefebvre, 2010, p. 278.

² Voy. notamment l'étiquette d'identification d'Hitachi, disponible sur <http://www.hitachi.com/New/cnews/030902.html>, consulté pour la dernière fois le 30 juillet 2014.

³ A. BENSOUSSAN, *op. cit.*, p. 278 ; S. LACOUR, « Ubiquitous computing et Droit : l'exemple de la radio-identification », in *La sécurité de l'individu numérisé : réflexions prospectives et internationales*, Paris, L'Harmattan, 2008, pp. 33-34.

d'identification a seulement besoin de se trouver à proximité d'un lecteur pour lui communiquer les informations.

Un lecteur d'étiquettes peut se rencontrer pour sa part, sous la forme d'un boîtier pas plus grand qu'un livre de chevet, d'un scanner de codes-barres portable, d'un dispositif antivol à la sortie d'un magasin,... C'est un dispositif qui envoie des ondes électromagnétiques autour de lui et, lorsqu'une étiquette se situe dans son champ d'ondes électromagnétiques, elle est détectée *via* son antenne. Le lecteur l'identifie alors à l'aide de l'identifiant qu'elle contient dans sa mémoire⁴ et, le cas échéant, lit les données y figurant.

Le plus souvent, le lecteur d'étiquettes est relié à un ordinateur/serveur qui conserve les données récoltées par celui-ci et les classe.

Il suffit donc qu'une étiquette d'identification se situe à proximité d'un lecteur d'identification pour qu'il y ait une identification par radiofréquence.

Cependant, cette présentation sommaire du mécanisme ne reflète pas la diversité rencontrée tant il existe d'étiquettes d'identification différentes.

Section 2. Les différentes étiquettes

Il existe de nombreuses sortes d'étiquettes en fonction de l'application à laquelle elles sont destinées. En effet, une étiquette apposée sur une marchandise en vue de sa traçabilité ne présentera pas les mêmes caractéristiques que celle apposée sur une carte d'identité.

Elles se distinguent soit par le mode d'alimentation de la puce, par le mode de communication avec le lecteur, par son mode de fonctionnement, par la sécurité accordée à la divulgation du contenu de la mémoire ou encore par la fréquence de l'onde électromagnétique. Ceci complexifie de façon plus ou moins prononcée le mécanisme d'identification : si, par exemple, le contenu de la mémoire est crypté lors de la transmission, le mécanisme d'identification se verra complexifié car le message devra être crypté et décrypté.

De plus, il est possible que plusieurs étiquettes soient présentes dans le champ d'un seul lecteur, ce dernier devra alors être capable d'identifier toutes les étiquettes et de communiquer individuellement avec chacune d'elles⁵.

⁴ S. LACOUR, *op.cit.*, pp. 33-34.

⁵ L. COSTA, *L'identification par radiofréquence et la protection des données à caractère personnel* (multig.), mémoire de master en droit de l'internet public, Université Paris-I Panthéon Sorbonne, 2009, p. 18.

§ 1^{er}. Selon le mode d'alimentation

L'étiquette est soit télé-alimentée, c'est-à-dire qu'elle fonctionne grâce au champ électromagnétique émis par le lecteur ; soit elle fonctionne grâce à l'alimentation par batterie locale, c'est-à-dire qu'elle dispose d'une batterie en son sein⁶.

§ 2. Selon le mode de communication

Une étiquette est dite active lorsqu'elle est apte à produire un signal de radiofréquence car elle dispose d'un émetteur ad hoc ; tandis qu'une étiquette est dite passive lorsqu'elle reflète simplement un signal reçu du lecteur⁷.

§ 3. Selon le mode de fonctionnement

Une étiquette peut faire l'objet d'une lecture et écriture seule ou multiple.

A. La lecture et écriture seule

Par ce mode de fonctionnement, le contenu de l'étiquette est préalablement inscrit de manière définitive dans la mémoire par le fabricant du composant ou par l'utilisateur. Le contenu peut être lu un nombre illimité de fois⁸.

B. Les lectures et écritures multiples

Tout comme le mode de lecture seule, le contenu peut être lu un nombre illimité de fois. A *contrario*, le contenu de l'étiquette n'est pas inscrit de manière définitive mais peut faire l'objet d'une réinscription unique (« mode programmable ») ou multiple (« mode read/write »)⁹.

§ 4. Selon la sécurité accordée à la divulgation du contenu de la mémoire

L'identification par radiofréquence peut fonctionner de diverses manières selon le degré de protection que celle-ci confère à son contenu.

La protection mise en place dans l'étiquette ne nécessite pas d'interaction humaine, c'est-à-dire que si pour être lue, l'étiquette nécessite un mot de passe, un code ou une clé cryptographique, c'est le lecteur qui va le lui fournir sans que la personne ou la chose dans laquelle l'étiquette est intégrée doive l'insérer dans une machine, comme nous en avons l'habitude avec les cartes à puce sans antenne.

⁶ L. COSTA, *op. cit.*, p.17.

⁷ *Idem.*

⁸ *Idem.*

⁹ *Idem.*

A. Les lectures et écritures simples

La simple proximité du lecteur implique la lecture¹⁰.

B. Les lectures et écritures protégées

Ce mode de fonctionnement implique l'accès à un contenu « secret » à un endroit particulier de la mémoire qui est sécurisé par un signe de reconnaissance¹¹. Ce signe de reconnaissance qui peut être un mot de passe par exemple, est une protection rudimentaire car elle peut facilement faire l'objet d'un hackage. Il n'y a aucune authentification de l'identifiant¹².

C. Les lectures et écritures sécurisées

La sécurisation du contenu par ce mode de fonctionnement est plus élevée car elle utilise généralement l'authentification de l'étiquette ou l'utilisation d'un code¹³.

D. Les lectures et écritures cryptées¹⁴

Ce mode de fonctionnement plus sécurisé utilise la cryptographie. Le contenu de la communication entre le lecteur et l'étiquette peut être crypté par des algorithmes de degrés de protections différentes.

La cryptographie est l' « ensemble des techniques de chiffrement qui assurent l'inviolabilité de textes et, en informatique, de données »¹⁵.

D'une part, l'étiquette peut être cryptée de façon symétrique ou autrement appelée cryptographie à clé secrète. Ce mécanisme de cryptage peut être résumé de manière sommaire de la façon suivante : l'étiquette souhaite envoyer au lecteur qui la sollicite l'identifiant qu'elle contient dans sa mémoire. Afin de préserver la sécurité de cet identifiant, l'étiquette et le lecteur utilisent une formule mathématique pour modifier l'identifiant. Une fois l'identifiant modifié, l'étiquette l'envoie ensuite au lecteur qui connaît la formule mathématique pour déchiffrer l'identifiant modifié et identifier l'étiquette. Par exemple, une étiquette pourrait avoir comme identifiant le mot « RFID », la formule de cryptage pourrait

¹⁰ L. COSTA, *op. cit.*, p.18.

¹¹ *Idem.*

¹² Sur la notion d'authentification, voy. *infra* p. 20.

¹³ L. COSTA, *op. cit.*, p.18.

¹⁴ G. ZEMOR, *Cours de cryptographie*, éd. Cassini, Paris, 2000.

¹⁵ Tel que défini dans le dictionnaire Larousse, disponible sur <http://www.larousse.fr/dictionnaires/francais/cryptographie/20864?q=cryptographie#20742>, consulté pour la dernière fois le 30 juillet 2014.

être « le remplacement de chaque lettre par la suivante dans l'alphabet » et donc l'identifiant envoyé serait « SGJE » ; le lecteur recevant cet identifiant connaît la clé secrète a priori, c'est-à-dire la formule de cryptage qu'a utilisée l'étiquette et peut donc retrouver facilement l'identifiant « RFID ». Ce cryptage est moins sécurisé que la cryptographie à clé publique, car une fois la clé secrète découverte par une entité externe, tous les messages cryptés pourront être lus de manière compréhensible.

D'autre part, l'étiquette peut être cryptée de façon asymétrique ou cryptographie à clé publique. Dans ce mécanisme de cryptage de messages, il existe deux clés : l'une secrète, l'autre publique. Il peut être résumé de la façon suivante : l'étiquette souhaite envoyer au lecteur qui la sollicite l'identifiant qu'elle contient dans sa mémoire. Afin de préserver de manière certaine la sécurité de cet identifiant, le lecteur et l'étiquette utilisent une formule mathématique beaucoup plus compliquée que celle de la cryptographie symétrique. À partir d'une première formule mathématique (la clé privée), connue par le lecteur seulement, ce dernier va créer une seconde formule mathématique (la clé publique) qu'il va envoyer à l'étiquette. L'étiquette va se servir de cette clé publique pour modifier l'identifiant et l'envoyer ensuite au lecteur. Le lecteur, connaissant la formule mathématique pour décrypter l'identifiant modifié pourra alors identifier l'étiquette. Ce mécanisme se base sur le principe que la formule de cryptage de la clé publique étant si complexe, il est impossible de savoir comment décrypter l'identifiant sans connaître la clé secrète. Un des systèmes de cryptage asymétrique les plus connus est le système RSA¹⁶. Afin de réaliser la complexité du cryptage asymétrique d'un identifiant, voici un exemple suivant cette méthode RSA pour l'identifiant « RFID ».

1. Le lecteur crée ses clés :

- La clé secrète : $p = 53$ et $q = 97$ (p et q sont des nombres premiers mais en réalité, ils devraient contenir plus de 100 chiffres)
- La clé publique : $e = 7$ (où $e =$ un entier premier strictement inférieur à $(p-1).(q-1)$, soit 52.96) et $n = p.q = 53.97 = 5141$

2. Le lecteur envoie sa clé publique (n,e) , à savoir $(7, 5141)$ à l'étiquette.

¹⁶ G. ZEMOR, *op.cit.*

3. L'étiquette chiffre d'abord son message en remplaçant chacune des lettres de l'identifiant par son nombre correspondant dans l'alphabet :

$$R=18 \quad F=6 \quad I=9 \quad D=4$$

→ RFID : 18 6 9 4

4. L'étiquette crée ensuite des blocs de même longueur, chacun représentant un nombre plus petit que n.

→ RFID : 01 86 94

5. L'étiquette chiffre chacun des blocs que l'on note B par la transformation $C = B^e \bmod n$ (où C est le bloc chiffré) :

$$C_1 = 1^7 \bmod 5141 = 1$$

$$C_2 = 86^7 \bmod 5141 = 32$$

$$C_3 = 94^7 \bmod 5141 = 432$$

→ RFID : 13 42 32

6. L'étiquette envoie au lecteur le message « 13 42 32 ».

7. Le lecteur qui reçoit le message « 13 42 32 » le déchiffre de la façon suivante : le lecteur chiffre chacun des blocs que l'on note C par la transformation $M = C^d \bmod n$ tel que $e.d = 1 \bmod [(p-1).(q-1)]$. Même en connaissant la clé publique, il est impossible à une entité extérieure de retrouver l'identifiant « RFID » puisque pour déchiffrer le message envoyé il est nécessaire de connaître la clé privée (p,q).

§ 5. Selon la fréquence de l'onde électromagnétique¹⁷

Les lecteurs d'identification par radiofréquence peuvent disposer de quatre types de fréquence d'ondes électromagnétiques de divers hertz. La fréquence dont dispose le lecteur détermine la distance de lecture possible entre celui-ci et l'étiquette, le nombre de lectures simultanées possibles ou encore la capacité de transfert des données.

¹⁷ S. LACOUR, *op.cit.*, pp. 34-35.

A. Les lecteurs basse fréquence

Ces lecteurs utilisant une fréquence d'environ 135 kHz ne bénéficient que d'un champ de lecture de 50 centimètres et ne peuvent transférer que peu de données.

B. Les lecteurs haute fréquence

Ces lecteurs utilisant une fréquence d'environ 13,6 MHz bénéficient d'un champ de lecture de 1 mètre et d'une plus ample capacité de données.

C. Les lecteurs ultra-haute fréquence

Ces lecteurs utilisant une fréquence de 863 à 915 MHz ont la possibilité de lire simultanément jusqu'à 200 autres étiquettes et sont donc plus intéressants d'un point de vue logistique.

D. Les lecteurs de type micro-ondes

Ces lecteurs utilisant une fréquence de 2,45 GHz à 5,4 GHz permettent une distance de lecture de plusieurs dizaines de mètres.

Section 3. La notion d'identification

La notion d'identification est au centre de la technologie d'identification par radiofréquence car la mission première d'une étiquette est de permettre d'identifier la chose ou la personne à laquelle elle est intégrée¹⁸.

Dans le domaine de l'identification par radiofréquence, le terme identification recouvre autant la notion d'identification au sens de déclarer un identifiant que celle d'authentification qui permet de vérifier l'authenticité de cet identifiant¹⁹. Il est dans certains cas, indispensable de garantir l'authenticité de l'identifiant comme dans le cas d'une pièce d'identité, d'un vêtement de luxe, etc. alors que dans d'autres, le risque d'usurpation d'identité est faible et une simple identification suffit²⁰.

¹⁸ X., « RFID : instrument de sécurité ou de surveillance ? », *MISC : Multi-system & Internet security Cookbook*, n°33, septembre-octobre 2007, p. 40.

¹⁹ *Ibidem*, pp. 40-43.

²⁰ *Ibidem*, p. 40.

§ 1^{er}. L'identification

L'identifiant de l'étiquette se situe dans sa mémoire. Il s'agira par exemple d'un numéro de série d'un dvd, de l'identité d'une personne dans une carte de transport ou carte bancaire, le numéro de série d'un smartphone²¹.

§ 2. L'authentification

On en distingue deux degrés : l'authentification faible et l'authentification forte.

Toutes deux ont la possibilité d'utiliser la cryptographie symétrique ou asymétrique²² pour authentifier les identifiants.

Le mécanisme d'authentification est additionnel au mécanisme de sécurité qui protège l'étiquette de la divulgation de son identifiant, il se peut donc très bien qu'une étiquette contienne deux mécanismes de clé cryptographique : l'une pour la divulgation de l'identifiant et l'autre pour l'authentification de l'identifiant.

A. L'authentification faible

L'identifiant présent dans la mémoire de l'étiquette est assorti d'une valeur d'authentification qui ne varie pas avec le temps. Le protocole de contrôle d'accès « *login-password* » est l'exemple type de mécanisme d'authentification faible²³. Ce mécanisme est dit faible car il est susceptible d'être intercepté par un ennemi et réutilisé à des fins d'usurpation.

B. L'authentification forte

L'identifiant est dans ce cas-ci assorti d'une valeur d'authentification qui n'est jamais la même car elle résulte d'un calcul dans lequel une des données est une valeur aléatoire, ce qui renforce l'authenticité de l'identifiant²⁴.

²¹ G. AVOINE, « Sécurité de la RFID : comprendre la technique sans être un technicien », in *La sécurité de l'individu numérisé : réflexions prospectives et internationales*, (sous la dir. de S. LACOUR), Paris, L'Harmattan, 2008, pp. 19-20.

²² Voy. *supra* pour les notions de cryptographies, pp. 16 et s.

²³ X., « RFID : instrument de sécurité ou de surveillance ? », *op. cit.*, p. 42 ; G. AVOINE, *op.cit.*, pp. 20-21.

²⁴ *Idem*.

Chapitre 2. Diverses applications de l'identification par radiofréquence

On peut retrouver des étiquettes d'identification à de nombreux endroits et pour de nombreuses raisons également, en voici une liste non-exhaustive.

Section 1^{ère}. L'identification des objets

§ 1^{er}. La logistique en entreprise

Les entreprises utilisent les étiquettes afin de tracer de façon certaine les marchandises dans les chaînes de production interne et externe²⁵. Dans la chaîne interne, il suffit de programmer les machines pour trier chaque composant de la marchandise par étiquettes afin de les diriger vers les chaînes de montage. Dans la chaîne externe, l'entreprise peut suivre le transport de ses marchandises par les différents services d'acheminement jusqu'à la réception par le détaillant.

§ 2. La lutte contre la contrefaçon

Si sur l'objet original, il est apposé une étiquette et non sur l'objet contrefait, la lutte contre la contrefaçon est d'autant plus efficace. On peut retrouver des étiquettes d'identification sur des billets de banque, des objets de luxe ou encore des médicaments²⁶.

§ 3. La gestion des bibliothèques

De plus en plus de bibliothèques disposent de la technologie d'identification par radiofréquence pour gérer la location et le rangement des bouquins²⁷. Grâce à cette technologie, plus aucun livre ne peut être volé sans retirer l'étiquette et les livres perdus au sein de la bibliothèque sont une histoire ancienne puisque chaque livre est identifiable et traçable.

§ 4. La domotique

La domotique est l'ensemble des techniques qui permet l'interconnexion des divers équipements au sein d'une maison de façon à les faire communiquer entre eux afin d'en

²⁵V. FOSSOUL, « RFID et biométrie : état des lieux », in *Actualités du droit de la vie privée* (sous la dir. de B. DOCQUIR et A. PUTTEMANS), Bruxelles, Bruylant, 2008, p. 146 ; D. DARQUENNES et Y. POULLET, « RFID : quelques réflexions introductives à un débat de société », *R.D.T.I.*, n°26/2006, p. 261.

²⁶A. BENSOUSSAN, *op. cit.*, p.278.

²⁷*Idem.*

multiplier les services²⁸. Par exemple, un lecteur d'étiquettes peut aujourd'hui être intégré dans un réfrigérateur et lire les étiquettes des aliments présents à l'intérieur de celui-ci afin de savoir si les aliments sont périmés ou non²⁹. De même, vous pouvez suivre sur Twitter le compte de la maison des Coats, maison interconnectée qui d'elle-même poste des tweets sur le temps qu'il fait et les occupations des membres de la famille repérables *via* l'identification par radiofréquence³⁰.

§ 5. L'antivol

Les étiquettes ont pour but de remplacer à terme les codes-barres figurant sur tous les produits car la traçabilité est beaucoup plus aisée³¹. On peut retrouver aujourd'hui des étiquettes d'identification sur les dvd ou cd, par exemple.

§ 6. Le contrôle d'identité

Les étiquettes présentes dans les nouvelles cartes d'identité ou les passeports permettent d'authentifier l'identité de la personne *via* un identifiant ou des données biométriques contenues dans sa mémoire³².

Section 2. L'identification des êtres vivants

§ 1^{er}. L'identification de tous les animaux domestiques ou non

Une étiquette est insérée dans tous les animaux d'élevage³³ ainsi que dans la plupart des animaux domestiques³⁴. Elle permet la traçabilité de la viande pour les animaux d'élevage mais contient aussi les antécédents médicaux pour les animaux domestiques.

§ 2. L'identification des êtres humains

De nos jours, peu de personnes se sont fait insérer des étiquettes d'identification sous-cutanées. Il existe cependant des étiquettes d'identification sous forme de bracelet qui peuvent être intéressantes dans divers domaines :

²⁸ Tel que défini dans le dictionnaire Larousse, disponible sur <http://www.larousse.fr/dictionnaires/francais/domotique/26402?q=domotique#26280>, consulté pour la dernière fois le 30 juillet 2014.

²⁹ J. DANIEL, « RFID-INES : la police totale », mai 2006, p. 5, disponible sur http://infokiosques.net/article.php3?id_article=349, consulté pour la dernière fois le 30 juillet 2014.

³⁰ Disponible sur <https://twitter.com/houseofcoates>, consulté pour la dernière fois le 30 juillet 2014.

³¹ A. BENSOUSSAN, *op. cit.*, p. 278 ; D. DARQUENNES et Y. POULLET, *op. cit.*, p. 261.

³² Des données biométriques sont par exemple une empreinte digitale, le son d'une voix, les particularités faciales,...

³³ X., « RFID intégrables pour animaux », disponible sur <http://www.hidglobal.fr/products/rfid-tags/identification-technologies/rfid-integrables-pour-animaux>, consulté pour la dernière fois le 30 juillet 2014.

³⁴ Voy. notamment la base de données qui enregistre les chiens en Belgique, disponible sur <http://www.abiec-bvirh.be>, consulté pour la dernière fois le 30 juillet 2014 ; dans laquelle sont disponibles les informations concernant l'animal mais également les coordonnées du propriétaire (identité, adresse et numéro de téléphone).

A. Le suivi des enfants à la maternité

Afin d'éviter l'échange de nouveau-nés, certaines cliniques disposent de bracelets d'identification dans lesquels sont répertoriés l'identité du bébé mais également des renseignements médicaux ou alimentaires³⁵.

B. L'aide aux personnes âgées

Plusieurs entreprises proposent au consommateur lambda tout un système d'identification par radiofréquence à installer chez une personne âgée vivant seule. Ce système se base sur l'enregistrement d'une routine journalière que la personne âgée effectue (divers lecteurs sont placés un peu partout dans la maison et s'activent dès que le bracelet porté par la personne âgée est à proximité) et dès qu'il y a une différence trop importante entre une journée et l'enregistrement d'une journée-type, l'ordinateur central prévient la famille ou les secours³⁶.

C. Les informations médicales

Une tendance à vouloir insérer une étiquette sous-cutanée à toute la population d'un pays afin d'y répertorier les antécédents médicaux et volontés thérapeutiques circule depuis quelques années sur la toile. Une telle insertion serait d'une efficacité redoutable en cas d'accident grave, la personne inconsciente pourrait bénéficier des meilleurs soins des médecins ne disposant pas de ses papiers d'identité, mais bien de toutes les informations médicales nécessaires présentes dans l'étiquette³⁷.

