COUNCIL OF EUROPE CONSEIL DE L'EUROPE

T-PD-BUR(2010)09

LE BUREAU DU COMITE CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISE DES DONNES A CARACTERE PERSONNEL

(T-PD-BUR)

22ème réunion
15-17 novembre 2010
Strasbourg, salle G04

Rapport sur les lacunes de la Convention n° 108 pou r la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques

(Partie I)

CENTRE DE RECHERCHES INFORMATIQUE ET DROIT

Auteur :

Jean-Marc Dinant,

Docteur en informatique

Directeur de recherche au Centre de Recherche Informatique et Droit

Expert judiciaire

Document du Secrétariat préparé par
la Direction Générale des affaires juridiques et des droits de l'Homme

TABLE DES MATIERES

1. Des nouveaux micro réseaux de télécommunication

La première décennie du 21ème siècle a vu se diffuser à une vitesse sans cesse croissante de nouveaux réseaux de télécommunication, tandis que la croissance du réseau Internet, tant en termes de rapidité que de mobilité et d'ubiquité, continuait à un rythme soutenu, du moins dans les pays développés.

Divers réseaux sans fil à courte portée (entre quelques centimètres et quelques dizaines de mètres et que nous appellerons dans ce qui suit "micro réseaux"), principalement les réseaux de type Wifi, RFID et BlueTooth, se sont récemment développés sans grande précaution par rapport à la protection des données et de la vie privée de leurs utilisateurs.
Les interfaces Wifi sont aujourd'hui généralisées dans les ordinateurs portables et équipent progressivement les téléphones mobiles. Il y a en pratique une convergence entre les « laptop » et les téléphones mobiles. Les premiers permettent de plus en plus la téléphonie grâce à des applications de VoIP comme Skype. Les seconds permettent de plus en plus à leur utilisateur, non seulement de téléphoner, mais aussi de surfer, de recevoir et d'envoyer des courriels ou même d'accéder aux réseaux sociaux via le réseau Internet. Ces réseaux représentent aujourd'hui une menace majeure et insuffisamment prise en compte par rapport à la traçabilité des utilisateurs, ou, plus largement par rapport aux êtres humains porteurs de ces terminaux connectés à ces nouveaux réseaux de télécommunication. Ces risques peuvent être synthétisés comme suit :

- Perte de contrôle : l'absence d'une connexion physique de type filaire pour ces nouveaux réseaux rend leur déconnection problématique et leur fonctionnement invisible même pour un utilisateur averti. Ce problème est particulièrement gênant pour les puces RFID qui fonctionnent sans batterie et dont la taille minuscule, de l'ordre de quelques millimètres, n'aide pas l'utilisateur à détecter leur présence. Comme ces puces sont notamment utilisées pour la lutte contre le vol dans les magasins, ces derniers n'ont évidemment pas d'intérêt à rendre ces puces visibles dans la mesure où un voleur potentiel pourrait les arracher ou les endommager.

- Absence de confidentialité : les trois réseaux précités ne sont pas chiffrés systématiquement. En particulier en ce qui concerne le réseau Wifi, il est relativement facile pour un tiers de capter et de lire le trafic entre un terminal sans fil et la borne Wifi

- Possibilité de traçabilité : Même lorsque les communications sont chiffrés, le numéro de série électronique statique qui équipe une borne Wifi, une puce RFID ou un mobile BlueTooth demeure généralement lisible en clair. Ces appareils sont de type serveur, c-à-d que, techniquement, ils répondent automatiquement à une tentative de connexion, même si elle est abusive et non suivie d'effet, en communiquant leur numéro de série électronique unique au monde (GUID = Global Unique Identifier). En général, il est donc techniquement possible de lire un numéro de série BlueTooth, l'adresse MAC d'une carte WiFi ou le numéro de série d'une puce RFID, même sans entamer une véritable communication

En conclusion, ces nouveaux réseaux largement disséminés et dont la croissance sera exponentielle durant les années à venir, permettent de manière technique et invisible le suivi individuel de chaque terminal équipé d'une interface WiFi, RFID ou BlueTooth, à l'insu de son détenteur, même lorsque l'équipement terminal n'est pas volontairement activé.