D. L'entrée dans les boîtes de nuit

Plusieurs boîtes de nuit utilisent le concept d'identification par radiofréquence afin de répondre au mieux aux besoins du client³⁸.

³⁵ H. PUEL, « Des bracelets électroniques pour empêcher le vol des nouveaux nés », disponible sur <http://www.01net.com/editorial/345930/mise-a-jour-des-bracelets-electroniques-pour-empêcher-le-vol-de-nouveau-nés/#forum>, consulté pour la dernière fois le 30 juillet 2014.

³⁶ K. FISHKIN et J. LUNDELL, « RFID in Healthcare », in *RFID, Applications, Security, and Privacy* (sous la dir. de S. GARFINKEL et B. ROSENBERG), Upper Saddle River, New Jersey, Addison-Wesley, 2006, pp. 211-226.

³⁷ L. REDON (sous la dir. de), *L'identification par radiofréquence*, disponible sur http://www.centrenational-rfid.com/docs/users/file/CNRFID_collusers_final_v2.pdf, consulté pour la dernière fois le 30 juillet 2014 ; V. FOSSOUL, « RFID et biométrie : état des lieux », *op.cit.*, p. 148.

³⁸ Voy. le cas de la discothèque Baja Beach Club implantée au Pays-Bas et en Espagne, disponible sur <http://www.courrierinternational.com/article/2004/06/03/une-puce-electronique-sous-la-peau-pour-entrer-en-discotheque>, consulté pour la dernière fois le 30 juillet 2014.

E. Le pointage

Diverses entreprises font appel à l'identification par radiofréquence afin de contrôler les heures de prestations de travail. Un lecteur est par exemple placé à l'entrée/sortie du bâtiment, un autre à la cafeteria, un autre à la machine à café, etc. Le même procédé est utilisé dans certaines garderies afin d'être certain du nombre d'heures à facturer aux parents.

Section 3. L'identification comme moyen de paiement

§ 1^{er}. Comme moyen de paiement traditionnel

Presque toutes les nouvelles cartes de banque disposent d'une étiquette d'identification par radiofréquence³⁹. Il suffit alors d'être à proximité du lecteur pour payer sa consommation sans même devoir sortir sa carte de banque de son portefeuille.

§ 2. Comme moyen de paiement dans les transports

Tant dans les transports en commun (Carte vélib', carte Mobib, installation de ski,...)⁴⁰ que dans les transports privés (péage des autoroutes à distance)⁴¹, les étiquettes d'identification par radiofréquence sont d'utilisation courante.

³⁹ Voy. notamment la carte sans contact de la banque postale française, disponible sur https://www.labanquepostale.fr/particulier/produits/quotidien/cartes/internationales/sans_contact.caracteristiques.html, consulté pour la dernière fois le 30 juillet 2014.

⁴⁰ L. REDON, *op. cit.*

⁴¹ Voy. notamment le péage du Colorado E-470, disponible sur <http://www.filrfid.org/article-rfid-uhf-passive-pour-les-payages-autoroutiers-aux-us-121462290.html>, consulté pour la dernière fois le 30 juillet 2014.

Chapitre 3. Tentative de définition

Suite à la présentation sommaire de la technologie d'identification par radiofréquence, il paraît opportun de tenter de la définir afin d'analyser par la suite la problématique qu'elle implique.

L'identification par radiofréquence est une nouvelle technologie de l'information et de la communication par laquelle une étiquette apposée sur un objet ou une personne communique les données présentes dans sa mémoire interne *via* des ondes électromagnétiques, à un lecteur qui identifie l'étiquette et les données qu'elle contient.

Cette communication peut être sécurisée ou non, authentifiée ou non. Elle peut avoir lieu dans un champ électromagnétique restreint ou étendu. L'étiquette peut disposer de sa propre batterie ou fonctionner grâce à la sollicitation externe du lecteur uniquement. L'étiquette peut se contenter de répondre à une sollicitation du lecteur ou solliciter elle-même le lecteur. Le contenu de sa mémoire peut faire l'objet de modifications ou peut être prédéfini.

Bref, l'identification par radiofréquence est une technologie extrêmement vaste et peut se rencontrer sous diverses formes, il n'en reste pas moins que l'identification par radiofréquence, quelle qu'elle soit, identifie tant la personne que l'objet sur lequel elle est apposée et qui appartient la plupart du temps à une personne.

Cette problématique fait l'objet du deuxième titre de la présente recherche.

Titre 2. Quelle est la problématique de l'identification par radiofréquence ?

Comme exposé au titre premier, l'identification par radiofréquence se rencontre sous diverses formes dans nos sociétés mais sont-elles toutes problématiques ?

Si l'identification par radiofréquence est uniquement destinée à la logistique au sein d'une entreprise et si l'étiquette est désactivée à la fin du processus interne à l'entreprise ou au groupe d'entreprises, l'identification par radiofréquence ne pose alors aucun problème et est au contraire une aide précieuse et un gain de temps considérable pour les entrepreneurs. En pratique cependant, peu d'entreprises désactivent les étiquettes d'identification apposées sur leurs produits.

A contrario, dès qu'une personne physique détient une étiquette d'identification non-désactivée et donc capable de divulguer les informations contenues dans sa mémoire, le problème de la protection des données incluses dans l'étiquette se pose. On entend par le verbe détenir, tant la détention directe d'une étiquette insérée dans le corps d'une personne physique que la détention indirecte d'une étiquette *via* un objet que la personne physique a en sa possession. L'individu n'est pas obligatoirement le propriétaire de l'étiquette, son employeur pourra l'être s'il s'agit d'un badge d'entrée aux locaux, le magasin d'alimentation si l'étiquette est apposée sur le caddie pour enregistrer le parcours du consommateur,...

Par-là, nous restreignons notre recherche aux étiquettes non-désactivées possédées par une personne physique.

Dans le présent titre, nous tenterons de répondre à la question de savoir quelles sont les particularités de la collecte de données issues de l'identification par radiofréquence et présenterons en quoi ces particularités posent problème face à la notion de « vie privée » après avoir donné un historique d'évolution de cette dernière.

Chapitre 1^{er}. La collecte des données...à caractère personnel ?

L'objectif premier de l'identification par radiofréquence est d'identifier l'étiquette que le lecteur sollicite. Par cette identification, le lecteur collecte les données présentes dans la mémoire de l'étiquette. Dans le présent chapitre, nous définirons tout d'abord ce qu'est une collecte de données issues de l'identification par radiofréquence pour ensuite expliquer les moyens par lesquels ces données sont collectées et les risques y afférents.

Section 1^{ère}. Notion

Afin de définir de façon rigoureuse la notion de collecte des données issues de l'identification par radiofréquence, il convient de préciser ce qu'est une « collecte », quelles « données » sont concernées et enfin se poser la question du « caractère personnel » ou non de ces dernières.

§ 1^{er}. La collecte...

Le dictionnaire Larousse définit la notion de collecte par la « réunion des informations nécessaires à l'établissement d'une série statistique », « réunion de choses »⁴².

Dans le cadre de l'identification par radiofréquence, la collecte se fait par des lecteurs d'étiquettes. Ceux-ci enregistrent tous les identifiants et toutes les données présentes dans les étiquettes pouvant être reliés à une personne physique. Par exemple, un lecteur disposé à l'entrée d'un magasin lit les identifiants et données de toutes les étiquettes présentes dans votre environnement immédiat et assemble toutes ces étiquettes dans un dossier. De cette manière, les données sont collectées, réunies.

§ 2. ...de données...

Une donnée est « ce qui est connu ou admis comme tel, sur lequel on peut fonder un raisonnement, qui sert de point de départ pour une recherche »⁴³. Les données issues de l'identification par radiofréquence sont les identifiants des étiquettes, les diverses informations divulguées qui étaient présentes dans la mémoire mais aussi les données GPS qu'une telle technologie peut impliquer. En effet, si des dispositifs de lecture sont placés à l'entrée/sortie des magasins d'un centre commercial, l'identification par radiofréquence

⁴² Tel que défini par le dictionnaire Larousse, disponible sur <http://www.larousse.fr/dictionnaires/francais/collecte/17166?q=collecte#17038>, consulté pour la dernière fois le 30 juillet 2014.

⁴³ Tel que défini par le dictionnaire Larousse, disponible sur <http://www.larousse.fr/dictionnaires/francais/donn%C3%A9e/26436?q=donn%C3%A9e#26312>, consulté pour la dernière fois le 30 juillet 2014.

fournira également des données telles que les magasins visités, le temps passé dans chaque magasin, voire dans chaque rayon⁴⁴.

§ 3. ...personnelles ou non ?

La question de savoir si les données issues de l'identification par radiofréquence peuvent être caractérisées comme personnelles ou non est essentielle.

En doctrine européenne, l'approche de qualification nous semble trop confinée dans la sphère juridico-légale. Certes, un juriste étudie le droit mais afin de le faire évoluer⁴⁵, ce dernier ne peut s'enfermer dans des définitions issues des lois, *in casu* la directive générale 95/46/CE. Tout au plus, en définissant un concept *via* une disposition législative et ses arrêts interprétatifs, le juriste analyse si cette disposition s'applique ou non au concept. Il détermine alors le champ d'application d'une disposition mais ne définit pas une notion. Ce n'est pas parce qu'une loi, au jour d'aujourd'hui, ne s'applique pas à un cas déterminé que l'on peut affirmer que ce cas n'a pas les caractéristiques requises pour bénéficier d'une protection légale identique. De même, interpréter extensivement une loi pour y soumettre de nouveaux cas d'application ne résout parfois pas les enjeux de ceux-ci. Les lois sont en effet des compromis, des balances d'intérêts entre différentes parties afin de contenter le plus grand nombre. Par conséquent, il peut arriver qu'un cas d'espèce soit exclu du champ d'application d'une loi. La définition de celui-ci diffère-t-elle cependant en fonction de cette balance d'intérêts ? De notre point de vue, la réponse devrait être non. La définition du concept devrait être identique, et l'application ou non de la loi devrait être justifiée non pas par une définition tronquée mais par des justificatifs de la balance d'intérêts en jeu.

D'une part, Yves Poullet, notamment, conclut que les données issues de l'identification par radiofréquence ne peuvent être qualifiées de données à caractère personnel car elles se rapportent à des objets⁴⁶. Nous sommes en désaccord avec son analyse⁴⁷.

D'autre part, le Groupe de l'article 29 interprète extensivement la notion de données à caractère personnel prévue dans la directive 95/46/CE afin d'y faire rentrer celles issues de

⁴⁴ J.F. HENROTTE et Y. POULLET, « La protection des données (à caractère personnel) à l'heure de l'Internet », in *Protection du consommateur, pratiques commerciales et TIC [technologies-information-communications]* (sous la dir. de J. LAFFINEUR), Liège, Anthémis, 2009, pp. 197-244.

⁴⁵ En particulier dans le domaine des nouvelles technologies où la législation est presque toujours en retard par rapport à l'évolution technologique.

⁴⁶ Y. POULLET, « Pour une troisième génération de réglementation de protection des données », in *Défis du droit à la protection de la vie privée* (sous la dir. de M. VERONICA et P. PALAZZI), Bruxelles, Bruylant, 2008, p. 31.

⁴⁷ Voy. *infra* pp. 30 et s.

l'identification par radiofréquence⁴⁸. Bien que l'interprétation soit rigoureusement juste, elle est toujours fonction d'une disposition législative et n'a pas de portée autonome, ce que nous critiquons⁴⁹.

De notre point de vue, il convient alors de se demander ce qu'est une donnée personnelle ou une donnée à caractère personnel sans passer uniquement par la définition d'une législation. Cette approche de définition est d'autant plus cohérente que la présente recherche est un travail de comparaison entre deux systèmes et régimes juridiques et, définir l'un des concepts clés en fonction de la législation de l'un d'eux seulement reviendrait à fausser ladite comparaison.

Une donnée est personnelle lorsqu'elle est relative à une personne⁵⁰, se rapporte à elle. Une étude comparative menée dans 36 pays a en effet démontré qu'une donnée personnelle est « *a data or an information relating to an identifiable person directly or indirectly* »⁵¹. Une donnée issue de l'identification par radiofréquence sera donc personnelle lorsqu'elle sera en lien avec une personne, le lien pouvant être direct ou indirect. Or, la plupart des étiquettes d'identification sont possédées par des personnes physiques (hormis, entre autres, les cas de désactivation lors de la fin de la chaîne de production et l'étiquetage des animaux d'élevage).

Mais la possession d'un objet sur lequel est apposée une étiquette implique-t-elle une relation entre la donnée incluse dans la mémoire de l'étiquette et la personne ? Pour répondre à cette question, il est nécessaire d'étudier au cas par cas s'il existe ou non une relation en fonction du traitement des données. En effet, dans certains cas, vous ne posséderez qu'une étiquette d'identification lors de la lecture : vous êtes en vacances, vous vous rendez au magasin sans portefeuille et en maillot de bain dont vous avez coupé l'étiquette et achetez une bouteille de jus de fruit avec de la monnaie. La seule étiquette lue en sortant du magasin sera celle de la bouteille de jus de fruit et celle-ci ne pourra pas être mise en lien avec la personne. La clarté de la solution s'obscurcit si des lecteurs sont placés dans chaque rayon du magasin et calculent le temps qu'une personne achetant une telle bouteille de jus de fruit passe dans

⁴⁸ GROUPE DE L'ARTICLE 29, « Avis 4/2007 sur le concept de données à caractère personnel », W.P. 136, 20 juin 2007.

⁴⁹ Voy. *infra* pp. 30 et s.

⁵⁰ Tel que défini par le dictionnaire Larousse, disponible sur <http://www.larousse.fr/dictionnaires/francais/personnel/59814?q=PERSONNEL#59449>, consulté pour la dernière fois le 30 juin 2014.

⁵¹ W. B. BAKER, « The changing meaning of « personal data » », disponible sur <http://www.wileyrein.com/publications.cfm?sp=articles&id=6926>, consulté pour la dernière fois 30 juin 2014.

chaque rayon. Mais cela n'implique toujours pas une relation entre ces données et la personne que vous êtes, identifiable parmi d'autres⁵².

Il est cependant nécessaire de se rendre à l'évidence que la plupart du temps, nous ne nous baladons pas en maillot de bain dans une supérette au bord de la plage, mais bien avec nos papiers : carte d'identité, carte(s) de banque, carte(s) de fidélité, etc. Ces cartes ont la capacité de nous identifier en communiquant leur identifiant au lecteur (peu d'étiquettes d'identification bénéficient de protection de sécurité de bonne qualité, le coût d'une protection étant conséquent)⁵³. Et quand bien même avons-nous laissé notre portefeuille à la maison, il suffit d'une montre, d'un bijou ou d'un GSM porteur d'une étiquette pour être identifiable par le lecteur. En effet, si lors de chacun de nos passages devant le lecteur, ce dernier collecte l'identifiant de notre carte d'identité, de fidélité ou de banque mais également l'identifiant de notre montre, alliance, collier ou GSM et peu importe l'oubli de cartes, lors de notre passage nous serons identifiables *via* les objets identifiés précédemment et contenus dans notre dossier de données sur le serveur.

Les données issues de l'identification par radiofréquence ne doivent pas dès lors, être analysées par étiquettes mais comme un tout, un ensemble de données issues de différentes étiquettes et lues par un même lecteur permettant l'identification d'un individu. Cette exigence de globalité est nécessitée par l'ubiquité de l'identification par radiofréquence⁵⁴. À quoi bon se borner à vouloir analyser la qualification des données présentes dans les différentes étiquettes de manière séparée alors que celles-ci formeront ensemble la base de données permettant ou non l'identification d'une personne ?

Il est en effet aisé d'énoncer que les données présentes dans une étiquette d'identification apposée sur un morceau de fromage n'ont aucune relation avec une personne physique et ne peuvent donc être qualifiées de données personnelles. Cependant, si ce morceau de fromage fait partie d'un tout, d'une liste de courses établie ; en passant à la caisse, le magasin d'alimentation a la possibilité de créer votre profil de consommateur⁵⁵ identifiable grâce à votre carte de fidélité, de banque ou d'identité, peu importe que vous la présentiez ou non au caissier. Ce morceau de fromage et pas un autre est alors relié à votre profil de

⁵² Notez que le Groupe de l'article 29, explique la condition d'identification comme la possibilité pour une personne d'être distinguée par rapport à d'autres dans un groupe, *in casu*, la personne pourrait être distinguable des autres consommateurs dans la supérette. Voy. GROUPE DE L'ARTICLE 29, « Avis 4/2007 sur le concept de données à caractère personnel », *op.cit.*, pp. 13 -24.

⁵³ G. AVOINE, *op. cit.*, pp. 17-27.

⁵⁴ Y. POULLET et J.F. HENROTTE, *op. cit.*, pp. 220-222.

⁵⁵ *Ibidem*, pp. 204-205.

consommation. Certes, cela pose-t-il véritablement problème que quiconque sache que vous appréciez le gouda mi-vieux plutôt que le gouda jeune ? Probablement pas. Que vous ayez pris 27 secondes à choisir votre fromage ? Probablement pas non plus. Mais qu'en est-il si l'étiquette était disposée sur un bouquin concernant les terreurs nocturnes ? Cela poserait-il problème que quiconque sache que vous souffrez de tels traumatismes ? Et si l'étiquette se trouvait sur votre médicament diabétique ou cancéreux ? Et si cette étiquette n'était pas seulement lue par le magasin où vous achetez l'objet mais également par le lecteur du supermarché au coin de la rue ? Par le lecteur de votre employeur ? Par un quidam disposant d'un lecteur ?

L'identification par radiofréquence est une technologie complexe aux applications multiples et variées. Partir du postulat que les données issues de cette technologie ne sont pas des données à caractère personnel nous semble erroné de même que considérer que les données issues de l'identification par radiofréquence sont identiques à celles issues des canaux d'informations ancestraux.

De plus en plus d'objets sont de nos jours porteurs d'étiquettes qui font rarement l'objet d'une protection satisfaisante. Les données présentes dans l'environnement direct d'une personne sont alors lisibles par quiconque disposant d'un lecteur.

Certes, il importe peu au consommateur que certaines données relatives à sa consommation soient collectées mais ces données couplées à d'autres peuvent lui poser problème et sont donc ressenties comme « personnelles » aux yeux du consommateur.

Les données issues de l'identification par radiofréquence constituent donc des données à caractère personnel au sens que leur collecte et le rassemblement de chacune d'elles en un tout, une base de données organisée ; impliquent la possible identification d'une personne physique de manière directe ou indirecte, en fonction de la possession d'une étiquette divulguant ou non l'identité de la personne physique.

Section 2. Moyens

Les moyens de collecte des données à caractère personnel sont importants aux yeux du consommateur. Une étude a été réalisée en ce sens par Caroline Lancelot dans laquelle elle conclut qu'afin que les personnes physiques aient une attitude positive envers la sollicitation de leurs données personnelles, il est nécessaire de réunir trois conditions : la personne doit être informée de la collecte et de ses suites, elle doit avoir donné son consentement préalable

et avoir la possibilité de s'opposer à la collecte et enfin, avoir confiance en l'entreprise pour se sentir dans un environnement sécurisé⁵⁶.

La collecte des données issues de l'identification par radiofréquence ne remplit pas ces conditions ; bien au contraire, les données sont collectées de manière invisible, indéfinie et par n'importe qui. Le sentiment de l'individu face à cette technologie est alors négatif.

§ 1^{er}. De manière invisible

Le mécanisme de l'identification par radiofréquence⁵⁷ implique une collecte invisible des données. Tant le matériel nécessaire pour la collecte qui est ridiculement petit ou dissimulé que le fonctionnement en lui-même qui est sans contact, n'informent pas l'individu de la collecte et en exigent encore moins le consentement. L'individu n'a pas conscience de l'identification due à cette invisibilité de double niveau.

§ 2. De manière indéfinie

À moins que l'étiquette ne soit désactivée ou qu'elle ne fasse l'objet d'une lecture seule, c'est-à-dire que la mémoire soit programmée pour être lue une et une seule fois⁵⁸ ; l'étiquette divulguera les données présentes dans sa mémoire de façon indéfinie dans le temps. Une limite d'alimentation pourrait toutefois exister pour les étiquettes autoalimentées qui s'arrêtent de fonctionner lorsqu'elles n'ont plus de batterie. Elles sont cependant moins nombreuses sur le marché que les étiquettes alimentées par le champ électromagnétique du lecteur car leur coût est plus important⁵⁹.

Cette identification a pour conséquence que l'individu oublie au fil du temps qu'il possède des objets porteurs d'étiquettes d'identification. Les conditions d'information et de consentement sont mises à mal.

§ 3. De manière interoperable

À moins que l'étiquette fasse l'objet d'une protection satisfaisante du contenu, ce qui augmente également le coût de l'étiquette et ralentit donc son développement à l'avantage des étiquettes non-protégées ou protégées de façon rudimentaire ; l'étiquette divulguera les

⁵⁶ C. LANCELOT MILTGEN, « Vie privée et internet : influence des caractéristiques individuelles et situationnelles sur les attitudes et les comportements des internautes face à la collecte de données personnelles », *Cahier de Recherche DMSP n°317 et Actes du Congrès AFM Tunis 2003*, disponible sur <http://basepub.dauphine.fr/bitstream/handle/123456789/4259/CR317.pdf?sequence=1>, consulté pour la dernière fois le 30 juillet 2014.

⁵⁷ Voy. *supra* pp. 13-14.

⁵⁸ Cas rares dans la pratique.

⁵⁹ G. AVOINE, *op. cit.*, pp. 17-27.

données présentes dans sa mémoire à n'importe quel lecteur qui en fera la demande. L'interopérabilité de l'identification par radiofréquence est la « capacité de matériels, de logiciels ou de protocoles différents à fonctionner ensemble et à partager des informations »⁶⁰. Un lecteur d'identification par radiofréquence est un objet accessible à tout public, vendu d'ailleurs par Amazon au prix de 74 euros⁶¹. Quiconque peut alors lire la plupart des données présentes sur les étiquettes qu'une personne possède⁶². La condition de confiance en le collecteur des données n'est clairement pas remplie.

Section 3. Risques

La collecte des données présente également des risques inhérents à celle-ci en plus de ceux présentés ci-dessus afférents aux moyens de collecte.

§ 1^{er}. La localisation des données

L'identification par radiofréquence est une nouvelle technologie dite sans-contact, l'identification a lieu dans le champ électromagnétique du lecteur. Par conséquent, la localisation de l'identification et donc des données, est possible car elles se situent dans le champ électromagnétique. Aussi, si une personne (physique ou morale) dispose de plusieurs lecteurs d'étiquettes, il lui est possible de tracer le parcours effectué par l'objet sur lequel est apposée l'étiquette.

Cette localisation présente un risque de contrôle d'une personne soit sur l'endroit où vous vous trouvez, soit sur le chemin que vous empruntez⁶³. Par exemple, votre employeur via votre badge d'entrée dans l'établissement, peut suivre vos mouvements tout au long de la journée et contrôler le temps que vous passez à la cafeteria, à la machine à café ou même aux toilettes⁶⁴; de même, des inspecteurs de police ont la possibilité de vous identifier à une manifestation.

⁶⁰ Tel que défini par le dictionnaire Larousse, disponible sur <http://www.larousse.fr/dictionnaires/francais/interop%C3%A9rabilit%C3%A9/43787>, consulté pour la dernière fois le 30 juillet 2014.

⁶¹ Disponible sur http://www.amazon.fr/RFID-NFC-Lecteur-Graveur-AVANC%C3%89/dp/9896740054/ref=sr_1_5?ie=UTF8&qid=1406706287&sr=8-5&keywords=lecteur+rfid, consulté pour la dernière fois le 30 juillet 2014.

⁶² OCDE, « L'identification par radiofréquence (RFID) - sécurité de l'information et protection de la vie privée », 29 avril 2008, p. 66, disponible sur <http://www.oecd.org/fr/sti/ieconomie/44688367.pdf>, consulté pour la dernière fois le 30 juillet 2014.

⁶³ *Ibidem*, pp. 64-65.

⁶⁴ D. DARQUENNES, Y. POULLET et A. ROUVROY, « Le droit à la rencontre des technologies de l'information et de la communication : le cas du RFID », *Cahiers Droit, Sciences et Technologies*, CNRS Editions, 2008, p. 119.

La localisation et le traçage des données issues de l'identification par radiofréquence sont des risques inhérents à la collecte de celles-ci.

§ 2. Le profilage

Par la réunion en une base de données ou un entrepôt de données (*datawarehouses*), des données issues de l'identification par radiofréquence et tout en utilisant des méthodes statistiques, il est usuel d'en ressortir des comportements types d'individus, des profils⁶⁵.

L'identification par radiofréquence permet en effet de caractériser les personnes détentrices d'objets sans que ces dernières soient identifiées formellement⁶⁶. Il n'est en effet pas nécessaire de connaître l'identité de la personne pour lier un objet et les informations que contient l'étiquette y apposée ou lier différents objets apposés d'une étiquette ensemble⁶⁷. Les liaisons sont alors transférées dans un entrepôt de données ayant les caractéristiques suivantes : « 1) il reprend les données collectées pour diverses finalités, 2) il les compile et les prépare pour une réutilisation dans un but de *data mining*, 3) il ne les modifie pas mais les analyse pour créer de l'information nouvelle, 4) ses finalités peuvent entraîner notamment des décisions relatives aux personnes et 5) son utilisation peut évoluer selon les besoins »⁶⁸. Le *data mining* est « le processus d'analyse de données collectées pour diverses finalités et résumées dans une information utile, information qui peut être utilisée pour augmenter les revenus d'une entreprise ou en réduire les coûts »⁶⁹. Les profils alors créés à partir des données issues de l'identification par radiofréquence peuvent fournir des informations très intéressantes aux entreprises de marketing. Par exemple, avec un taux de 89% de certitude, il est possible de déduire grâce à la composition d'un panier d'achats dans une grande surface à une heure établie que la personne ayant composé le panier est vraisemblablement amateur de voyages lointains, célibataire et fraudeur potentiel⁷⁰.

Le profil peut même induire que le responsable du traitement ou la personne ayant acheté les conclusions du traitement, ait une meilleure connaissance des habitudes de consommation de

⁶⁵ J.F. HENROTTE et Y. POULLET, *op. cit.*, pp. 202-211.

⁶⁶ V. FOSSOUL, « RFID et biométrie : état des lieux », *op.cit.*, p. 150.

⁶⁷ D. DARQUENNES et Y. POULLET, *op. cit.*, p. 272.

⁶⁸ N. LEFEVER et Y. POULLET, « Entrepôts de données et vie privée », *R.D.T.I.*, 2008/30, pp. 7-20, disponible sur <http://www.strada.be>, consulté pour la dernière fois le 30 juillet 2014.

⁶⁹ Traduction libre, tel que défini par Pr. J. FRAND, disponible sur <http://www.anderson.ucla.edu/faculty/jason.frand/teacher/technologies/palace/datamining.htm>, consulté pour la dernière fois le 30 juillet 2014.

⁷⁰ J.F. HENROTTE et Y. POULLET, *op. cit.*, p. 205.

la personne à qui appartenait les données initiales. Pire encore, il reviendra à cette même personne de prouver l'inexactitude des données si elles sont erronées⁷¹.

La création de profil de consommation suite à la collecte de données issues de l'identification par radiofréquence est une réalité dont le consommateur n'a pas conscience.

§ 3. La sécurité des données

Comme exposé ci-dessus, les données présentes dans la mémoire de l'étiquette peuvent faire l'objet de diverses protections, tant au niveau de la divulgation qu'au niveau de l'authentification des données transmises⁷². Cependant, dans la pratique, peu d'étiquettes bénéficient d'une protection adéquate. En effet, même l'étiquette protégée par une divulgation cryptée asymétriquement et authentifiée de manière forte pourra faire l'objet d'un hackage car les fonctions cryptographiques ne sont pas expertisées⁷³.

En fonction des données présentes dans la mémoire de l'étiquette, le hackage peut consister en un vol d'identité ou en un vol d'informations.

La question est de savoir quand sommes-nous en présence d'un vol ? Est-ce comparable à la collecte de données à l'insu de l'utilisateur ? Le vol est communément défini comme la soustraction frauduleuse de la chose d'autrui⁷⁴. Nous pouvons dès lors établir qu'il y aura vol lorsqu'il y a des manœuvres frauduleuses pour accéder aux informations ou à l'identifiant. Par conséquent, la simple collecte de données à l'insu de l'utilisateur ne constitue pas un vol si les données ne sont pas protégées. Au contraire, si les données bénéficient d'une quelconque protection, même ingénue, la collecte sera qualifiée de vol puisque le hacker devra user de manœuvres frauduleuses pour collecter les données.

A. Le vol d'identité

Le vol d'identité est le hackage le plus dangereux car l'étiquette peut faire l'objet d'une reproduction identique. Le hacker pourra alors facilement se faire passer pour vous lors d'un contrôle d'identité avec toutes les conséquences dramatiques qui peuvent en découler.

⁷¹ D.J. STEINBOCK, « Data Matching, Data Mining et Due Process », *40 GA Law Rev*, (2005), 1, pp. 82 et s.

⁷² Voy. *supra* p. 10.

⁷³ G. AVOINE, *op.cit.*, p. 21.

⁷⁴ Tel que défini par le dictionnaire Larousse, disponible sur <http://www.larousse.fr/dictionnaires/francais/vol/82422?q=vol#81452>, consulté pour la dernière fois le 30 juillet 2014.

Le vol d'identité ne concerne que les étiquettes protégées par une authentification⁷⁵, le hacker authentifiera votre identité lorsqu'il se fera passer pour vous.

B. Le vol d'informations

Le vol d'informations personnelles est problématique également car même si le hacker ne peut usurper votre identité, il détient désormais des informations vous concernant personnellement. Il peut alors soit utiliser votre identité de façon non authentifiable, soit revendre les données collectées ayant une valeur commerciale importante.

Le vol d'informations trouve à s'appliquer de façon récurrente dans le cas d'espionnage industriel, ce dernier ne fait cependant pas l'objet de la présente recherche.

⁷⁵ G. AVOINE, *op.cit.*, p. 22.

Chapitre 2. La vie privée et les données à caractère personnel⁷⁶

Afin de déterminer en quoi les moyens et risques exposés ci-dessus heurtent un quelconque droit à la vie privée de l'individu, il convient de se demander ce qu'est le droit à la vie privée.

La Commission européenne a en effet indiqué dans une communication concernant l'identification par radiofréquence en Europe que « des mesures appropriées de protection de la vie privée sont donc préconisées comme condition d'une large adhésion du public à la RFID »⁷⁷. De même, le *National Research Council* américain soulignait que « compte tenu des grandes différences existant entre les individus sur la question de la vie privée, ainsi que des nombreuses normes sociales, l'instauration d'une confiance publique à l'égard de la technologie RFID sera une tâche ardue et de longue haleine(...) »⁷⁸.

Mais qu'est-ce que la vie privée ?

Section 1^{ère}. De la vie privée au droit à la vie privée

La distinction entre la vie privée et le droit à la vie privée est essentielle comme le faisait remarquer J. Michael dans sa publication *Privacy and Human Right*⁷⁹, tous les aspects de la première ne recevant pas une protection légale. Le droit à la vie privée étant les intérêts que la société a reconnus à la vie privée.

§ 1^{er}. De la vie privée...

Même si la notion de droit à la vie privée est relativement récente, le besoin de protéger sa vie privée ne l'est quant à lui pas. La vie privée fait depuis longtemps l'objet de questionnements

⁷⁶ Le présent chapitre a largement été inspiré par les lectures suivantes, voy. notamment B. DOCQUIR, *Le droit à la vie privée*, Bruxelles, Larcier, 2008, pp. 27-35 ; H. BURKERT, « Introduction. Dualities of privacy – An introduction to « personal data protection and fundamental rights », in *Défis du droit à la protection de la vie privée* (sous la dir. de M. VERONICA et P. PALAZZI), Bruxelles, Bruylant, 2008, pp. 14-23 ; A.R. NADEAU, *Vie privée et droits fondamentaux*, Canada, Editions Yvon Blais Inc., 2000, pp. 19-31.; Y. POULLET, « La protection des données, entre libertés, droits subjectifs et intérêts légitimes », in *Liber amicorum Paul Martens*, Bruxelles, Larcier, 2007, pp. 133-150 ; Y. POULLET, « Pour une troisième génération de réglementation de protection des données », *op. cit.*, pp. 35-54 ; O.R. PUCCINELLI, « Apuntes sobre la evolución normativa y el desarrollo conceptual de los derechos de y a la protección de datos », in *Défis du droit à la protection de la vie privée* (sous la dir. de M. VERONICA et P. PALAZZI), Bruxelles, Bruylant, 2008, pp. 99-130 et F. RIGAUX, « Protection de la vie privée », *R.P.D.B.*, Complément t. IX, Bruxelles, Bruylant, 2004, n^{os} 3-17.

⁷⁷ Communication de la Commission au Parlement européen, au Conseil, au Conseil économique et social européen et au Comité des régions, « L'identification par radiofréquence (RFID) en Europe : vers un cadre politique », document COM(2007)96, 15 mars 2003, p. 5.

⁷⁸ Cité par l'Organisation de Coopération et de Développement Economique (OCDE) in « L'identification par radiofréquence (RFID) – sécurité de l'information et protection de la vie privée », *op.cit.*, p. 62.

⁷⁹ J. MICHAEL, *Privacy and Human Right – An International and Comparative Study With Special Reference to Developments in Information Technology*, Dartmouth, UNESCO Publishing, 1994, p. 2.

profonds tant dans les textes bibliques que philosophiques de Socrate ou John Locke en passant par Platon ou Thomas More⁸⁰.

La préservation d'une zone d'intimité, d'un espace privé territorialisé est un besoin universel de toutes espèces animales⁸¹. La protection de la vie privée a pour fonction de fournir une zone dans laquelle l'individu peut se développer, faire des choix personnels sans être observé. Le sénateur Edward V. Long constatait en effet que « nous agissons différemment si nous pensons être observé ; si nous ne pouvons jamais être certain d'être ou non écouté ou observé, toutes nos actions seront altérées et notre caractère, notre façon d'être changera »⁸². Ce besoin de réclusion est essentiel à la réalisation de l'individu. Yves Poullet l'explique de cette manière : « Déjà dans les villages traditionnels, le rôle joué par les murs des habitations privées était de protéger une sphère d'intimité dans laquelle les individus se sentaient libres d'abandonner le rôle qu'ils endossent en public, le temps de leurs activités privées »⁸³.

Si cette sphère privée n'existait pas, cela mènerait à l'homogénéisation de la pensée, au conformisme et irait même jusqu'à engendrer la violence⁸⁴.

Mais cette nécessité de préservation d'un espace privé doit également être mise en perspective avec le besoin pour l'homme d'interagir avec ses semblables, d'avoir des stimulations sociales. Le manque de relation sociale pourrait engendrer des maux similaires au manque de sphère privée. Il convient dès lors d'établir un juste équilibre entre l'intimité et les stimulations sociales⁸⁵.

Le droit a alors pour fonction de protéger cette zone de vie privée afin que l'individu ait une relation authentique avec lui-même mais également avec autrui.

§ 2. ...au droit à la vie privée

La première expression doctrinale du droit au respect de la vie privée est communément attribuée à Samuel Warren et Louis Brandeis dans leur article « *The Right to Privacy* »⁸⁶ par

⁸⁰ M.R. KONVITZ, « Privacy and the Law – A Philosophical Prelude », *31 Law and Contemporary Problems*, 1996, p. 273.

⁸¹ A.F. WESTIN, *Privacy and Freedoms*, New York, Atheneum, 1967, pp. 10-11.

⁸² Traduction libre, voy. H. HUMPHREY, *The Intruders*, New York, 1967, viii, cité par S. BENN, « Privacy, Freedom and Respect for Persons », in *Privacy (Nomos XIII)* (sous la dir. de J.R. PENNOCK et J.W. CHAPMAN), New York, Atherton Press, 1971, pp. 71-74.

⁸³ J.F. HENROTTE et Y. POULLET, *op. cit.*, pp.202-208.

⁸⁴ S.M. JOUNARD, « Some Psychological Aspects of Privacy », *31 Law and Contemporary Problems*, 1966, p. 307.

⁸⁵ UNITED KINGDOM, *Report of the Committee on Privacy*, CMND 5012, 1972, § 109.

⁸⁶ S.D. WARREN et L.D. BRANDEIS, « The Right to Privacy », *4 Harvard Law Review*, 1890, p. 193.

les mots « *the right to be let alone* »⁸⁷. Les deux avocats américains se sont basés sur la jurisprudence *Boyd v. United States* qui déclarait inconstitutionnelle une loi qui contraignait un contribuable à communiquer ses livres comptables⁸⁸, la jurisprudence anglaise *Abernethy v. Hutchinson*, dans laquelle le juge déclarait illicite la publication d'une reproduction écrite d'une conférence sans l'autorisation du conférencier⁸⁹ et la jurisprudence anglaise *Prince Albert v. Strange*, interdisant la reproduction d'un album familial de la famille royale⁹⁰ ; dans lesquelles on peut retrouver à plusieurs reprises le terme *privacy*. Ces exemples jurisprudentiels exposent déjà certains traits du droit à la vie privée actuel : « l'affirmation du droit à la vie privée face à l'exploitation commerciale de l'image d'autrui, l'importance donnée au consentement de la personne,... »⁹¹.

Suite à cet article, le droit à la vie privée a fait l'objet de nombreux débats doctrinaux tant au niveau de son existence⁹² que de sa définition. Le droit à la vie privée est en effet un droit contextuel, qui ne peut être défini à l'avance⁹³ car il est lié à des considérations culturelles⁹⁴.

Après la Seconde Guerre mondiale et le développement des droits de l'homme, le droit à la vie privée acquiert son autonomie en tant que concept juridique en étant consacré comme droit fondamental dans plusieurs traités internationaux, notamment à l'article 12 de la Déclaration universelle des droits de l'homme du 10 décembre 1948, l'article 17 du Pacte international du 16 décembre 1966 relatif aux droits civils et politiques ainsi que l'article 8, alinéa premier de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales.

La notion de droit à la vie privée (et donc la notion même de vie privée) s'élargit par la suite au droit à l'épanouissement⁹⁵ qui n'est plus relatif à une sphère privée où l'individu peut se construire et vivre comme il l'entend mais, le concept englobe dorénavant le droit de nouer des relations avec autrui et de les développer⁹⁶.

⁸⁷ La femme du second ayant fait l'objet d'un article non-glorieux dans la presse locale, les deux avocats se sont alors penchés sur cette notion qui devait être protégée dans une société où les moyens de communication commençaient à se développer.

⁸⁸ *Boyd v. United States*, 116 US 616 (1886).

⁸⁹ *Abernethy v. Hutchinson*, 1 H. and Tw. 28 (1825), 47 ER 1313 (Chanc.).

⁹⁰ *Prince Albert v. Strange*, 2DeG. And Sm. 712 (1849), 64 ER, 293 (Chanc.).

⁹¹ B. DOCQUIR, *op.cit.*, p. 27.

⁹² W. PROSSER, « Privacy », 48 *California Law Review*, 1960, p. 383.

⁹³ Voy. notamment O. DE SCHUTTER, « La vie privée entre droit de la personnalité et libéralité », *Rev. Trim. D. H.*, 1999, pp. 827 et s.

⁹⁴ Y. POULLET, « Pour une troisième génération de réglementation de protection des données », *op. cit.*, p. 36.

⁹⁵ O. DE SCHUTTER, *op.cit.*, pp. 827 et s.

⁹⁶ Cour eur. D. H., arrêt *Niemetz c. Allemagne*, 16 décembre 1992, §29, *Rev. trim. dr. h.*, 1993, p. 647.

Le droit à la vie privée est un des droits les plus fondamentaux, source de nombreux autres droits et libertés fondamentaux⁹⁷. Son caractère indéfinissable et contextuel convient parfaitement à l'évolution de la société, par exemple c'est sur base du droit au respect de la vie privée que les homosexuels ont obtenu le droit de parentalité⁹⁸.

Le droit à la vie privée revêt aujourd'hui deux aspects⁹⁹ : la vie privée passive au sens que chacun ait la possibilité de vivre à l'abri du regard d'autrui et la vie privée active au sens que chacun ait la possibilité de choisir seul la façon dont il veut vivre sa vie et divulguer les informations le concernant¹⁰⁰.

Section 2. Du droit à la vie privée au droit à la protection des données à caractère personnel

Avec les débuts des avancées technologiques dans les années 1970, il est apparu que l'individu devait avoir la possibilité d'exercer une certaine maîtrise sur ses données utilisées par des tiers. Bien avant cette période, il existait déjà des bases de données¹⁰¹, comme les registres allemands ; mais avec l'avènement de l'informatique et les possibilités de traitement de données y afférentes, la question de la protection des données s'est posée. En effet, l'individu a le droit de maîtriser les informations le concernant et la communication de celles-ci. Certains auteurs affirment que l'adoption d'un droit à la protection des données à caractère personnel peut également être perçue comme une mesure économique protectionniste en tant que barrières non-tarifaires¹⁰².

Le droit à la protection de données à caractère personnel a acquis une portée autonome en Europe avec la publication de la Convention n°108 du Conseil de l'Europe en 1981. Aux

⁹⁷ Comme le droit à la protection des données, le droit à l'image, ... Voy. notamment la citation de F. VOLIO : « *Indeed in one sense all human rights are aspects of the right to privacy* » in F. VOLIO, « Legal Personality, Privacy and the Family », in *The International Bill of Rights*, New York, Columbia University Press, 1981, p. 185.

⁹⁸ Voy. par exemple la proposition de loi modifiant la législation relative à la protection de l'enfant, en ce qui concerne l'instauration de la parentalité sociale, Avis du Conseil d'Etat, *Doc. parl.*, Chambre, 2007-2008, n°52 1303/002, p. 19.

⁹⁹ Également appelé « *Derechos de la proteccion de datos y derechos a la proteccion de datos* » par PUCCINELLI in O.R. PUCCINELLI, *op.cit.*, pp. 99-130 ; « *Informational privacy and decisional privacy* » par KING in N.J. KING, « Fundamental human right principle inspires U.S. data privacy law, but protections are less than fundamental », in *Défis du droit à la protection de la vie privée* (sous la dir. de M. VERONICA et P. PALAZZI), Bruxelles, Bruylant, 2008, pp. 71-98 et « la vie-privée-intimité et la vie-privée-libertés » par POULLET in Y. POULLET, « Pour une troisième génération de réglementation de protection des données », *op.cit.*, pp. 25-70.

¹⁰⁰ H. BURKERT, *op.cit.*, pp. 14-23 ; B. DOCQUIR, *op.cit.*, pp. 65-66.

¹⁰¹ O.R. PUCCINELLI, *op. cit.*, pp. 110-118.