2. L'explosion de la géolocalisation

La captation d'un numéro de série d'un terminal sans fil peut s'opérer par le biais d'un ordinateur équipé de capacités de géo localisation, typiquement d'un système GPS1. Comme ces nouveaux micro réseaux sont de plus en plus reliés à des terminaux aussi sont eux-mêmes reliés au réseau Internet, l'adresse Ipv4 dynamique qui se renouvelle aléatoirement et de manière régulière ne procure plus de protection efficace contre la traçabilité des utilisateurs de réseaux de télécommunication. En effet, il est souvent possible d'identifier un numéro de série ou un tag unique propre au micro réseau utilisé. La fusion de ces micro réseaux avec le réseau global Internet conduit de manière silencieuse et inéluctable à un suivi de plus en plus systématique de la localisation des individus.

Il faut analyser les risques de cette géo localisation de manière globale. Il s'agit bien plus que de savoir où un individu se trouve à un moment donné :

- Ce système appliqué à une part importante de la population permet de savoir **avec qui** une personne déterminée se trouve et d'ainsi pouvoir dresser une cartographie des relations familiales, professionnelles ou amicales de chaque personne.

- De nombreux lieux sont empreints d'une signification particulière. La connaissance se situe bien au delà de la simple information. Le numéro 25 de la rue principale d'une grande ville n'est a priori pas très significatif, sauf si l'on sait qu'il s'agit d'une mosquée, d'un hôpital psychiatrique, d'un local syndical, d'un commissariat de police ou d'un tribunal.

- Les trajectoires d'un individu sont typiques d'un certain type de comportement. Il est ainsi possible de savoir si une personne s'arrête devant une vitrine ou si elle fait du jogging. A l'intérieur d'un grand magasin, les trajectoires des individus sont représentatives de comportement d'achat.

Cette géo localisation peut en outre se coupler avec la surveillance systématique du comportement en ligne des utilisateurs que nous avons décrite précédemment2. Le couplage des deux systèmes (profilage en ligne et géo localisation) est techniquement facilité par l'interconnexion des micros réseaux de géo localisation avec le terminal utilisé pour se connecter à Internet.

---

[1] Le système GPS est purement passif : une puce GPS capte des signaux issus de satellites géostationnaires situés à plusieurs dizaines de milliers de kilomètres et n'émet aucun signal. La puce calcule en permanence la distance qui la sépare des satellites dont elle connaît la position et calcule, par triangulation, sa position exacte (à quelques mètres près). Les problèmes de privacy ne sont pas liés au GPS lui-même mais au stockage et à la transmission des données de géo localisation par le terminal incorporant cette puce GPS.

[2] Poullet, Yves & Dinant Jean-Marc**Report on the application of data protection principles to the worldwide telecommunication networks***Information self-determination in the internet era*Rapport d'expertise à l'attention du Conseil de l'Europe, Strasbourg, 2004 http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/

3. L'invasion des cookies ou la disparition de l'intraçabilité

Les cookies ont été construits afin de permettre la traçabilité des utilisateurs du Web, nonobstant le changement d'adresse IP ou le partage d'une même adresse entre plusieurs utilisateurs3. Cette traçabilité peut être nécessaire pour les transactions électronique en ligne mais, techniquement, seuls les cookies de session directs se justifient pour cette finalité. Or, ce qui pose aujourd'hui problème, ce sont les cookies rémanents ou les cookies de tierces parties et, corollairement les cookies rémanents de tierces parties qui surveillent le trafic par transclusivité. Dans ce registre, le champion du monde en titre est indiscutablement Google qui grâce à son système Google Analytics collecte en permanence le trafic (les URL et donc le contenu) le trafic sur la majorité des sites Internet4.

Toutefois, jusqu'il y a peu, un paramétrage du navigateur permettait à l'utilisateur averti de bloquer les cookies tierces parties. Il est à souligner qu'aucun navigateur classique ne permet de bloquer la transclusivité (c-à-d l'incorporation automatique de contenus par des sites tiers inconnus de l'internaute (contactibilité) et la communication des données de trafic à ces mêmes sites tiers (observabilité)). Le blocage des cookies rémanents tierce partie agit uniquement sur la traçabilité. Deux éléments importants ont remis en cause ce contrôle marginal de la traçabilité.

La première remise en cause de cette possibilité que possède l'utilisateur averti de bloquer les cookies au niveau du protocole HTTP du WEB a été provoquée par l'apparition des cookies FLASH. Macromedia diffuse à une échelle mondiale la technologie FLASH sous forme de plug-in qui est installé sur les navigateurs les plus courants. Ce plug-in possède un fonctionnement propre et un système de gestion de données indépendant qui peut être utilisé comme un système de cookies. Dans ce cas, le blocage opéré par le navigateur se relève totalement inopérant. Il est possible pour l'utilisateur expert de trouver une parade à ce comportement étrange du plug-in qui possède donc cette capacité de lire et d'écrire des données sur la mémoire de masse du terminal. Toutefois, comme les cookies Flash sont peu connus et comme la démarche de blocage nécessite des connaissances techniques approfondies, ce type de blocage est peu utilisé.