¹⁰² Voy. notamment J. MICHAEL, *op.cit.*, p. 32.

Etats-Unis, la première législation protégeant les données personnelles est le *Privacy Act* de 1974.

Au départ, le droit de la protection des données ne concernait que les données relevant de la vie privée et plus précisément de la vie privée active¹⁰³. Avec le temps, ce droit acquit une autonomie et se détacha du droit à la vie privée pour protéger les données à caractère personnel, qu'elles soient relatives à la vie privée ou à la vie publique¹⁰⁴.

¹⁰³ Voy. *supra* p. 41.

¹⁰⁴ Les données personnelles relatives à la vie publique peuvent par exemple être celles des individus jouant un rôle sur la scène publique : les hommes politiques, les stars,...

Chapitre 3. La collecte de données contraire à la vie privée et à la protection des données à caractère personnel

Les données issues de l'identification par radiofréquence sont des données à caractère personnel dont les moyens discutables mis en œuvre pour les collecter et les risques en découlant sont connus depuis un certain temps, comme le reflète le document de travail sur la RFID élaboré en 2008 par l'Organisation de Coopération et de Développement Economique (OCDE)¹⁰⁵.

Ces données doivent être protégées dans une certaine mesure par le droit à la vie privée et le droit à la protection des données personnelles puisque leur collecte met à mal la protection de la vie privée des individus. Des étiquettes d'identification par radiofréquence sont insérées dans nos habits et nos produits de consommation et divulguent nos habitudes à l'intérieur de notre sphère privée à des destinataires en dehors de celle-ci. Nous nous sentons alors sans cesse observés, « les murs de notre maison ne nous cachent plus du regard d'autrui »¹⁰⁶. De même, nous ne contrôlons plus la communication de nos informations personnelles.

Les deux aspects de la vie privée sont alors négligés par l'identification par radiofréquence telle qu'elle se présente aujourd'hui et la protection des données personnelles, droit autonome aujourd'hui, est également bafouée.

Le titre suivant de la présente recherche analyse les protections offertes par le régime juridique européen d'une part et le régime juridique américain fédéral d'autre part afin d'en dégager une solution globale et satisfaisante pour la protection des données personnelles issues de l'identification par radiofréquence.

¹⁰⁵ OCDE, *op.cit.*, pp. 62 et s.

¹⁰⁶ J.F. HENROTTE et Y. POULLET, *op. cit.*, p. 203.

Titre 3. Quelles sont les solutions proposées ?

Au titre précédent, nous avons identifié six risques potentiels que représente l'identification par radiofréquence : l'invisibilité, l'ininterruption et l'interopérabilité du mécanisme, ainsi que la traçabilité des individus, leur profilage et les atteintes à la sécurité du système pouvant entraîner un vol d'identité ou de données.

Le présent titre analyse tout d'abord les diverses solutions proposées tant au niveau de l'Union européenne qu'au niveau fédéral des Etats-Unis et ce, pour chaque problème posé. Une telle démarche comparative a été choisie car les nouvelles technologies et en particulier l'identification par radiofréquence, abolissent les frontières entre les Etats. En effet, l'étiquette apposée sur l'un de vos objets ne va pas s'arrêter de fonctionner lors d'un passage aux frontières. L'étude d'un seul régime paraissait dès lors pauvre quant à la pertinence des solutions envisagées. En étudiant deux régimes juridiques, il est possible de dégager une solution globale reflétant les meilleurs côtés de chacun et d'espérer qu'ils s'harmonisent. Le choix des régimes juridiques à analyser découle de la connaissance de leur fonctionnement par l'auteur, de l'importance donnée aux nouvelles technologies dans ces sociétés, celles-ci étant une terre fertile pour leur avènement, mais aussi de la différence des systèmes juridiques, respectivement l'un de Civil Law, l'autre de Common Law, pouvant rendre l'étude plus intéressante.

Suite à l'analyse des différentes propositions de solutions, les raisons des discordances existantes seront brièvement expliquées.

Enfin, nous tenterons d'exposer une solution globale, acceptable et dont l'effectivité est possible en rejoignant les deux encadrements analysés.

Chapitre 1^{er}. Les divers encadrements

L'analyse qui suit a pour objet les solutions proposées par le droit de l'Union européenne et par le droit américain fédéral aux problèmes inhérents à l'identification par radiofréquence.

Section 1^{ère}. L'encadrement européen

L'étude des solutions est circonscrite au droit de l'Union européenne uniquement. Il ne sera dès lors aucunement fait mention du droit des Etats membres, même lorsqu'il s'agira d'une directive, celle-ci nécessitant une transposition dans le droit interne. Ce choix est motivé par le caractère limité de la présente recherche.

§ 1^{er}. Analyse préliminaire

Le droit de l'Union européenne est en pleine mouvance concernant la protection des données à caractère personnel¹⁰⁷, les solutions en vigueur seront alors explicitées tout en exposant les futures possibles.

Le droit applicable aux diverses solutions en vigueur découle principalement de deux sources cumulatives¹⁰⁸, la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données¹⁰⁹, sujette à la réforme (ci-après la directive générale) ; et la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (ci-après, la directive communications électroniques)¹¹⁰.

Avant d'analyser les solutions proposées par ces deux directives encadrant le traitement de données, il convient de déterminer leur champ d'application pour comprendre tous les enjeux de l'identification par radiofréquence.

¹⁰⁷ Proposition de règlement 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 (règlement général sur la protection des données), document COM/2012/011, 25 janvier 2012.

¹⁰⁸ Voy. en ce sens K. ROSIER, « La directive 2002/58/CE vie privée et communications électroniques et la directive 95/46/CE relative au traitement des données à caractère personnel : comment les (ré)concilier ? » in *Défis du droit à la protection de la vie privée* (sous la dir. de M. VERONICA et P. PALAZZI), Bruxelles, Bruylant, 2008, pp. 331 et 354 ; Y. POULLET, « Pour une troisième génération de réglementation de protection des données », *op.cit.*, pp. 35-49.

¹⁰⁹ Directive (CE) n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 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, *J.O.C.E.*, L 281, 23 novembre 1995.

¹¹⁰ Directive (CE) n° 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, *J.O.C.E.*, L 201, 31 juillet 2002.

A. Champ d'application territorial

La directive communications électroniques s'applique, en vertu de son article 3, « à la fourniture de services de communications électroniques accessible au public sur les réseaux publics de communications dans la Communauté »¹¹¹. La directive s'applique en fonction de la localisation du destinataire¹¹² : si la fourniture de service a lieu sur le territoire de l'Union européenne, la directive est d'application.

La directive générale, quant à elle, s'applique en fonction de la localisation du responsable du traitement, c'est-à-dire que la directive s'applique si le responsable du traitement a un établissement dans la Communauté ou s'il utilise des moyens automatisés (ou non) situés sur le territoire de la Communauté¹¹³. Ce champ d'application devrait être étendu par l'adoption du règlement et ce dernier serait alors d'application si le responsable du traitement a un établissement sur le territoire de l'Union ou si les personnes concernées par le traitement ont leur résidence sur le territoire de l'Union dans les cas où le traitement est lié à une offre de biens ou de services dans l'Union ou si le traitement a pour but l'observation de leur comportement¹¹⁴. Le champ territorial de la protection générale des données passe dès lors d'une simple localisation du responsable du traitement à une localisation de ce dernier ou du destinataire.

B. Champ d'application matériel

La directive communications électroniques s'applique au « traitement de données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessible au public sur les réseaux publics de communication ». L'identification par radiofréquence est considérée comme une fourniture de services de communications électroniques accessible au public sur les réseaux publics de communication en vertu de l'article 2 de la directive 2002/21/CE qui définit le service de communications électroniques comme « le service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques »¹¹⁵ qui sont des systèmes de transmission de signaux par voie hertzienne¹¹⁶.

¹¹¹ Article 3 de la directive n° 2002/58/CE.

¹¹² K. ROSIER, *op. cit.*, p. 332.

¹¹³ Article 4 de la directive n° 95/46/CE.

¹¹⁴ Article 3 de la proposition de règlement.

¹¹⁵ Article 2, c) de la directive (CE) n° 2002/21/CE du Parlement européen et de Conseil du 27 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, *J.O.C.E.*, L 108, 24 avril 2002.

L'identification par radiofréquence est un service qui consiste en la transmission de signaux par voie hertzienne.

Quant au caractère personnel des données traitées, il est fait référence à l'analyse de la notion en vertu de la directive générale¹¹⁷. Il convient par ailleurs de préciser que certains articles de la directive communications électroniques ne requièrent pas que les données soient personnelles, comme l'indiquent l'article 6 ou l'article 9 relatifs respectivement aux données de trafic et aux données de localisation, ces dernières sont en effet définies comme « toutes données traitées »¹¹⁸.

L'identification par radiofréquence relève du champ d'application de la directive communications électroniques, en ce sens que les données issues de celle-ci sont des données à caractère personnel traitées dans le cadre de la fourniture d'un service de communications électroniques accessible au public.

La directive générale quant à elle, s'applique au traitement de données à caractère personnel, celles-ci étant définies comme « toute information concernant une personne physique identifiée ou identifiable »¹¹⁹. Cette notion a fait l'objet de nombreux débats doctrinaux ou jurisprudentiels¹²⁰ et c'est pourquoi le Groupe de l'article 29 sur la protection des données à caractère personnel, organe consultatif indépendant au sein de l'Union européenne, a publié un avis le 20 juin 2007 sur le concept de données à caractère personnel¹²¹ où il décompose la définition de la directive en quatre éléments constitutifs : « toute information », « concernant », « une personne physique », « identifiée ou identifiable ».

« Toute information » est définie comme n'importe quel renseignement objectif ou subjectif concernant la vie privée d'une personne, sa vie familiale, ses activités, ses relations de travail ou son comportement économique ou social présent sur n'importe quel support (sur papier, sur une mémoire,...) et relevant de n'importe quel format (alphabétique, numérique, graphique, ...). Les données issues de l'identification par radiofréquence sont donc « toute information ».

¹¹⁶ Article 2, a) de la directive n° 2002/21/CE.

¹¹⁷ Voy. *infra* pp. 48-50.

¹¹⁸ Article 2, b) et c) de la directive n° 2002/58/CE.

¹¹⁹ Article 2, a) de la directive n° 95/46/CE.

¹²⁰ Voy. par exemple B. DOCQUIR., *Le droit à la vie privée*, Bruxelles, Larcier, 2008 ; C.J.C.E., 6 novembre 2003 (Procédure pénale contre Bodil Lindqvist), 6 novembre 2003, C-101/01, disponible sur <http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=27533>.

¹²¹ GROUPE DE L'ARTICLE 29, « Avis 4/2007 sur le concept de données à caractère personnel », *op.cit.*.

Une information « concernant » « une personne physique » est une information qui a « trait à cette personne physique »¹²². Les informations concernent une personne physique « si elles ont trait à l'identité, aux caractéristiques ou au comportement d'une personne ou si cette information est utilisée pour déterminer ou influencer la façon dont cette personne est traitée ou évaluée »¹²³. Les données issues de l'identification par radiofréquence « concernent » « une personne physique » au vu de cette définition.

Et cette personne sera « identifiée » si elle se distingue des autres personnes présentes au sein d'un groupe, ou « identifiable » lorsque cette possibilité existe. La personne n'est alors plus identifiée ou identifiable mais distinguée ou distinguable. De même, la Cour de justice considère qu'il n'est plus nécessaire pour identifier une personne de connaître son nom : « l'opération consistant à faire référence, sur une page Internet, à diverses personnes et à les identifier soit par leur nom, soit par d'autres moyens, par exemple leur numéro de téléphone ou des informations relatives à leurs conditions de travail et à leurs passe-temps, constitue un "traitement de données à caractère personnel, automatisé en tout ou en partie", au sens [...] de la directive 95/46 »¹²⁴. L'identification par radiofréquence identifie alors une personne physique ou permet la possible identification puisqu'elle est apte à la distinguer dans un groupe d'individus.

L'identification par radiofréquence relève du champ d'application matériel de la directive générale puisque les données issues de cette dernière sont des données à caractère personnel telles qu'elles sont définies par la directive.

Le projet de règlement définit les données à caractère personnel comme « toute information se rapportant à une personne concernée »¹²⁵ ou comme « toute information se rapportant à une personne physique identifiée ou identifiable »¹²⁶. L'analyse du concept est par conséquent

¹²² GROUPE DE L'ARTICLE 29, « Avis 4/2007 sur le concept de données à caractère personnel », *op. cit.*, p. 10.

¹²³ GROUPE DE L'ARTICLE 29, « Document de travail sur les questions de protection des données liées à la technologie RFID (radio-identification) », W.P. 105, 19 janvier 2005, p. 9.

¹²⁴ C.J.C.E., 6 novembre 2003 (Procédure pénale contre Bodil Lindqvist), 6 novembre 2003, C-101/01, disponible sur <http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=27533>, point 27.

¹²⁵ Article 4 de la proposition de règlement.

¹²⁶ Amendement 98 de la résolution législative de Parlement européen du 12 mars 2014 sur la proposition de règlement 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, disponible sur <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//FR>, consulté pour la dernière fois le 30 juillet 2014.

impossible à réaliser tant qu'un texte définitif ne sera pas adopté afin de ne pas entrer dans des digressions.

Bref, l'identification par radiofréquence telle que faisant l'objet de la présente recherche, c'est-à-dire non-désactivée et en la possession d'une personne physique, relève du champ d'application matériel tant de la directive communications électroniques que de la directive générale¹²⁷.

C. Champ d'application personnel

La directive communications électroniques s'applique au fournisseur d'un service de communication électronique¹²⁸, c'est-à-dire celui qui met en place, exploite, surveille ou met à la disposition un tel service¹²⁹. Dans le cas de l'identification par radiofréquence, le fournisseur sera alors la personne physique ou morale, l'autorité publique, qui fournit l'étiquette à l'individu.

La directive générale quant à elle s'applique au responsable du traitement¹³⁰ (de même que le projet de règlement)¹³¹, c'est-à-dire « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel »¹³². Dans le cas de l'identification par radiofréquence, le responsable du traitement n'est pas toujours le fournisseur de l'étiquette. C'est le cas si le fournisseur de l'étiquette opère également un traitement de données ; mais le responsable du traitement peut être également toutes les autres personnes ou entités qui disposent d'un lecteur aux fins de traitement de données à caractère personnel.

Il convient dès à présent d'analyser les solutions que propose le droit européen aux problèmes exposés ci-dessus.

§ 2. Contrer le caractère invisible

L'invisibilité de l'identification par radiofréquence se présente à deux niveaux : l'un relatif au fonctionnement même du mécanisme sans contact et l'autre relatif à la petitesse des éléments.

¹²⁷ GROUPE DE L'ARTICLE 29, « Document de travail sur les questions de protection des données liées à la technologie RFID (radio-identification) », *op.cit.*, p. 6.

¹²⁸ Articles 4, 1. ; 6, 1. ; etc. de la directive n° 2002/58/CE.

¹²⁹ Par analogie à l'article 2, m) de la directive n° 2002/21/CE.

¹³⁰ Articles 10 ; 17 ; etc. de la directive n° 95/46/CE.

¹³¹ Articles 8 ; 14 ; etc. de la proposition de règlement.

¹³² Article 2, d) de la directive n° 95/46/CE.

Ces deux degrés d'invisibilité impliquent que l'individu n'a pas conscience du processus d'identification en jeu. En tant qu'éléments intrinsèques de l'identification par radiofréquence, modifier le fonctionnement sans contact ou la taille des composants serait absurde. Il convient alors d'informer l'individu du processus d'identification par radiofréquence présent dans les objets qu'il utilise.

L'information de l'individu devrait avoir lieu en deux temps, l'un de façon générale, informer l'individu du mécanisme de l'identification par radiofréquence, des risques y afférents mais également des points positifs d'une telle technologie ; l'autre de façon personnalisée lors de l'achat d'un produit sur lequel est apposée une étiquette.

L'information générale de l'individu au sujet de l'identification par radiofréquence en Europe est déplorable. Notons toutefois l'article 52 de la proposition de règlement qui charge une autorité de contrôle de sensibiliser « le public aux risques, aux règles, aux garanties et aux droits relatifs au traitement des données à caractère personnel »¹³³.

Concernant l'information personnalisée, trois directives imposent une obligation d'information de l'individu en possession d'une étiquette d'identification.

Tout d'abord, la directive générale impose un devoir d'information assez large comprenant au minimum: « a) l'identité du responsable du traitement et, le cas échéant, de son représentant ; b) les finalités du traitement auquel les données sont destinées ; c) toute information supplémentaire telle que : - les destinataires ou les catégories de destinataires des données, - le fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences éventuelles d'un défaut de réponse, - l'existence d'un droit d'accès aux données la concernant et de rectification de ces données »¹³⁴. Ce devoir d'information incombe au responsable du traitement qui est la personne utilisant le lecteur d'étiquettes. Ce devoir d'information est ineffectif en réalité : un responsable de traitement indépendant de la fourniture de l'étiquette ne va jamais informer l'individu de la collecte des données. Par exemple, imaginez-vous être informé de la collecte des données à chaque entrée ou sortie d'un magasin d'alimentation ? La proposition de règlement, bien qu'imposant un nombre d'informations à divulguer plus important, souffre également de cette ineffectivité puisque cette obligation incombe toujours au responsable du traitement.

¹³³ Article 52, 2. de la proposition de règlement.

¹³⁴ Article 11 de la directive n° 95/46/CE.

Ensuite, la directive 1999/5/CE du Parlement européen et du Conseil du 9 mars 1999 concernant les équipements hertziens et les équipements terminaux de télécommunications et la reconnaissance mutuelle de leur conformité¹³⁵ qui s'applique à l'identification par radiofréquence, impose en son article 6 que « le fabricant ou la personne responsable de la mise sur le marché de l'appareil fournisse à l'utilisateur des informations sur l'usage auquel il est destiné, accompagnées de la déclaration de conformité aux exigences essentielles »¹³⁶. Cette disposition paraît plus effective et facile à mettre en œuvre puisque l'obligation d'information incombe à celui qui fournit l'étiquette. En réalité, aucune information n'est délivrée lors de l'achat d'un produit sur lequel est apposée une étiquette¹³⁷.

Enfin, la directive communications électroniques impose au fournisseur de service et donc au fournisseur de l'étiquette, une obligation d'information à l'utilisateur¹³⁸ et ce, dans le respect de la directive 95/46/CE. On peut donc en déduire que les informations devant être divulguées en vertu de la directive générale, doivent l'être également en vertu de la directive communications électroniques. *In casu*, l'effectivité devrait être garantie puisque l'obligation incombe à celui qui fournit l'étiquette, cependant, aucune information n'est délivrée en réalité.

L'information de l'individu concernant l'identification par radiofréquence qu'elle soit personnalisée ou globale est donc inexistante au sein de l'Union européenne.

§ 3. Contrer le caractère indéfini

L'identification par radiofréquence fonctionne de manière indéfinie lorsque l'étiquette ne dispose pas d'une batterie, le cas le plus courant en pratique car à moindre coût. Afin de contrer ce caractère indéfini, il suffirait de désactiver l'étiquette lors de la fourniture du produit sur lequel elle est apposée¹³⁹. Celle-ci ne devrait cependant pas être une désactivation par défaut car, comme exposé tout au long de ce travail, l'identification par radiofréquence peut trouver à s'appliquer dans la vie de tous les jours des individus afin de leur faciliter

¹³⁵ Directive (CE) n° 1999/5/CE du Parlement européen et du Conseil du 9 mars 1999 concernant les équipements hertziens et les équipements terminaux de télécommunications et la reconnaissance mutuelle de leur conformité, *J.O.C.E.*, L 91, 7 avril 1999.

¹³⁶ Article 6 de la directive n° 1999/5/CE.

¹³⁷ Constatez-le par vous-même lors de l'achat d'un CD ou DVD, tous sont munis de telles étiquettes aujourd'hui.

¹³⁸ Article 9 de la directive 2002/58/CE.

¹³⁹ En ce sens, la Résolution de la 25^{ème} conférence internationale de Commissaires à la protection des données, prise à Sydney en 2003 : « Chacun... devrait avoir la possibilité de supprimer, désactiver ou détruire les étiquettes », cité par Y. POULLET, « Pour une troisième génération de réglementation de protection des données », *op. cit.*, p. 57.

certaines tâches, et désactiver les étiquettes par défaut reviendrait à réduire à néant toutes ces applications. Par exemple, si vous utilisez un frigo intelligent qui vous informe lorsque l'un de vos aliments est périmé ou vous propose des recettes en fonction de ce qui se trouve en son sein, la désactivation des étiquettes présentes sur vos biens de consommation vous posera problème car votre frigo ne sera plus apte à lire les informations contenues dans ces étiquettes¹⁴⁰.

La désactivation devrait alors être possible et à la portée de tout utilisateur.

Pouvons-nous comparer la désactivation au fait de refuser le traitement de données ? De notre point de vue, non. La désactivation est une formalité unique et irréversible alors que le consentement ou le refus de traitement des données peut différer en fonction du responsable du traitement. De plus, le refus de traitement ne contre pas le caractère indéfini de l'identification par radiofréquence en général, mais pour un responsable de traitement seulement.

En vertu de l'article 14 de la directive communications électroniques, « des mesures peuvent être adoptées afin de garantir que les équipements terminaux seront construits de manière compatible avec le droit des utilisateurs de protéger et de contrôler l'utilisation de leurs données à caractère personnel »¹⁴¹.

De même, l'article 9 de la directive 1999/5/CE lu en parallèle avec l'article 3 de la même loi permet à un Etat membre de retirer du marché un appareil qui ne respecte pas l'exigence de protection des données à caractère personnel si la Commission décide qu'une telle exigence est requise pour les appareils d'identification par radiofréquence¹⁴².

Des bases légales existent donc au niveau européen pour contraindre les concepteurs d'étiquettes d'identification à être désactivables. Encore faudrait-il que ces bases légales soient effectives et que le possesseur d'une étiquette soit informé de la possible désactivation de celle-ci.

§ 4. Contrer le caractère interopérable

Les étiquettes d'identification par radiofréquence peuvent être lues par n'importe quel lecteur si celui-ci dispose de la fréquence hertzienne applicable (aisément trouvable en pratique).

¹⁴⁰ Certes, cette application n'est pas usuelle pour le moment mais avec la rapidité des avancées technologiques, il n'est pas fou de penser que nous disposerons tous d'un tel frigo dans les années à venir.

¹⁴¹ Article 14, 3. de la directive n° 2002/58/CE.

¹⁴² Article 9, 1. et article 3, 2. c) de la directive n° 1999/5/CE.

Cela a pour conséquence que non seulement le fournisseur de l'étiquette pourra lire les informations contenues dans sa mémoire mais également toutes personnes disposant d'un lecteur.

Afin de contrer le caractère interopérable, il suffirait que l'individu ait la possibilité de consentir ou non au traitement de données d'un tel responsable de traitement comme prévu dans les différentes directives¹⁴³. Cependant, et comme exposé ci-dessus¹⁴⁴, l'individu a rarement conscience qu'un tel mécanisme est en place alors, comment pourrait-il y consentir ? Et quand bien même l'individu serait informé de l'étiquette et des risques qu'elle comporte, comment peut-il notifier à tous les lecteurs potentiels son non-consentement ?

Une des solutions pourrait alors être la sécurisation des données ; de la plus simple (mot de passe pour accéder à la mémoire) pour les étiquettes ne contenant pas de données sensibles¹⁴⁵, à la plus complexe (cryptographie asymétrique et authentification) pour celles en contenant. Par exemple, les étiquettes apposées sur les biens de consommation ordinaire seraient protégées par un mot de passe, celui-ci pouvant être connu par les lecteurs inclus dans les frigos afin que les applications privées de la technologie restent possibles.

Toutes les étiquettes alors sécurisées seraient protégées par la réglementation relative au vol de données si elles étaient collectées¹⁴⁶ puisqu'il faudrait user de manœuvres frauduleuses pour collecter des données intelligibles et cela dissuaderait alors la collecte interopérable.

De plus, une telle sécurisation des données pourrait être imposée par les articles exposés ci-dessus concernant le caractère indéfini de l'identification par radiofréquence.

§ 5. Contrer la traçabilité

Les données issues de l'identification par radiofréquence sont intrinsèquement des données de localisation puisqu'elles sont localisables *via* le champ électromagnétique et permettent donc la traçabilité des personnes qui possèdent les objets sur lesquels sont apposées des étiquettes d'identification.

En vertu de son article 9, la directive communications électroniques régit le traitement des données de localisation. Celui-ci expose que les données de localisation peuvent faire l'objet d'un traitement seulement si elles ont « été rendues anonymes ou moyennant le

¹⁴³ Article 5 de la directive n° 2002/58/CE ou l'article 7, a) de la directive n° 95/46/CE.

¹⁴⁴ Voy. *supra* p. 23.

¹⁴⁵ Telles que l'identité, les données biométriques, etc.

¹⁴⁶ Voy. *infra* pp. 58 et s.

consentement des utilisateurs [...], dans la mesure et pour la durée nécessaires à la fourniture d'un service de valeur ajoutée¹⁴⁷ »¹⁴⁸ après avoir informé l'utilisateur sur « les objectifs et la durée du traitement et du fait que les données sont ou non transmises à un tiers »¹⁴⁹. Ces obligations incombent au fournisseur de l'étiquette, la directive ne s'applique alors qu'à la traçabilité effectuée par le fournisseur de l'étiquette. La directive ne contient aucune sanction possible en cas de non-respect des obligations. L'effectivité d'une telle norme est alors à définir.

Les données de localisation peuvent-elles être définies comme des données à caractère personnel au sens de la directive générale et par-là bénéficier de sa protection ? A notre sens, oui puisqu'elles répondent aux conditions énoncées par l'avis du Groupe de l'article 29¹⁵⁰ ; elles permettent en effet de distinguer une personne dans un groupe d'individus et sont relatives à cette personne. De plus, la proposition de règlement énonce explicitement que les données de localisation sont des données qui identifient les personnes¹⁵¹.

La directive générale s'applique donc au traitement des données de localisation collectées par un lecteur d'étiquettes qui n'est pas le fournisseur de celles-ci.

La directive générale énonce les principes devant être respectés lors d'un tel traitement ainsi que les obligations incombant au responsable du traitement.

Les principes sont soit relatifs à la qualité des données : elles doivent être cumulativement « a) traitées loyalement et licitement ; b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités [...] ; c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement ; d) exactes et, si nécessaire, mises à jour [...] ; e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement »¹⁵² ; soit relatifs à la légitimation des traitements de données en ce sens que le traitement ne peut avoir lieu que si « a) le personne concernée a indubitablement donné son

¹⁴⁷ Un service de valeur ajoutée est « tout service qui exige le traitement de données relatives au trafic ou à la localisation », tel que défini à l'article 2, g) de la directive n° 2002/58/CE.

¹⁴⁸ Article 9 de la directive n° 2002/58/CE.

¹⁴⁹ Article 9 de la directive n° 2002/58/CE.

¹⁵⁰ GROUPE DE L'ARTICLE 29, « Avis 4/2007 sur le concept de données à caractère personnel », *op.cit.*.

¹⁵¹ Amendement 98 de la résolution législative de Parlement européen du 12 mars 2014, *op. cit.*.

¹⁵² Article 6 de la directive n° 95/46/CE.

consentement ou b) il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie [...] ou c) il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ou d) il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ou e) il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement [...] ou f) il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée »¹⁵³.

Les obligations incombant au responsable du traitement sont tout d'abord le respect de ces principes, ensuite l'information de la personne concernée¹⁵⁴, le droit d'accès de la personne concernée aux données¹⁵⁵ ainsi que son droit d'opposition¹⁵⁶.

La proposition de règlement ajoute différentes obligations incombant au responsable du traitement¹⁵⁷ mais garde les mêmes causes de licéité du traitement¹⁵⁸.

Il est pertinent de constater de prime abord que le responsable de traitement ne respecte pas les principes relatifs à la légitimation du traitement de données. En effet, seul le consentement de l'individu pourrait de manière générale légitimer le traitement des données issues de l'identification par radiofréquence ; les autres légitimations étant des cas spécifiques peu usuels pour le moment dans la pratique. Il est donc nécessaire pour la plupart des traitements que le responsable obtienne le consentement de la personne. Or, comme expliqué ci-dessus¹⁵⁹, obtenir le consentement de la personne possédant des objets apposés d'étiquettes est illusoire pour un responsable de traitement non-fournisseur d'étiquettes.

Le traitement de données issues de l'identification par radiofréquence peut-il alors être considéré comme enfreignant les règles de la directive dès lors que ce traitement est fait par un lecteur non-fournisseur de l'étiquette et pour autant que ce traitement ne soit pas légitimé par une autre cause ? La réponse nous semble être positive.

Cela pose évidemment problème, pour exemple, un magasin disposant d'un lecteur pour collecter les informations des étiquettes qu'il a lui-même fournies, lira également les

¹⁵³ Article 7 de la directive n° 95/46/CE.

¹⁵⁴ Article 10 de la directive n° 95/46/CE.

¹⁵⁵ Article 12 de la directive n° 95/46/CE.

¹⁵⁶ Article 14 de la directive n° 95/46/CE.

¹⁵⁷ Voy. par exemple l'article 5 de la proposition de règlement.

¹⁵⁸ Article 6 de la proposition de règlement.

¹⁵⁹ Voy. *supra* p. 51.

étiquettes provenant d'autres magasins. La collecte des données issues des étiquettes provenant d'autres magasins devra être sanctionnée au regard du droit européen ¹⁶⁰ puisqu'aucun consentement n'a été donné. La solution de sécurisation des données exposée ci-dessus ¹⁶¹ devrait cependant résoudre ce problème puisque le magasin ne collecterait alors plus les données issues d'étiquettes qu'il n'a pas fournies mais seulement les données issues de ses propres étiquettes.

Bref, les bases légales européennes existent pour contrer la traçabilité, qu'elle soit effectuée par le fournisseur d'étiquettes (directive communications électroniques) ou par un lecteur *lambda* (directive générale). Cependant, ces bases légales manquent d'effectivité lorsqu'elles doivent s'appliquer à l'identification par radiofréquence. Le consentement de la personne est une condition de licéité du traitement qu'oublie tant le fournisseur d'étiquettes que le lecteur, il ne reste plus qu'à espérer que le traitement est alors légitimé soit par une anonymisation des données, soit par d'autres motifs légitimes.

§ 6. Contrer le profilage

Le profilage est défini par la résolution sur la proposition de règlement comme « toute forme de traitement automatisé de données à caractère personnel destinées à évaluer certains aspects personnels propres à une personne physique ou à analyser ou prévoir en particulier le rendement professionnel de celle-ci, sa situation économique, sa localisation, son état de santé, ses préférences personnelles, sa fiabilité ou son comportement » ¹⁶². Le profilage est réalisé la plupart du temps par le croisement entre plusieurs bases de données. Ces bases de données sont constituées grâce aux traitements de données à caractère personnel.

Par son article 5, la directive communications électroniques fait explicitement référence à la directive générale en ce qui concerne le traitement des données ¹⁶³. On peut donc en conclure que cette dernière s'applique au traitement effectué par le fournisseur d'étiquettes mais aussi au traitement effectué par un lecteur *lambda*.

¹⁶⁰ Article 28 de la directive n° 95/46/CE et les articles 78 et 79 de la proposition de règlement.

¹⁶¹ Voy. *supra* p. 54.

¹⁶² Amendement 98 de la résolution législative de Parlement européen du 12 mars 2014, *op. cit.*,

¹⁶³ Article 5 de la directive n° 2002/58/CE.

Le raisonnement exposé ci-dessus concernant la traçabilité s'applique au profilage¹⁶⁴. En effet, à l'origine des deux traitements, on retrouve la collecte des données et la légitimité de celui-ci.

D'une part, nous pouvons conclure que le traitement effectué par le fournisseur de l'étiquette nécessite le consentement de la personne ou un autre motif légitime ; et qu'en réalité cette disposition bénéficie de peu d'effectivité malgré les sanctions applicables¹⁶⁵.

D'autre part, nous concluons que le traitement effectué par un lecteur *lambda* enfreint d'office la législation européenne pour autant que ce dernier ne soit pas légitimé par d'autres motifs ; la condition de consentement de la personne concernée étant illusoire dans le cas d'un traitement effectué par un lecteur non-fournisseur d'étiquettes. Cette situation pose problème au niveau des sanctions et peut être résolue par la sécurisation des données¹⁶⁶.

Cette sécurisation de données permettra de continuer à profiler sur base cette fois de données traitées avec le consentement de la personne concernée ou sur base d'autres motifs légitimes. Le profilage découlera alors de bases de données dont la légitimité sera certaine, ce qui rendra les profils encore plus précis. Le but n'étant pas de contrer tout profilage puisque ce dernier facilite la vie des individus mais bien de contrer le profilage illégitime, fait sans le consentement des personnes concernées.

Bref, les bases légales européennes existent pour contrer le profilage illégitime, quelle que soit la personne effectuant le traitement des données servant au profilage. Cependant, ces bases légales manquent d'effectivité lorsqu'elles ont à s'appliquer à l'identification par radiofréquence. Le consentement de la personne est une condition de licéité du traitement qu'oublie tant le fournisseur d'étiquettes que le lecteur, il ne reste plus qu'à espérer que le traitement soit alors légitimé par d'autres motifs.

§ 7. Contrer les atteintes à la sécurité

Les atteintes à la sécurité de l'identification par radiofréquence ont pour conséquence le vol de données et d'identité.

La directive communications électroniques prévoit en vertu de son article 4 que « le fournisseur d'un service de communications électroniques accessible au public prend les

¹⁶⁴ Voy. *supra* pp. 54-57.

¹⁶⁵ Voy. les articles 23 et 24 de la directive n° 95/46/CE.

¹⁶⁶ Voy. *supra* p. 54.

mesures d'ordre technique et organisationnel appropriées afin de garantir la sécurité de ses services »¹⁶⁷. Les mesures d'ordre technique peuvent par exemple consister en la sécurisation renforcée des données contenues dans la mémoire de l'étiquette. L'article 4 prévoit également que « lorsqu'il existe un risque particulier de violation de la sécurité du réseau, le fournisseur d'un service de communications électroniques accessible au public informe les abonnés de ce risque et, si les mesures que peut prendre le fournisseur du service ne permettent pas de l'écarter, de tout moyen éventuel d'y remédier, y compris en indiquant le coût probable »¹⁶⁸. Le règlement 611/13 du 24 juin 2013 de la Commission concernant les mesures relatives à la notification des violations de données à caractère personnel organise quant à lui cette notification tant à la personne concernée qu'à l'autorité nationale compétente¹⁶⁹. Ces mesures sont d'application seulement en cas de violation des données détenues par le fournisseur de l'étiquette. C'est pourquoi l'article 30 de la proposition de règlement met en place un système comparable pour les données détenues légitimement par un responsable de traitement-lecteur d'étiquettes¹⁷⁰.

De plus, en vertu de son article 9, la directive 1999/5/CE dispose que « lorsqu'un Etat membre constate qu'un appareil relevant du champ d'application de la présente directive n'est pas conforme aux exigences de celles-ci, il prend toutes les mesures utiles sur son territoire pour retirer l'appareil du marché »¹⁷¹, l'une des exigences est la protection de la sécurité de l'utilisateur¹⁷².

Bref, l'Union européenne dispose de bases légales afin de prévenir les atteintes à la sécurité des données à caractère personnel. Mais qu'en est-il du pendant répressif d'une telle prévention ? La réponse doit probablement se trouver dans la législation nationale de chaque Etat membre.

§ 8. Conclusion

Le traitement des données issues de l'identification par radiofréquence n'est licite en droit de l'Union européenne que lorsqu'il y a consentement de la personne concernée par les données ou lorsqu'il existe d'autres motifs légitimes prévus par la loi. Ce traitement est soit réalisé par

¹⁶⁷ Article 4 de la directive n° 2002/58/CE.

¹⁶⁸ Article 4 de la directive n° 2002/58/CE.

¹⁶⁹ Règlement (UE) n° 611/13 du 24 juin 2013 de la Commission concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques, *J.O.U.E.*, L 173, 26 juin 2013.

¹⁷⁰ Article 30 de la proposition de règlement.

¹⁷¹ Article 9 de la directive n° 1999/5/CE.

¹⁷² Article 3 de la directive n° 1999/5/CE.

le fournisseur de l'étiquette et la base légale de la protection des données sera la directive 2002/58/CE ; soit réalisé par un responsable de traitement disposant d'un lecteur d'étiquettes et la base légale de la protection sera alors la directive 95/46/CE bientôt remplacée par le règlement faisant l'objet d'une proposition.

Diverses autres bases légales existent également afin de répondre à toutes les protections législatives que demande une telle technologie, tant au niveau de la sécurité que de la technique.

L'Union européenne dispose dès lors de tous les instruments législatifs pour contrer les problèmes liés à l'identification par radiofréquence mais ceux-ci souffrent d'un cruel manque d'effectivité. Ce dernier pourrait être comblé par l'autorégulation mise en place¹⁷³ mais ces divers documents datent de plusieurs années et l'information de l'individu, clé solutionnant les problèmes liés à l'identification par radiofréquence, est toujours inexistante.

Sans cette information essentielle, il est alors inopportun d'exposer les garanties qu'offrent la Charte des droits fondamentaux de l'Union européenne et la Convention européenne des droits de l'homme aux données à caractère personnel puisque le citoyen n'a pas conscience qu'un tel mécanisme est mis en place. En effet, comment pourrait-il en revendiquer la protection ?

Section 2. L'encadrement américain

L'étude des solutions est circonscrite au droit américain fédéral. Ce système repose en effet sur deux niveaux de pouvoir, l'un fédéral et l'autre fédéré, le droit des différents Etats. L'analyse législative ci-dessus se restreignant au droit de l'Union européenne, il était judicieux de limiter également l'étude du régime américain par la législation harmonisant celles des différents Etats (telle est également la *ratio legis* du droit de l'Union européenne). Il ne sera dès lors aucunement fait mention du droit des Etats même si, dans certains cas, ceux-ci auront été les premiers à établir une législation protectrice face au stoïcisme de l'Etat fédéral¹⁷⁴.

¹⁷³ Voy. par exemple Recommandation (UE) n° 2009/387/CE de la Commission du 12 mai 2009 sur la mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence, *J.O.U.E.*, L 122, 16 mai 2009 et GROUPE DE L'ARTICLE 29, « Avis 9/2011 sur la proposition révisée des entreprises relative au cadre d'évaluation de l'impact sur la protection des données et sur la vie privée des applications reposant sur l'identification par radiofréquence (RFID) », *W.P.* 180, 11 février 2011.

¹⁷⁴ Tel est le cas de la Californie avec l'adoption du Cal. Civ. Code §1789. 82.

§ 1^{er}. Analyse préliminaire

Tout comme le droit de l'Union européenne, le droit américain fédéral est en pleine mouvance concernant la protection des données à caractère personnel¹⁷⁵. En effet pour combler le manque accru de législations, de nombreuses propositions ont été envoyées au *Congress*, il nous sera dès lors impossible d'analyser chacune d'elles. Nous nommerons cependant la proposition *RFID Right to Know Act of 2003*¹⁷⁶ de l'association de consommateur CASPIAN qui a pour principal objectif l'information des consommateurs de la présence d'étiquettes sur les produits qu'ils achètent en magasins ; et la proposition *Personal Data Protection and Breach Accountability Act of 2014*¹⁷⁷ du Sénateur Richard Blumenthal, pouvant être comparée à la directive européenne sur la protection des données tout en pénalisant certaines violations de dispositions.

Ces propositions découlent du fait qu'il n'existe pas de législation générale concernant la protection des données en droit fédéral américain ; tout au plus, il existe le *Privacy Act*¹⁷⁸ s'appliquant uniquement aux administrations et le *Consumer Privacy Bill of Rights*¹⁷⁹ de la *White House*, pouvant être considéré comme des lignes directrices, des principes à suivre pour les entreprises dans leur rapport avec les données personnelles des individus, ceux-ci ayant été élaborés en vertu des *Fair Information Practices Principles*¹⁸⁰. Ces principes peuvent être résumés comme suit :

- « le principe de transparence qui oblige les organisations à être transparentes dans leur démarche de collecte, d'utilisation, de diffusion et de conservation des données à caractère personnel et les oblige à informer les individus d'une telle démarche ;
- le principe d'implication de l'individu qui oblige les organisations à impliquer les individus dans le processus d'utilisation de leurs données personnelles et dans la mesure du possible, à obtenir leur consentement individuel pour la collecte,

¹⁷⁵ Proposition de règlement 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 (règlement général sur la protection des données), document COM/2012/011, 25 janvier 2012.

¹⁷⁶ Proposition *RFID Right to Know Act of 2003*, disponible sur <http://www.nocards.org/rfid/rfidbill.shtml>, consulté pour la dernière fois le 30 juillet 2014.

¹⁷⁷ Proposition *Personal Data Protection and Breach Accountability Act of 2014*, disponible sur <https://beta.congress.gov/113/bills/s1995/BILLS-113s1995is.pdf>, consulté pour la dernière fois le 30 juillet 2014.

¹⁷⁸ Privacy Act, 5 U.S.C. § 552a.

¹⁷⁹ THE WHITE HOUSE, « Consumer data privacy in a networked world : a framework for protecting privacy and promoting innovation in the digital global economy », février 2012, disponible sur <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>, consulté pour la dernière fois le 30 juillet 2014.

¹⁸⁰ U.S. DEPT. OF HEALTH, EDUCATION AND WELFARE, « Record, computers and the rights of citizens », 1973, disponible que <http://www.rand.org/content/dam/rand/pubs/papers/2008/P5077.pdf>, consulté pour la dernière fois le 30 juillet 2014.

l'utilisation, la diffusion et la conservation des données à caractère personnel. Les organisations devraient également prévoir des mécanismes appropriés pour leur garantir l'accès aux données et leur rectification et le droit de recours concernant l'utilisation de celles-ci ;

- le principe de spécification des finalités qui oblige les organisations à informer l'individu sur l'autorité qui collecte les données à caractère personnel mais aussi la ou les finalités pour lesquelles les données sont collectées ;
- le principe de minimisation des données qui oblige les organisations à ne recueillir que des données directement pertinentes et nécessaires pour atteindre la finalité spécifiée et les oblige à conserver ces données pour aussi longtemps que nécessaire afin d'atteindre la finalité spécifiée ;
- le principe de limitation d'utilisation qui oblige les organisations à utiliser les informations personnelles uniquement dans la finalité spécifiée. S'il y a partage des données, celui-ci devra avoir une finalité compatible avec l'objectif pour lequel les données à caractère personnel ont été recueillies au départ ;
- le principe de qualité et d'intégrité des données qui oblige les organismes à vérifier, dans la mesure du possible, si les données à caractère personnel sont exactes, pertinentes, opportunes et complètes ;
- le principe de sécurité qui oblige les organisations à protéger les données à caractère personnel *via* une sécurité appropriée, ces protections seront par exemple, des garanties contre des risques tels que la perte, l'accès non autorisé ou l'utilisation, la destruction, la modification, ou la divulgation involontaire ou inappropriée ;
- et le principe de responsabilisation et d'audit qui responsabilise les organisations en les obligeant à respecter ces principes, par la formation de tous leurs employés et entrepreneurs qui utilisent les données à caractère personnel, et à contrôler l'utilisation réelle de ces données afin de démontrer le respect de ces principes et de toutes les exigences de protection de la vie privée applicables »¹⁸¹.

Il existe également des législations spécifiques mettant en œuvre une protection particulière pour un secteur particulier, tel est le cas par exemple du *Gramm-Leach-Bliley Act*¹⁸² protégeant les données à caractère personnel dans le secteur des institutions financières.

¹⁸¹ Traduction libre, voy. NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE, « Appendix A », disponible sur <http://www.nist.gov/nstic/NSTIC-FIPPs.pdf>, consulté pour la dernière fois le 30 juillet 2014.

¹⁸² Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809.

La jurisprudence de la *Supreme Court of the United States* n'éclaire pas non plus de manière significative les rapports entre les individus sur la notion de protection des données¹⁸³, celle-ci a d'ailleurs conclu à de nombreuses reprises qu'il n'y avait pas de violation de la vie privée lorsqu'une atteinte était portée à la protection des données entre personnes privées¹⁸⁴. Cette jurisprudence se base sur la théorie de l'acceptation des risques¹⁸⁵ selon laquelle un individu qui divulgue des informations personnelles le concernant accepte le risque que ses informations soient divulguées par après. Tandis que concernant les immixtions de l'Etat dans les affaires privées du citoyen, la *Supreme Court* a conclu qu'il y avait violation du droit à la protection des données à caractère personnel¹⁸⁶.

Bref, le droit américain fédéral à la protection des données est un droit dispersé qui ne s'applique qu'à des cas particuliers dans des secteurs particuliers, cela entraîne une inexistence de législation dans certains secteurs : par exemple, il n'existe au niveau fédéral aucune législation concernant la protection des données collectées par Amazon ou Facebook.

Dans une telle discorde au niveau des relations entre particuliers, l'autorégulation est dès lors une composante importante du droit à la protection des données de l'autre côté de l'Atlantique. Cette autorégulation est contrôlée par une autorité indépendante, la *Federal Trade Commission*. Celle-ci dispose d'un pouvoir de contrôle du respect des engagements des entreprises et ce dernier est extrêmement large en vertu du *Federal Trade Commission Act*¹⁸⁷ ; sa jurisprudence administrative et les *settlements*¹⁸⁸ conclus avec les entreprises sont d'ailleurs devenus en quinze ans, la source de droit concernant la vie privée la plus large et la plus contraignante des Etats Unis, devant la législation et les *Common Law Tort* (la jurisprudence)¹⁸⁹. Armée des *Fair Information Practices Principles* et des *Privacy Policy* élaborées par les entreprises (ensemble de règles concernant la vie privée que les entreprises s'engagent à respecter), la *FTC* domine le droit de la protection des données à caractère

¹⁸³ N.M. RICHARDS, « The Limits of Tort Privacy », *Journal of Telecommunications and High Technology Law*, Vol. 9, 2011, disponible sur http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1862264, consulté pour la dernière fois le 30 juillet 2014.

¹⁸⁴ Voy. notamment *Donaldson v. United States*, 400 U.S. 517 (1971) et *United States v. Miller*, 425 U.S. 435 (1976).

¹⁸⁵ *United States v. White*, 401 U.S. 745 (1971).

¹⁸⁶ Voy. notamment *Katz v. United States*, 389 U.S. 347 (1967).

¹⁸⁷ Federal Trade Commission Act, 15 U.S.C. §§ 41-58.

¹⁸⁸ Les *settlements* sont des accords conclus entre la *FTC* et les entreprises et ayant pour objectif de régler le conflit afin d'éviter de présenter le cas devant un juge.

¹⁸⁹ W. HARTZOG et D.J. SOLOVE, « The FTC and the New Common Law of Privacy », *Columbia Law Review*, Vol. 114, 583, 2013, pp. 585 et s, disponible sur http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913, consulté pour la dernière fois le 30 juillet 2014.

personnel. Le champ d'application émanant des principes de la *FTC* est alors défini au cas par cas par les *Privacy Policy* et ne peut faire l'objet d'une étude détaillée.

En vertu du *Federal Trade Commission Act*, la *FTC* a le pouvoir d'interdire des *deceptive trade practices* ou des *unfair trade practices*¹⁹⁰. Les premières font référence non seulement « aux promesses non-tenues concernant la vie privée et la sécurité mais aussi à une théorie générale de tromperie dans l'obtention de renseignements personnels et dans la notification d'information de l'individu concernant la violation de sa vie privée lorsque cette information est non-suffisante »¹⁹¹ tandis que les secondes font référence « au changement rétroactif des *Privacy Policy*, à la collecte trompeuse de données, à une mauvaise utilisation des données, au fait que les données ne soient pas collectées en vue de respecter le droit à la vie privée et aux pratiques de sécurité de l'information déloyales »¹⁹².

En vertu des législations *FCRA*¹⁹³, *COPPA*¹⁹⁴ et *GLBA*¹⁹⁵, la *FTC* a également le pouvoir de contrôler leur application effective et de poser des sanctions en cas de manquement. Ces législations semblent cependant difficilement applicables à l'identification par radiofréquence.

La *FTC* a également un pouvoir de contrôle sur l'application du *Safe Harbor* mais la présente recherche n'a pas pour objet d'étude la transmission transnationale de données¹⁹⁶.

Mais qu'en est-il des réponses qu'apporte le régime juridique fédéral américain aux problèmes posés au titre 2 ?

§ 2. Contrer le caractère invisible

Comme exposé ci-dessus¹⁹⁷, afin de contrer le caractère invisible de l'identification par radiofréquence, il est nécessaire d'informer l'individu d'une part de manière générale par une information à la société sur ce qu'est la technologie et, d'autre part par une information individuelle à propos de la présence d'une étiquette sur un objet qu'il acquiert.

L'information générale sur la technologie est bien plus présente aux Etats-Unis qu'en Europe. Grâce à elle, les citoyens se sentent concernés lorsqu'il est fait mention d'identification par

¹⁹⁰ Federal Trade Commission Act, 15 U.S.C. § 45.

¹⁹¹ Traduction libre, voy. W. HARTZOG et D. J. SOLOVE, *op. cit.*, pp. 628 et s.

¹⁹² *Idem.*

¹⁹³ Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681x.

¹⁹⁴ Children's Online Privacy Protection, 15 U.S.C. §§ 6501-6506.

¹⁹⁵ Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809.

¹⁹⁶ Pour de plus amples informations, voy. par exemple <http://www.export.gov/safeharbor/index.asp>.

¹⁹⁷ Voy. *supra* pp. 50 et s.

radiofréquence. Ce propos peut par exemple être illustré par l'hoax¹⁹⁸ de l'*Obama Care* par lequel circulait l'information que le département américain de la santé allait obliger tout citoyen à s'insérer une étiquette d'identification par radiofréquence sous-cutanée pour raisons médicales : l'hoax fait l'objet d'environ 1.320.000 résultats sur Google¹⁹⁹, les américains ont donc connaissance qu'un tel mécanisme d'identification existe. Cependant, malgré ce sentiment d'inquiétude face à l'insertion sous-cutanée d'une étiquette d'identification, les citoyens américains ne sont pas plus informés sur les applications de la vie courante de l'identification par radiofréquence, que les citoyens européens.

De même, alors que les principes émergeant des pouvoirs de la *FTC*, tel que la nécessité d'informer l'individu sur la collecte possible des données à caractère personnel²⁰⁰; pourraient obliger les entreprises à informer les individus sur la présence d'une étiquette apposée sur les objets qu'ils achètent, il n'en est rien en réalité : vous pouvez aller acheter une tablette Apple aux Etats-Unis sans que le vendeur ne vous prévienne qu'une étiquette d'identification se trouve à l'intérieur du produit. Si la personne qui fournit l'étiquette est un représentant de l'Etat, le *Privacy Act* sera d'application et imposera l'information du citoyen²⁰¹.

Bien que bénéficiant d'une information un peu plus diluée dans la société concernant l'existence d'une telle technologie, le régime américain souffre du même problème d'effectivité que le régime européen. Tous deux disposent en effet de sources juridiques pouvant contrer le problème d'invisibilité mais aucun n'arrive à l'appliquer adéquatement à l'identification par radiofréquence.

§ 3. Contrer le caractère indéfini

Afin de contrer cet obstacle, la désactivation de l'étiquette devrait être possible et à la portée de tout utilisateur²⁰².

Les *Fair Information Practices Principles*²⁰³ imposent une obligation aux organisations de protéger les données à caractère personnel *via* une sécurité appropriée. Ces *FIPPs* sont à la

¹⁹⁸ Un hoax est un canular.

¹⁹⁹ En recherchant les mots : RFID Obama care.

²⁰⁰ Voy. par exemple, *Sony BMG Music Entm't*, FTC File No. 062 3019, No. C- 4195 (F.T.C. June 28, 2007), disponible sur <http://www.ftc.gov/sites/default/files/documents/cases/2007/01/070130cmp0623019.pdf>, consulté pour la dernière fois le 30 juillet 2014.

²⁰¹ Privacy Act, 5 U.S.C. § 552a.

²⁰² Voy. raisonnement *supra* pp. 52 et s.

²⁰³ U.S. DEPT. OF HEALTH, EDUCATION AND WELFARE, « Record, computers and the rights of citizens », *op. cit.*.

base de la législation du *Privacy Act* et fondent les principes de la *FTC*²⁰⁴. Tant les entreprises que les administrations devraient alors, en vue de protéger les données à caractère personnel, permettre la désactivation de l'étiquette, celle-ci pouvant être définie comme une mesure de sécurité puisqu'elle vise à garantir des risques tels que la perte, la destruction, la modification, etc²⁰⁵.

En réalité, aucune possibilité de désactivation de l'étiquette n'est proposée à la personne concernée ; au mieux, si cette dernière a connaissance qu'une telle étiquette est apposée sur l'un de ses objets, il suffit de la détruire mais la plupart du temps, l'individu n'a pas conscience que les objets qui l'entourent relèvent de l'intelligence ambiante.

Le régime américain, tout comme le régime européen, dispose également de bases juridiques, même si elles sont de nature différente, afin de contrer le caractère indéfini de l'identification par radiofréquence mais aucun des deux régimes ne proposent de solutions effectives à la personne concernée.

§ 4. Contrer le caractère interopérable

Une des solutions pour contrer l'interopérabilité de l'identification par radiofréquence pourrait être la sécurisation des données²⁰⁶.

Comme expliqué au point précédent, tant les entreprises que les administrations doivent respecter les *FIPPs* qui imposent une obligation de protéger les données à caractère personnel via une sécurité appropriée. Elles devraient alors, en vue de protéger les données à caractère personnel, sécuriser les étiquettes qu'elles fournissent de façon sommaire ou complexe en fonction des données à protéger²⁰⁷. Cette sécurisation peut être définie comme une mesure de sécurité puisqu'elle vise à garantir des risques tels que l'accès non autorisé et la divulgation involontaire ou inappropriée²⁰⁸.

Cette obligation est assortie d'une peine pénale en vertu de l'*Electronic Communication Privacy Act*²⁰⁹ qui dispose qu'« est punie d'une amende ou d'un emprisonnement de maximum cinq ans la personne qui intercepte intentionnellement par des dispositifs

²⁰⁴ *Compete, Inc.*, FTC File No. 102 3155, No. C-4384 (F.T.C. Feb. 20, 2013), disponible sur <http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130222competecmpt.pdf>, consulté pour la dernière fois le 30 juillet 2014.

²⁰⁵ Voy. NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE, « Appendix A », *op.cit.*.

²⁰⁶ Voy. *supra* pp. 54 et s.

²⁰⁷ *Compete, Inc.*, FTC File No. 102 3155, *op. cit.*.

²⁰⁸ Voy. NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE, « Appendix A », *op. cit.*.

²⁰⁹ Electronic Communication Privacy Act, 18 U.S.C. §2511.

électroniques, une communication électronique ; à moins que cette personne détienne le consentement d'une des parties à la communication »²¹⁰. L'identification par radiofréquence est une communication électronique²¹¹. Cette disposition pénale s'applique alors à toute personne interceptant les données présentes sur la mémoire de l'étiquette pour autant que cette personne ne possède pas le consentement de la personne ayant en sa possession l'étiquette. Une telle peine a pour corollaire l'atténuation de l'interopérabilité de l'identification par radiofréquence.

Cependant, aucune condamnation n'a déjà été prononcée en défaveur d'une personne interceptant des données à caractère personnel issues de l'identification par radiofréquence. L'effectivité d'une telle norme est mise à mal quand elle doit s'appliquer à un tel mécanisme, comme c'est le cas dans le régime européen. La peine pénale devrait cependant faciliter l'application d'une telle norme au problème posé.

§ 5. Contrer la traçabilité

Afin de contrer la traçabilité effectuée via l'identification par radiofréquence, il convient d'établir si le traitement des données de localisation est licite ou non. Si le traitement est illicite, la traçabilité du mécanisme sera anéantie car illégale.

Les *FIPPs* prévoient que la personne doit consentir au traitement de ses données personnelles pour autant qu'il n'existe pas d'autres motifs légitimant le traitement²¹². Tant les entreprises que les administrations doivent alors disposer, le cas échéant, du consentement de la personne concernée avant de tracer celle-ci *via* les données de localisation²¹³.

Cette obligation est assortie d'une peine pénale en vertu du *GPS Act*²¹⁴ qui dispose qu'« est punie d'une amende ou d'un emprisonnement de maximum cinq ans la personne qui intercepte intentionnellement par des dispositifs électroniques une information GPS à moins que cette personne détienne le consentement d'une des parties à la communication »²¹⁵. Cette législation a été adoptée suite à l'arrêt *United States v. Jones*²¹⁶ dans lequel la *Supreme Court*

²¹⁰ Traduction libre de l'Electronic Communication Privacy Act, 18 U.S.C. §2511.

²¹¹ Voy. *supra* pp. 47 et s., l'analyse européenne sur la caractérisation de l'identification par radiofréquence comme communication électronique.

²¹² Voy. NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE, « Appendix A », *op.cit.*

²¹³ Voy. la Complaint for Injunctive and Other Equitable Relief in *FTC v. Accusearch Inc.*, No. 06-CV-0105 (D. Wyo. Sept. 28, 2007), disponible sur <http://www.ftc.gov/sites/default/files/documents/cases/2006/05/060501accusearchcomplaint.pdf>, consulté pour la dernière fois le 30 juillet 2014.

²¹⁴ GPS Act, 18 U.S.C. §§ 2601-2605.

²¹⁵ Traduction libre de GPS Act, 18 U.S.C. §§ 2601-2605.

²¹⁶ *United States v. Jones*, 132 S. Ct. 945, (2012).

conclu que le 4^{ème} amendement du *Bill of Rights* est d'application pour les localisations GPS. L'identification par radiofréquence est une information GPS puisque celle-ci permet la localisation d'une étiquette dans un champ électromagnétique. Cette disposition pénale s'applique alors à toute personne interceptant les données de localisation pour autant que cette personne ne possède pas le consentement de la personne ayant en sa possession l'étiquette.

Le droit fédéral américain bénéficie donc de bases juridiques pour contrer la traçabilité, tout comme le régime européen, mais l'effectivité reste à prouver quant à leur application à l'identification par radiofréquence.

§ 6. Contrer le profilage

Tout comme la traçabilité, le profilage est relatif au consentement et à la licéité du traitement de données. Si le traitement est illicite, le profilage le sera également.

Comme exposé ci-dessus, les *FIPPs* prévoient que la personne doit consentir au traitement de ses données personnelles pour autant qu'il n'existe par d'autres motifs légitimant le traitement²¹⁷. Tant les administrations que les entreprises doivent alors, le cas échéant, détenir le consentement de la personne concernée avant de collecter ses données en vue de son profilage²¹⁸.

Cette obligation est assortie d'une peine pénale en vertu de l'*Electronic Communication Privacy Act*²¹⁹ qui dispose qu'« est punie d'une amende ou d'un emprisonnement de maximum cinq ans la personne qui intercepte intentionnellement par des dispositifs électroniques, une communication électronique ; à moins que cette personne détienne le consentement d'une des parties à la communication »²²⁰. Comme expliqué ci-dessus, l'identification par radiofréquence est une communication électronique et cette disposition pénale s'applique alors à toute personne interceptant les données présentes sur la mémoire de l'étiquette pour autant que cette personne ne possède pas le consentement de la personne ayant en sa possession l'étiquette.

Aucune condamnation n'a cependant été prononcée actuellement en défaveur d'une personne interceptant des données à caractère personnel issues de l'identification par radiofréquence. Bien que la sanction pénale présente dans le régime américain devrait suffire à contrer le

²¹⁷ Voy. NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE, « Appendix A », *op.cit.*.

²¹⁸ Voy. la Complaint for Injunctive and Other Equitable Relief in *FTC v. Accusearch Inc.*, *op.cit.*.

²¹⁹ Electronic Communication Privacy Act, 18 U.S.C. § 2511.

²²⁰ Traduction libre de l'Electronic Communication Privacy Act, 18 U.S.C. § 2511.

profilage illégitime issu de données d'identification par radiofréquence, ce dernier souffre toujours du même mal d'effectivité que le régime européen.

§ 7. Contrer les atteintes à la sécurité

Le vol de données et d'identité sont les principales conséquences des atteintes à la sécurité de l'identification par radiofréquence.

Comme exposé ci-dessus, les entreprises et les administrations ont l'obligation en vertu des *FIPPs* et des différentes sources juridiques en découlant, de sécuriser les étiquettes d'identification par radiofréquence en vue de garantir les risques de malveillance²²¹.

Cette obligation est assortie de peines pénales. Concernant le vol de données, nous nous référons à l'exposé relatif au profilage²²². Concernant le vol d'identité, l'article § 1028a du titre 18 du U.S. Code²²³ punit « la personne qui, au cours d'un traitement de données à caractère personnel illégal, transfère sciemment, possède ou utilise, sans autorisation légale, un moyen d'identification d'une autre personne ; à une peine d'emprisonnement de deux ans en plus de la peine prévue pour le crime »²²⁴. Cette disposition pénale s'applique alors à toute personne volant l'identité d'une autre *via* l'identification par radiofréquence.

Comme pour les autres solutions aux problèmes, l'application de ces dispositions à l'identification par radiofréquence pose un problème d'effectivité tant dans le régime américain que dans le régime européen puisque la personne concernée n'a pas conscience du processus d'identification en jeu et donc encore moins du possible vol de données ou d'identité.

§ 8. Conclusion

Le traitement des données issues de l'identification par radiofréquence n'est licite en droit fédéral américain que lorsqu'il y a consentement de la personne concernée par les données ou lorsqu'il existe d'autres motifs légitimes. Le consentement est donc une condition de licéité d'un traitement dans les deux régimes juridiques étudiés.

Le droit fédéral américain distingue l'application des diverses sources juridiques en fonction non pas du fournisseur-lecteur d'étiquettes comme le fait le droit de l'Union européenne mais bien en fonction de la qualité de la personne : personne privée physique, personne privée

²²¹ Voy. NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE, « Appendix A », *op.cit.*.

²²² Voy. *supra* pp. 68 et s.

²²³ 18 U.S.C. § 1028a.

²²⁴ Traduction libre de l'article 18 U.S.C. § 1028a.

morale ou personne de droit public. Cette différence a pour conséquence que les obligations incombant au fournisseur de l'étiquette ne sont pas explicitées de manière claire en droit fédéral américain car celui-ci s'applique plus particulièrement aux traitements des données et à leur répression pénale. Les obligations du fournisseur devront alors faire l'objet soit d'une loi générale fédérale, soit d'une interprétation de la *FTC*.

La protection des données à caractère personnel est assurée inconditionnellement lorsque la fourniture de l'étiquette ou le traitement est exécuté par une personne de droit public.

Si ces derniers sont réalisés par une entreprise, la protection sera assurée par les *Privacy Policy* que cette dernière aura rédigées en fonction de principes généraux édictés par le Gouvernement américain et contrôlées par la *FTC*, la protection sera donc moins absolue.

Le droit fédéral américain ne garantit cependant aucune protection concernant la prévention des atteintes à la vie privée des individus si la personne qui viole le droit à la protection des données à caractère personnel est une personne physique privée. L'atteinte des personnes physiques privées au droit à la protection des données à caractère personnel des individus est tout de même punie en vertu du titre *Crimes and Criminal Procedure* de l'U.S.Code²²⁵.

Les Etats-Unis disposent alors de la plupart des instruments juridiques pour contrer les problèmes liés à l'identification par radiofréquence mais ceux-ci souffrent d'un cruel manque d'effectivité, manque également mis en avant dans l'analyse du droit de l'Union européenne alors que les deux régimes disposent d'un système juridique différent.

Ce manque d'effectivité est dû, il nous semble, à la piètre information de l'individu, clé solutionnant les problèmes liés à l'identification par radiofréquence. Suite à cela, il est alors inopportun d'exposer les garanties qu'offrent les traités de droit international au citoyen américain puisque celui qui n'a pas conscience qu'un tel mécanisme est mis en place ne peut en revendiquer la protection.

²²⁵ 18 U.S.C. §§ 1-6005.

Chapitre 2. Comment expliquer ces disparités ?

Les deux régimes étudiés présentent de nombreuses disparités quant au fonctionnement de leur système alors que leurs régimes juridiques applicables à la protection des données à caractère personnel sont plus ou moins équivalents.

Les disparités systémiques peuvent s'expliquer principalement par l'importance que porte le droit américain au droit à la sécurité. Le droit à la sécurité est celui qui a pour but de garantir une «situation dans laquelle quelqu'un, quelque chose n'est exposé à aucun danger, à aucun risque, en particulier d'agression physique, d'accidents, de vol, de détérioration»²²⁶. Cet intérêt porté à la sécurité s'est accru suite aux attentats du 11 septembre 2001, ayant pour corollaire l'immixtion de l'Etat dans les affaires privées du citoyen afin de garantir la sécurité. Une telle position de l'Etat, déjà repérable sous le Gouvernement de Clinton qui préférait laisser la protection de la vie privée à l'autorégulation²²⁷, implique forcément une absence de protection de la vie privée du citoyen au niveau législatif ou à tout le moins une protection dérisoire. La politisation de la *Supreme Court* américaine explique également que cette dernière n'ait pas interprété de façon large la notion de vie privée. La régulation nécessaire a alors été créée par un organe indépendant, soucieux du bien-être des consommateurs. Tandis qu'en Europe, la création des droits de l'homme, et donc la consécration législative de la vie privée, découlait des atrocités vécues lors de la deuxième guerre mondiale, la protection mise en place avait donc un caractère beaucoup plus absolu et ne pouvait permettre les ingérences de l'Etat que dans les cas déterminés par la loi si ceux-ci étaient proportionnels et nécessaires dans une société démocratique²²⁸. Cela a eu pour conséquence que l'Union européenne ait adopté de nombreuses législations afin d'assurer une protection effective de ce droit.

Nous pouvons remarquer que dans les deux régimes juridiques analysés, la mise en balance des intérêts soit de l'Etat et des citoyens, soit de l'entreprise et des consommateurs²²⁹ en est une caractéristique. La protection des données à caractère personnel n'est donc pas absolue puisque de telles données représentent un intérêt tant pour l'Etat au niveau de la sécurité et de la répression des crimes que pour les entreprises à des fins commerciales et de marketing.

²²⁶ Tel que défini par le dictionnaire Larousse, disponible sur <http://www.larousse.fr/dictionnaires/francais/s%C3%A9curit%C3%A9/71792>, consulté pour la dernière fois le 30 juillet 2014.

²²⁷ W. HARTZOG et D. J. SOLOVE, « The FTC and the New Common Law of Privacy », *op. cit.*, p. 594.

²²⁸ Article 8 CEDH.

²²⁹ Voy. par exemple les articles fondant la législation européenne qui ont pour objectif de garantir le marché commun au sein de l'Union.

Les régimes juridiques étudiés présentent malgré la différence systémique, les mêmes caractéristiques : nécessité de consentement ou d'autres motifs légitimes, information de la personne concernée, droit d'accès et de rectification, droit d'opposition, etc. Une telle comparabilité est logique puisque ces caractéristiques sont à même, de façon abstraite, à protéger correctement les données à caractère personnel. Nous noterons également que celles-ci sont explicitées dans les lignes directrices de l'OCDE²³⁰. Cela ne veut pas dire que les deux régimes ont simplement recopié les lignes directrices mais plutôt, que ces dernières ayant synthétisé les deux régimes, sont arrivées à la même conclusion que nous : les caractéristiques présentes dans les deux régimes sont inhérentes à la protection des données à caractère personnel.

Un autre élément de comparabilité est l'ineffectivité de la protection juridique existante concernant son application à l'identification par radiofréquence. Comme énoncé plus haut, cette ineffectivité nous semble être la conséquence directe du manque d'information de l'individu sur l'existence même de l'identification par radiofréquence. Tout un chacun ne perçoit pas le processus en jeu, et ne pourrait donc en appréhender les risques. Tant que l'individu ne réclamera pas une protection adéquate pour ses données issues de l'identification par radiofréquence, les autorités ne forceront ni les entreprises, ni les administrations à respecter le régime de protection mis en place, nous semble-t-il.

²³⁰ OCDE, « Lignes directrices régissant la protection de la vie privée et les flux transfrontaliers de données de caractère personnel », 23 septembre 1980, disponible sur <http://www.oecd.org/fr/internet/ieconomie/lignesdirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm>, consulté pour la dernière fois le 30 juillet 2014.

Chapitre 3. Solution globale ?

La clé de la solution devrait être l'information de l'individu, tant au niveau général par une conscientisation de la population de l'existence d'un tel mécanisme, qu'au niveau individuel lors de la fourniture d'une étiquette. Cette information entraînera une responsabilisation de l'individu sur ses données à caractère personnel et ce dernier aura alors le choix, en tout état de cause, d'accepter le traitement de ses données afin de participer légitimement à la croissance des bases de données pour faciliter la vie de tout un chacun par la proposition de services personnalisés grâce à des profils ; ou de ne pas consentir au traitement de ses données.

Par cette information, l'individu aura la capacité d'ester en justice ou de porter plainte auprès d'une autorité indépendante lorsqu'il prendra conscience que ses droits ne sont pas respectés. Le régime de protection n'en ressortira que plus effectif.

Ce devoir d'information générale devrait incomber à une autorité indépendante disposant d'une large autonomie de pouvoir, telle que la *FTC*. Autorité manquante au niveau européen : on ne peut en effet comparer le Groupe de l'article 29 à la *FTC*.

La *FTC* détient son autorité à l'égard des entreprises américaines via la crainte d'une expertise approfondie du respect des obligations incombant au responsable du traitement des données²³¹. Cette expertise dure en moyenne vingt ans, le processus de vérification étant exhaustif et exigeant. Elle évalue par exemple « la façon dont les garanties de protection de la vie privée sont appropriées à la taille et à la complexité de l'entreprise, la nature et la portée des activités de l'entreprise ainsi que la sensibilité du dispositif visé au niveau fonctionnel ou encore les données couvertes par la protection »²³². Vingt années d'analyse coûtent énormément à une entreprise tant au niveau du coût à proprement parler, qu'au niveau temps et personnel à y consacrer. Une entreprise préfère alors adapter ses *Privacy Policy* et respecter les principes dégagés par la *FTC* plutôt que de risquer une telle évaluation. Un mécanisme de pression autre que pécuniaire est une très bonne solution sachant que les entreprises traitant les données à caractère personnel sont le plus souvent des multinationales pour lesquelles la crainte d'une amende est futile.

²³¹ W. HARTZOG et D. J. SOLOVE, « The FTC and the New Common Law of Privacy », *op. cit.*, p. 606.

²³² Traduit librement de W. HARTZOG et D. J. SOLOVE, « The FTC and the New Common Law of Privacy », *op. cit.*, p. 606.

En plus du cadre législatif européen plutôt satisfaisant dans l'ensemble, l'existence d'une autorité indépendante comparable à la *FTC* serait nécessaire afin d'appliquer de manière effective le régime de protection.

De même qu'une harmonisation des sanctions au niveau européen, comme c'est le cas au niveau fédéral américain, permettrait une application plus effective de la législation et contrecarrerait un « forum shopping »²³³ des sociétés.

²³³ Le forum shopping est la possibilité pour une entreprise de choisir le juge qui sera le plus clément envers la violation dont elle est l'auteur, voy. l'explication donnée par l'Union européenne, disponible sur http://ec.europa.eu/justice/glossary/forum-shopping_fr.htm, consulté pour la dernière fois le 30 juillet 2014.

Conclusion

La présente recherche avait pour ambition de définir ce qu'est l'identification par radiofréquence, d'en analyser les risques en vertu de la vie privée comme valeur et non comme droit ; et d'examiner les différentes solutions que le droit de l'Union européenne et le droit américain fédéral proposent à ces problématiques pour en ressortir une solution globale.

L'identification par radiofréquence peut être définie comme une nouvelle technologie de l'information et de la communication par laquelle une étiquette apposée sur un objet ou une personne, communique les données présentes dans sa mémoire interne *via* des ondes électromagnétiques, à un lecteur qui identifie l'étiquette et les données qu'elle contient.

L'identification par radiofréquence ayant pour objet la collecte de données, la question s'est posée de savoir s'il l'on pouvait caractériser celles-ci de personnelles. Nous avons conclu à une réponse positive puisque les données bien que relatives à un objet, localisent la personne qui détient celui-ci et permettent par exemple, d'en dresser le profil de consommation. Ces données sont donc personnelles au sens commun du terme car elles sont relatives à une personne. Nous avons ensuite analysé les six risques potentiels que représente l'identification par radiofréquence : le caractère invisible, indéfini et interopérable du mécanisme, la traçabilité, le profilage et les atteintes à la sécurité des données. Cette technologie ne collectant plus de simples données mais des données concernant des personnes, il était alors pertinent de se demander si la vie privée de celles-ci était atteinte lors d'un tel traitement. Par l'impossibilité de définir le concept de vie privée, celui-ci étant contextuel et vague à souhait, nous avons retracé l'évolution du concept en partant de la vie privée comme valeur pour en arriver au droit à la protection des données à caractère personnel et constater dès lors, que la collecte des données issues de l'identification par radiofréquence devait bénéficier de cette protection.

Nous avons alors étudié les régimes juridiques du droit de l'Union européenne et du droit américain fédéral afin de déterminer s'ils accordent une telle protection aux données issues de l'identification par radiofréquence. Suite à cette étude, nous en avons conclu que les régimes juridiques disposent chacun de bases juridiques pouvant protéger les données issues de l'identification par radiofréquence ; bien que leur système soit profondément différent l'un de l'autre, le premier reposant sur un corpus législatif solide, le second sur des *settlements* d'une autorité indépendante en matière de vie privée. Cependant, ces régimes sont ineffectifs en pratique, l'application de leurs bases juridiques à l'identification par radiofréquence étant la

plupart du temps inexistante. Une telle ineffectivité découle selon nous, du manque d'information de l'individu sur l'existence même de l'identification par radiofréquence et des risques inhérents à celle-ci. Par-là, humblement, nous proposons alors à une autorité indépendante disposant d'une autonomie de pouvoir assez large comme la *FTC* américaine d'informer le public au sujet de l'identification par radiofréquence afin d'assurer une meilleure effectivité aux bases juridiques en vigueur.

Loin d'être terminée, l'analyse des risques liés à l'identification par radiofréquence dévoile d'autres problématiques : les étiquettes fonctionnent en effet sur base d'ondes électromagnétiques, dont les médias nous répètent sans cesse qu'elles représentent un danger pour la santé. Quelles en seront alors les conséquences ? L'avenir nous le dira...

Bibliographie

Législation

Nations Unies

Déclaration universelle des droits de l'homme du 10 décembre 1948 ;

Pacte international du 16 décembre 1966 relatif aux droits civils et politiques.

Conseil de l'Europe

Convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 ;

Convention n°108 du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

Organisation des Etats américains

American Declaration of the Rights and Duties of Man, adoptée par la neuvième conférence internationale des Etats américains en avril 1948.

Union Européenne

Traité sur l'Union européenne ;

Traité sur le fonctionnement de l'Union européenne ;

Charte des droits fondamentaux de l'Union européenne ;

Règlement (UE) n° 611/13 du 24 juin 2013 de la Commission concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques, *J.O.U.E.*, L 173, 26 juin 2013 ;

Directive (CE) n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 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, *J.O.C.E.*, L 281, 23 novembre 1995 ;

Directive (CE) n° 1999/5/CE du Parlement européen et du Conseil du 9 mars 1999 concernant les équipements hertziens et les équipements terminaux de télécommunications et la reconnaissance mutuelle de leur conformité, *J.O.C.E.*, L 91, 7 avril 1999 ;

Directive (CE) n° 2002/21/CE du Parlement européen et de Conseil du 27 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, *J.O.C.E.*, L 108, 24 avril 2002 ;

Directive (CE) n° 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, *J.O.C.E.*, L 201, 31 juillet 2002 ;

Directive (CE) n° 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, *J.O.U.E.*, L 105, 13 avril 2004 ;

Directive (CE) n°2009/136/CE du Parlement européen et de Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la 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 et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs, *J.O.U.E.*, L 337, 18 décembre 2009 ;

Proposition de règlement 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 (règlement général sur la protection des données), document COM/2012/011, 25 janvier 2012 ;

Amendement 98 de la résolution législative de Parlement européen du 12 mars 2014 sur la proposition de règlement 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, disponible sur <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//FR>.

Etats-Unis

Bill of Rights ;

Privacy Act, 5 U.S.C. § 552a ;

Federal Trade Commission Act, 15 U.S.C. §§ 41-58 ;

Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681x ;

Children's Online Privacy Protection, 15 U.S.C. §§ 6501-6506 ;

Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809 ;

18 U.S.C. §§ 1-6005 ;

18 U.S.C. § 1028a ;

Electronic Communication Privacy Act, 18 U.S.C. § 2511 ;

GPS Act, 18 U.S.C. §§ 2601-2605 ;

Proposition *RFID Right to Know Act of 2003*, disponible sur <http://www.nocards.org/rfid/rfidbill.shtml> ;

Proposition *Personal Data Protection and Breach Accountability Act of 2014*, disponible sur <https://beta.congress.gov/113/bills/s1995/BILLS-113s1995is.pdf> ;

Cal. Civ. Code §1789. 82.

Belgique

Proposition de loi modifiant la législation relative à la protection de l'enfant, en ce qui concerne l'instauration de la parentalité sociale, Avis du Conseil d'Etat, *Doc. parl.*, Chambre, 2007-2008, n°52 1303/002.

Jurisprudence

Cour européenne des droits de l'homme

Cour eur. D. H., arrêt Niemetz c. Allemagne, 16 décembre 1992, *Rev. trim. dr. h.*, 1993, p. 647.

Cour de justice de l'Union européenne

C.J.C.E., 6 novembre 2003 (Procédure pénale contre Bodil Lindqvist), 6 novembre 2003, C-101/01, disponible sur <http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=27533>.

Supreme Court of United States

Boyd v. United States, 116 US 616 (1886) ;

Katz v. United States, 389 U.S. 347 (1967) ;

Donaldson v. United States, 400 U.S. 517 (1971) ;

United States v. White, 401 U.S. 745 (1971) ;

United States v. Miller, 425 U.S. 435 (1976) ;

United States v. Jones, 132 S. Ct. 945, (2012).

Jurisprudence nationale anglaise

Abernethy v. Hutchinson, 1 H. and Tw. 28 (1825), 47 ER 1313 (Chanc.) ;

Prince Albert v. Strange, 2DeG. And Sm. 712 (1849), 64 ER, 293 (Chanc.).

Doctrine et autres contributions scientifiques

Ouvrages

Monographies

BENSOUSSAN A., *Informatique et libertés*, Levallois, Editions Francis Lefebvre, 2010 ;

DOCQUIR B., *Le droit à la vie privée*, Bruxelles, Larcier, 2008 ;

MICHAEL J., *Privacy and Human Right – An International and Comparative Study With Special Reference to Developments in Information Technology*, Dartmouth, UNESCO Publishing, 1994 ;

NADEAU A.R., *Vie privée et droits fondamentaux*, Canada, Editions Yvon Blais Inc., 2000 ;

SOLOVE D.J., *The digital Person*, New York and London, New York University Press, 2004;

WESTIN A.F., *Privacy and Freedoms*, New York, Atheneum, 1967.

Ouvrages collectifs

X., *Défis du droit à la protection de la vie privée* (sous la dir. de VERONICA M. et PALAZZI P.), Bruxelles, Bruylant, 2008 ;

X., *Reinventing Data Protection ?* (sous la dir. de GUTWIRTH S. et POULLET Y.), Dordrecht, Springer Editions, 2009 ;

X., *RFID, Applications, Security, and Privacy* (sous la dir. de GARFINKEL S. et ROSENBERG B.), Upper Saddle River, New Jersey, Addison-Wesley, 2006;

X., *Safeguards in a world of Ambient Intelligence* (sous la dir. de WRIGHT D. et AHONEN P.), New-York, Springer Editions, 2008.

Contributions à des ouvrages collectifs et à des périodiques

Contributions à des ouvrages collectifs

AVOINE G., « Sécurité de la RFID : comprendre la technique sans être un technicien », in *La sécurité de l'individu numérisé : réflexions prospectives et internationales*, (sous la dir. de LACOUR S.), Paris, L'Harmattan, 2008, pp. 17-27 ;

BENN S., « Privacy, Freedom and Respect for Persons », in *Privacy (Nomos XIII)* (sous la dir. de PENNOCK J.R. et CHAPMAN J.W.), New York, Atherton Press, 1971, pp. 71-74 ;

BURKERT H., « Introduction. Dualities of privacy – An introduction to « personal data protection and fundamental rights », in *Défis du droit à la protection de la vie privée* (sous la dir. de VERONICA M. et PALAZZI P.), Bruxelles, Bruylant, 2008, pp. 14-23 ;

DE HERT P. et RAAB C., « Tools for Technology Regulation: Seeking Analytical Approaches Beyond Lessig and Hood », in *Regulating Technologies: legal futures, regulatory frames and technological fixes*, (sous la dir. de BROWNSWORD R. et YEUNG K.), Oxford, Hart, 2008, pp. 263-285 ;

DE TERWANGNE C. et LOUVEAUX S., « Protection des données à caractère personnel : application en Belgique de la directive européenne », in *Actualité du droit des techniques de l'information et de la communication*, Liège, CUP, 2001, vol. 45, pp. 9-34 ;

FISHKIN K. et LUNDELL J., « RFID in Healthcare », in *RFID, Applications, Security, and Privacy* (sous la dir. de GARFINKEL S. et ROSENBERG B.), Upper Saddle River, New Jersey, Addison-Wesley, 2006, pp. 211-226 ;

FOSSOUL V., « L'identification par radiofréquence (RFID) : reflet des nouvelles tendances en matières de protection des données à caractère personnel », in *Le droit des nouvelles technologies et de l'internet*, Bruxelles, Bruylant, 2012, pp. 109-136 ;

FOSSOUL V., « RFID et biométrie : état des lieux », in *Actualités du droit de la vie privée* (sous la dir. de DOCQUIR B. et PUTTEMANS A.), Bruxelles, Bruylant, 2008, pp. 139-202 ;

HENROTTE J.F. et POULLET Y., « La protection des données (à caractère personnel) à l'heure de l'Internet », in *Protection du consommateur, pratiques commerciales et TIC [technologies-information-communications]* (sous la dir. de LAFFINEUR J.), Liège, Anthémis, 2009, pp. 197-244 ;

HILDEBRANDT M., « Vision of Ambient Law », in *Regulating Technologies: legal futures, regulatory frames and technological fixes*, (sous la dir. de BROWNSWORD R. et YEUNG K.), Oxford, Hart, 2008, pp. 175-191 ;

KING N.J., « Fundamental human right principle inspires U.S. data privacy law, but protections are less than fundamental », in *Défis du droit à la protection de la vie privée* (sous la dir. de VERONICA M. et PALAZZI P.), Bruxelles, Bruylant, 2008, pp. 71-98 ;

KIRBY M., « New Frontier: Regulating Technology by Law and 'Code' », in *Regulating Technologies: legal futures, regulatory frames and technological fixes*, (sous la dir. de BROWNSWORD R. et YEUNG K.), Oxford, Hart, 2008, pp. 367-388 ;

LACOUR S., « Ubiquitous computing et Droit : l'exemple de la radio-identification », in *La sécurité de l'individu numérisé : réflexions prospectives et internationales*, Paris, L'Harmattan, 2008, pp. 29-46 ;

MURRAY A., « Conceptualising the Post-Regulatory (Cyber)state », in *Regulating Technologies: legal futures, regulatory frames and technological fixes*, (sous la dir. de BROWNSWORD R. et YEUNG K.), Oxford, Hart, 2008, pp. 287-315 ;

POULLET Y., « La protection des données, entre libertés, droits subjectifs et intérêts légitimes », in *Liber amicorum Paul Martens*, Bruxelles, Larcier, 2007, pp. 133-150 ;

POULLET Y., « Pour une troisième génération de réglementation de protection des données », in *Défis du droit à la protection de la vie privée* (sous la dir. de VERONICA M. et PALAZZI P.), Bruxelles, Bruylant, 2008, pp. 26-65 ;

PUCCINELLI O.R., « Apuntes sobre la evolución normativa y el desarrollo conceptual de los derechos de y a la protección de datos », in *Défis du droit à la protection de la vie privée* (sous la dir. de VERONICA M. et PALAZZI P.), Bruxelles, Bruylant, 2008, pp. 99-130 ;

ROSIER K., « La directive 2002/58/CE vie privée et communications électroniques et la directive 95/46/CE relative au traitement des données à caractère personnel : comment les (ré)concilier ? » in *Défis du droit à la protection de la vie privée* (sous la dir. de VERONICA M. et PALAZZI P.), Bruxelles, Bruylant, 2008, pp. 328-352 ;

SPIEKERMANN S., « The RFID PIA – developed by industry, agreed by regulators », in *Privacy Impact Assessment: Engaging Stakeholders in Protecting Privacy*, Springer, Dordrecht, 2012, disponible sur http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2050902;

VOLIO F., « Legal Personality, Privacy and the Family », in *The International Bill of Rights*, New York, Columbia University Press, 1981, pp. 185 et s.

Contributions à des périodiques

X., « RFID : instrument de sécurité ou de surveillance ? », *MISC : Multi-system & Internet security Cookbook*, n°33, septembre-octobre 2007, pp. 40-54 ;

ALLEN A., « Associational Privacy and the First Amendment: NAACP v. Alabama, Privacy and Data Protection », *Alabama Civil Rights and Civil Liberties Law Review*, Vol. 1, Issue 1 (2011), pp. 1-14 ;

BRANDEIS L.D. et WARREN S.D., « The Right to Privacy », 4 *Harvard Law Review*, 1890, disponible sur http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html ;

BRUMNIK R. et PODBREGAR I., « Biometric Technology and Human Rights », *US-China Law Review*, Vol. 7, Issue 2 (February 2010), pp. 1-11 ;

BUITELAAR J., « Privacy: Back to the Roots », *German Law Journal*, Vol. 13, Issue 3 (March 2012), pp. IV-202 ;

BURTEN C., « Unwarranted - Privacy in a Technological Age: The Fourth Amendment Difficulty in Protecting against Warrantless GPS Tracking and the Substantive Due Process and First Amendment Boost », *Southern California Interdisciplinary Law Journal*, Vol. 21, Issue 2 (Winter 2012), pp. 359-402 ;

CITRON D. et GRAY D., « Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards », *Harvard Law Review Forum*, Vol. 126, pp. 262-274 ;

CLARKE R., « An evaluation of privacy impact assessment guidance documents », *International Data Privacy Law*, 2011, Vol. 1, n°2, disponible sur <http://idpl.oxfordjournals.org/content/early/2011/02/15/idpl.ipr002.full.pdf> ;

CLARKE R., « Privacy Impact Assessment : Its Origin and Development », *Computer Law & Security Review* 25, 2, pp. 123-135, disponible sur <http://www.rogerclarke.com/DV/PIAHist-08.html> ;

COHEN J., « Examined Lives: Informational Privacy and the Subject as Object », 52 *Stanford Law Rev.*, 2000, pp. 1373 et s. ;

CONDON C., « RFID and Privacy: A Look at Where the Chips are Falling », *Appalachian Journal of Law*, Vol. 11, Issue 1 (Winter 2011), pp. 101-122 ;

COVEY R., « Pervasive Surveillance and the Future of the Fourth Amendment », *Mississippi Law Journal*, Vol. 80, Issue 4 (Summer 2011), pp. 1289-1318 ;

DARQUENNES D. et POULLET Y., « RFID : Quelques réflexions introductives à un débat de société », *R.D.T.I.*, janvier 2007, pp. 255-285 ;

DARQUENNES D., « Les cartes sans contact : d'une comparaison de trois utilisations en billettique à la recommandation européenne en matière de RFID », *R.D.T.I.*, 2009, pp. 41 et s. ;

DARQUENNES D., POULLET Y. et ROUVROY A., « Le droit à la rencontre des technologies de l'information et de la communication : le cas du RFID », *Cahiers Droit, Sciences et Technologies*, CNRS Editions, 2008, pp. 117-134 ;

DE ANDRADE N., « Electronic Identity for Europe: Moving from Problems to Solutions », *Journal of International Commercial Law and Technology*, Vol. 8, Issue 2 (2013), pp. 104-109 ;

DE SCHUTTER O., « La vie privée entre droit de la personnalité et libéralité », *Rev. Trim. D. H.*, 1999, pp. 827 et s. ;

ELTIS K., « Breaking through the Tower of Babel: A Right to be Forgotten and How Trans-Systemic Thinking Can Help Re-Conceptualize Privacy Harm in the Age of Analytics », *Fordham Intellectual Property, Media & Entertainment Law Journal*, Vol. 22, Issue 1 (Autumn 2011), pp. 69-96 ;

FIALOVA E., « Identity Management In RFID Application », *Masaryk University Journal of Law and Technology*, Vol. 6, Issue 2 (Fall 2012), pp. 223-232 ;

FIALOVA E., « RFID and Consumers' Privacy Protection », *Masaryk University Journal of Law and Technology*, Vol. 5, Issue 1 (Summer 2011), pp. 11-22 ;

FISCHER R., FRADELLA H., IRELAND C. et MORROW W., « Quantifying Katz: Empirically Measuring Reasonable Expectations of Privacy in the Fourth Amendment Context », *American Journal of Criminal Law*, Vol. 38, Issue 3 (Summer 2011), pp. 289-374 ;

GAVISON R., « Privacy and limits of Law », *89 Yale Law Journal*, 1980, pp. 433 et s. ;

GHOSHRAJ S., « Privacy Distortion Rationale for Reinterpreting the Third-Party Doctrine of the Fourth Amendment », *Florida Coastal Law Review*, Vol. 13, Issue 1 (Fall 2011), pp. 33-84 ;

HADFIELD G., « Legal Infrastructure and the New Economy », *I/S: A Journal of Law and Policy for the Information Society*, Vol. 8, Issue 1 (Summer 2012), pp. 1-60 ;

HARTZOG W. et SOLOVE D.J., « The FTC and the New Common Law of Privacy », *Columbia Law Review*, Vol. 114.583, 2013, disponible sur http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913;

HORWATH K., « Check-in on Privacy after United States v. Jones: Current Fourth Amendment Jurisprudence in the Context of Location-Based Applications and Services », *Hastings Constitutional Law Quarterly*, Vol. 40, Issue 4 (Summer 2013), pp. 925-966 ;

HU M., « Biometric ID Cybersurveillance », *Indiana Law Journal*, Vol. 88, Issue 4 (Fall 2013), pp. 1475-1558 ;

JOUNARD S.M., « Some Psychological Aspects of Privacy », *31 Law and Contemporary Problems*, 1966, disponible sur <http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3110&context=lcp> ;

KING N.J., « Direct Marketing, Mobile Phone and Consumer Privacy Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices », *Federal Communications Law Journal*, March 2008, 2, Vol. 60, pp. 229 et s. ;

KIRBY M., « History, Achievement and Future of the 1980 OECD Guidelines on Privacy », *Journal of Law, Information and Science*, Vol. 20, Issue 2 (2009/2010), pp. 1-14 ;

KONVITZ M.R., « Privacy and the Law – A Philosophical Prelude », 31 *Law and Contemporary Problems*, 1996, disponible sur <http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3108&context=lcp> ;

KOZINSKI A. et NGUYEN E., « Has Technology Killed the Fourth Amendment », *Cato Supreme Court Review*, Vol. 2011-2012, pp. 15-30 ;

LANCELOT MILTGEN C., « Vie privée et internet : influence des caractéristiques individuelles et situationnelles sur les attitudes et les comportements des internautes face à la collecte de données personnelles », *Cahier de Recherche DMSP n°317 et Actes du Congrès AFM Tunis 2003*, disponible sur <http://basepub.dauphine.fr/bitstream/handle/123456789/4259/CR317.pdf?sequence=1> ;

LEFEVER N. et POULLET Y., « Entrepôts de données et vie privée », *R.D.T.I.*, 2008, disponible sur <http://www.crid.be/pdf/public/5664.pdf> ;

MAHLER T., « Governance Models for Interoperable Electronic Identities », *Journal of International Commercial Law and Technology*, Vol. 8, Issue 2 (2013), pp. 148-159 ;

NISSEN-BAUM H., « Privacy as contextual Integrity », 79 *George Washington Law Rev.*, 2004, pp. 150 et s. ;

PAVOLOTSKY J., « Demystifying Big Data », *Business Law Today*, Vol. 2012, Issue 11 (November 2012), pp. 1-4 ;

PIERCE D., « Reasons Why We Should Amend the Constitution to Protect Privacy », *Chicago-Kent Law Review*, Vol. 84, Issue 3 (2010), pp. 851-860 ;

PRIESTER B., « Five Answers and Three Questions after United States v. Jones (2012), the Fourth Amendment GPS Case », *Oklahoma Law Review*, Vol. 65, Issue 3 (Spring 2013), pp. 491-532 ;

PROSSER W., « Privacy », 48 *California Law Review*, 1960, disponible sur http://www.californialawreview.org/assets/pdfs/misc/prosser_privacy.pdf ;

RAYMAN J., « Driving to the Panopticon : A Philosophical Exploration of the Risk to Privacy Posed by the Highway of the Futur », *11 Santa Clara Computer & Techn. Law Journal*, 1995, pp. 22 et s. ;

RICHARDS N.M., « Dangers of Surveillance », *Harvard Law Review*, Vol. 126, Issue 7 (May 2013), pp. 1934-1965 ;

RICHARDS N.M., « The Limits of Tort Privacy », *Journal of Telecommunications and High Technology Law*, Vol. 9, 2011, disponible sur http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1862264 ;

RIGAUX F., « Protection de la vie privée », *R.P.D.B.*, Complément t. IX, Bruxelles, Bruylant, 2004, n^{os} 3-17 ;

ROUVROY A., « Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence », *Studies in Ethics, Law, and Technology*, Berkley Electronic Press, 2008, disponible sur http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1013984 ;

RUBINSTEIN I., « Privacy and Regulatory Innovation: Moving beyond Voluntary Codes », *I/S: A Journal of Law and Policy for the Information Society*, Vol. 6, Issue 3 (Summer 2011), pp. 355-424 ;

SCHWARTZ P. et SOLOVE D.J., « PII Problem: Privacy and a New Concept of Personally Identifiable Information », *New York University Law Review*, Vol. 86, Issue 6 (December 2011), pp. 1814-1894 ;

SOLOVE D.J., « Data Mining and The Security- Liberty Debate », *75 University Chicago Law Review*, 2008, pp. 343 et s. ;

SPARKS K., « Medication Adherence Technology: Medicine of the Future, Emerging Privacy Concern », *Journal of Contemporary Health Law and Policy*, Vol. 28, Issue 2 (Spring 2012), pp. 324-349 ;

STEINBOCK D.-J., « Data Matching, Data Mining and Due Process », *40 GA Law Rev.*, 2005, 1, pp. 82 et s. ;

STEINBOCK D.J., « Data Matching, Data Mining et Due Process », *40 GA Law Rev*, (2005), 1, pp. 82 et s. ;

TEECE D., «Next-Generation Competition: New Concepts for Understanding How Innovation Shapes Competition and Policy in the Digital Economy », *Journal of Law, Economics & Policy*, Vol. 9, Issue 1 (Fall 2012), pp. 97-118 ;

TERRY N., « Information Technology's Failure to Disrupt Health Care », *Nevada Law Journal*, Vol. 13, Issue 3 (Spring 2013), pp. 722-758 ;

TERRY N., « Protecting Patient Privacy in the Age of Big Data », *UMKC Law Review*, Vol. 81, Issue 2 (Winter 2012), pp. 385-416 ;

THIERER A., « Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle », *Minnesota Journal of Law, Science and Technology*, Vol. 14, Issue 1 (Winter 2013), pp. 309-386 ;

WARNER R., « Undermined Norms: The Corrosive Effect of Information Processing Technology on Informational Privacy », *Saint Louis University Law Journal*, Vol. 55, Issue 3 (Spring 2011), pp. 1047-[ii] ;

WEISER M., «The computer for the 21st Century », *Scientific American*, 1991, Vol. 265, n°3, pp. 66-75.

Autres contributions scientifiques

BAKER W.B., « The changing meaning of « personal data » », disponible sur <http://www.wileyrein.com/publications.cfm?sp=articles&id=6926> ;

COSTA L., *L'identification par radiofréquence et la protection des données à caractère personnel* (multig.), mémoire de master en droit de l'internet public, Université Paris-I Panthéon Sorbonne, 2009 ;

DINANT J.-M., LAZARO C., LEFEVER N., POULLET Y. et ROUVROY A., « L'application de la Convention 108 au mécanisme de profilage – Eléments de réflexion destinés au travail du futur Comité consultatif (T-PD) », 11 janvier 2008, disponible sur http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/CRID_Profilage_2008_fr.pdf ;

ZEMOR G., *Cours de cryptographie*, éd. Cassini, Paris, 2000.

Avis, recommandations et communiqués d'organes divers

Organisation de coopération et de développement économique

OCDE, « Lignes directrices régissant la protection de la vie privée et les flux transfrontaliers de données de caractère personnel », 23 septembre 1980, disponible sur <http://www.oecd.org/fr/internet/ieconomie/lignesdirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm> ;

OCDE, « L'identification par radiofréquence (RFID) - sécurité de l'information et protection de la vie privée », 29 avril 2008, disponible sur <http://www.oecd.org/fr/sti/ieconomie/44688367.pdf>.

Union européenne

Communication de la Commission au Parlement européen, au Conseil, au Conseil économique et social européen et au Comité des régions, « L'identification par radiofréquence (RFID) en Europe : vers un cadre politique », document COM(2007)96, 15 mars 2003 ;

Recommandation (UE) n° 2009/387/CE de la Commission du 12 mai 2009 sur la mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence, *J.O.U.E.*, L 122, 16 mai 2009 ;

Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions, « Une approche globale de la protection des données à caractère personnel dans l'Union européenne », document COM(2010)609, 14 novembre 2010 ;

Recommandation CM/Rec(2010)13 du Comité des Ministres aux Etats membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, adoptée le 23 novembre 2010 ;

Résolution du Parlement, « Resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union », document 2011/2025(INI), du 6 juillet 2011.

Groupe de l'article 29

GROUPE DE L'ARTICLE 29, « Document de travail sur les questions de protection des données liées à la technologie RFID (radio-identification) », W.P. 105, 19 janvier 2005 ;

GROUPE DE L'ARTICLE 29, « Avis 4/2007 sur le concept de données à caractère personnel », W.P. 136, 20 juin 2007 ;

GROUPE DE L'ARTICLE 29, « Avis 1/2009 concernant les propositions modifiant la directive 2002/58/CE sur la protection de la vie privée dans le secteur des communications électroniques (directive 'vie privée et communications électroniques') », W.P. 159, 10 février 2009 ;

GROUPE DE L'ARTICLE 29, « L'avenir de la protection de la vie privée. Contribution conjointe de la Commission européenne sur le cadre juridique de droit fondamental à la protection des données à caractère personnel », W.P. 168, décembre 2009 ;

GROUPE DE L'ARTICLE 29, « Avis 5/2010 sur la proposition des entreprises relative au cadre d'évaluation de l'impact sur la protection des données et de la vie privée des applications reposant sur l'identification par radiofréquence (RFID) », W.P. 175, 13 juillet 2010 ;

GROUPE DE L'ARTICLE 29, « Avis 9/2011 sur la proposition révisée des entreprises relative au cadre d'évaluation de l'impact sur la protection des données et de la vie privée des applications reposant sur l'identification par radiofréquence (RFID) », W.P. 180, 11 février 2011 ;

GROUPE DE L'ARTICLE 29, « Document de travail 01/2011 concernant le cadre juridique relatif aux violations de données à caractère personnel actuellement en vigueur dans l'UE et présentant des recommandations quant aux actions à entreprendre », W.P. 184, 5 avril 2011.

United Kingdom Government

UNITED KINGDOM, *Report of the Committee on Privacy*, CMND 5012, 1972.

United States Government

NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE, « Appendix A », disponible sur <http://www.nist.gov/nstic/NSTIC-FIPPs.pdf> ;

THE WHITE HOUSE, « Consumer data privacy in a networked world : a framework for protecting privacy and promoting innovation in the digital global economy », février 2012, disponible sur <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf> ;

U.S. DEPT. OF HEALTH, EDUCATION AND WELFARE, « Record, computers and the rights of citizens », 1973, disponible sur <http://www.rand.org/content/dam/rand/pubs/papers/2008/P5077.pdf> .

Federal Trade Commission

Sony BMG Music Entm't, FTC File No. 062 3019, No. C- 4195 (F.T.C. June 28, 2007), disponible sur <http://www.ftc.gov/sites/default/files/documents/cases/2007/01/070130cmp0623019.pdf> ;

Compete, Inc., FTC File No. 102 3155, No. C-4384 (F.T.C. Feb. 20, 2013), disponible sur <http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130222competecmpt.pdf> ;

FTC v. Accusearch Inc., No. 06-CV-0105 (D. Wyo. Sept. 28, 2007), disponible sur <http://www.ftc.gov/sites/default/files/documents/cases/2006/05/060501accusearchcomplaint.pdf> ;

FEDERAL TRADE COMMISSION, « The internet of Things – Final Transcript », 19 novembre 2013, disponible sur <http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world>.

Articles et communiqués de presse

X., « National Strategy for trusted identities in cyberspace », disponible sur <http://www.nist.gov/nstic/NSTIC-FIPPs.pdf> ;

X., « RFID intégrables pour animaux », disponible sur <http://www.hidglobal.fr/products/rfid-tags/identification-technologies/rfid-integrables-pour-animaux> ;

DANIEL J., « RFID-INES : la police totale », mai 2006, p. 5, disponible sur http://infokiosques.net/article.php3?id_article=349 ;

PUEL H., « Des bracelets électroniques pour empêcher le vol des nouveaux nés », disponible sur <http://www.01net.com/editorial/345930/mise-a-jour-des-bracelets-electroniques-pour-empêcher-le-vol-de-nouveaux-nés/#forum> ;

REDON L. (sous la dir. de), *L'identification par radiofréquence*, disponible sur http://www.centrenational-rfid.com/docs/users/file/CNRFID_collusers_final_v2.pdf.

Sites internet

<http://www.ftc.gov/>

http://ec.europa.eu/justice/data-protection/article-29/index_fr.htm

<http://www.oecd.org/fr/>

Tous les sites internet ont été consultés pour la dernière fois le 30 juillet 2014.

Table des matières

Introduction	11
Titre 1 ^{er} . Qu'est-ce que l'identification par radiofréquence ?	13
Chapitre 1 ^{er} . Explication du processus d'identification par radiofréquence	13
Section 1 ^{ère} . Le mécanisme	13
Section 2. Les différentes étiquettes.....	14
§ 1 ^{er} . Selon le mode d'alimentation.....	15
§ 2. Selon le mode de communication	15
§ 3. Selon le mode de fonctionnement	15
§ 4. Selon la sécurité accordée à la divulgation du contenu de la mémoire.....	15
§ 5. Selon la fréquence de l'onde électromagnétique.....	18
Section 3. La notion d'identification.....	19
§ 1 ^{er} . L'identification.....	20
§ 2. L'authentification	20
Chapitre 2. Diverses applications de l'identification par radiofréquence	21
Section 1 ^{ère} . L'identification des objets.....	21
§ 1 ^{er} . La logistique en entreprise	21
§ 2. La lutte contre la contrefaçon.....	21
§ 3. La gestion des bibliothèques	21
§ 4. La domotique.....	21
§ 5. L'antivol.....	22
§ 6. Le contrôle d'identité	22
Section 2. L'identification des êtres vivants	22
§ 1 ^{er} . L'identification de tous les animaux domestiques ou non	22
§ 2. L'identification des êtres humains	22

Section 3. L'identification comme moyen de paiement.....	24
§ 1 ^{er} . Comme moyen de paiement traditionnel	24
§ 2. Comme moyen de paiement dans les transports	24
Chapitre 3. Tentative de définition.....	25
Titre 2. Quelle est la problématique de l'identification par radiofréquence ?.....	27
Chapitre 1 ^{er} . La collecte des données...à caractère personnel ?	28
Section 1 ^{ère} . Notion.....	28
§ 1 ^{er} . La collecte... ..	28
§ 2. ...de données... ..	28
§ 3. ...personnelles ou non ?	29
Section 2. Moyens	32
§ 1 ^{er} . De manière invisible.....	33
§ 2. De manière indéfinie	33
§ 3. De manière interopérable	33
Section 3. Risques	34
§ 1 ^{er} . La localisation des données.....	34
§ 2. Le profilage	35
§ 3. La sécurité des données.....	36
Chapitre 2. La vie privée et les données à caractère personnel	38
Section 1 ^{ère} . De la vie privée au droit à la vie privée	38
§ 1 ^{er} . De la vie privée... ..	38
§ 2. ...au droit à la vie privée	39
Section 2. Du droit à la vie privée au droit à la protection des données à caractère personnel	41
Chapitre 3. La collecte de données contraire à la vie privée et à la protection des données à caractère personnel.....	43

Titre 3. Quelles sont les solutions proposées ?.....	45
Chapitre 1 ^{er} . Les divers encadrements.....	46
Section 1 ^{ère} . L’encadrement européen.....	46
§ 1 ^{er} . Analyse préliminaire	46
§ 2. Contrer le caractère invisible.....	50
§ 3. Contrer le caractère indéfini	52
§ 4. Contrer le caractère interopérable	53
§ 5. Contrer la traçabilité.....	54
§ 6. Contrer le profilage	57
§ 7. Contrer les atteintes à la sécurité.....	58
§ 8. Conclusion.....	59
Section 2. L’encadrement américain	60
§ 1 ^{er} . Analyse préliminaire	61
§ 2. Contrer le caractère invisible.....	64
§ 3. Contrer le caractère indéfini	65
§ 4. Contrer le caractère interopérable	66
§ 5. Contrer la traçabilité.....	67
§ 6. Contrer le profilage	68
§ 7. Contrer les atteintes à la sécurité.....	69
§ 8. Conclusion.....	69
Chapitre 2. Comment expliquer ces disparités ?	71
Chapitre 3. Solution globale ?	73
Conclusion.....	75
Bibliographie	77

Place Montesquieu, 2 bte L2.07.01, 1348 Louvain-la-Neuve, Belgique www.uclouvain.be/drt