Une deuxième phénomène remet en cause ce blocage des cookies tierces-partie par l'utilisateur averti. Pour les téléphones mobiles en général et pour l'Iphone d'Apple en particulier, il existe une tendance pour les sites web importants de développer leur propre application. Alors que leur site pourrait être utilisé via un navigateur classique de type Firefox, de nombreuses sociétés (Amazon, FaceBook, Google, certains journaux) développent et distribuent leur propre application. Cette application utilise le protocole HTTP mais l'utilisateur ne possède plus la possibilité de bloquer les cookies et encore moins la transclusivité.

Dans la même lignée, l'incorporation systématique de l'adresse MAC5 dans l'adresse IP version 6 (Ipv6) augmente(ra) de manière importante et en catimini les capacités de traçabilité des surfeurs sur les sites Web. Malgré un changement d'adresse IP et contrairement à l'actuel protocole IP version 4 (Ipv4), chaque adresse Ipv6 contiendra le numéro de série unique de la carte réseau de l'ordinateur.

---

[3] Système NAT présent sur la plupart des bornes Wifi et des routeur ADSL domestiques qui permet à plusieurs utilisateurs distincts d'utiliser simultanément une même adresse IP sur Internet

[4] Etude de Berkeley portant sur un échantillion de 400.000 sites en mai 2009 et montrant que 88% d'entre eux utililisent Google Analytics

[5] Medium Access Control. Numéro de série unique au niveau mondial de chaque périphérique Ethernet comme par exemple, les carte et les bornes Wifi, les cartes réseau. Les puces Bluetooth rproduisent souvent ne numéro de série de la carte Ethernet de l'appareil surlequel elles se trouvent.

Ce risque, bien plus grand que les cookies rémanents de tierces parties, demeure actuellement insuffisamment pris en considération par les autorités de protection des données. Un protocole IPv6 alternatif générant une adresse aléatoire existe et a été approuvé par le W3C.

De manière générale, on constate donc que les bien faibles remparts qui permettaient à l'utilisateur averti de lutter contre la traçabilité sur le réseau Internet sont en train, lentement mais sûrement, de s'éroder.

4. Les réseaux sociaux

Si à la fin du vingtième siècle, le courriel et le chat étaient les moyens de communication interpersonnelle les plus prisés sur Internet, on a vu se développer les réseaux sociaux qui sont une évolution technique naturelle des blogs d'antan. L'innovation est ici sociale : là où les blogs se concentraient sur une problématique ou un thème particulier, les réseaux sociaux se concentrent sur les individus. Rapidement, ces réseaux sociaux sont devenus une manière d'entrer en relation et de se faire connaître sur Internet. Les concepteurs de ces réseaux sociaux ont rapidement mis au point des applications spécifiques qui permettent à des tiers de parcourir ces réseaux et d'intervenir sur les profils qui y sont stockés, selon les modalités permises par les utilisateurs et par le concepteur du réseau. Ces réseaux sociaux sont généralement faussement gratuits, c-à-d que leur utilisateur rémunère le réseau social par le biais de son exposition publicitaire. Les politiques de protection de la vie privée de ces réseaux sont généralement dictées par le concepteur du site qui peut permettre aux personnes concernées de paramétrer, dans une certaine mesure qu'il détermine, la visibilité des informations stockées vis-à-vis des tiers.

Depuis toujours, les lois relatives à la protection des données à caractère personnel se sont focalisées sur le double concept de données à caractère personnel et de "maître du fichier" ou "responsable du traitement". Ces deux concepts semblent devenus aujourd'hui à la fois trop flous et trop étroits pour conduire à une réglementation efficace du droit au respect de la vie privée au sein des technologies et usages sans cesse changeants de la société de l'information et de la communication.

5. Une approche fonctionnelle du concept de donnée à caractère personnel

Toute donnée liée à un individu identifie généralement une caractéristique de ce dernier. Cette donnée peut être biographique et/ou traçante.

Dans le premier cas, la donnée qui se rapporte à un individu raconte quelque chose par rapport à cette personne : par exemple un fait, un geste, un parcours ou un achat ; il s'agit d'une propriété de la personne qui peut être partagée entre plusieurs individus. Par exemple, le fait d'être corse ou catalan est une donnée personnelle de chaque corse ou chaque catalan. Il s'agit d'une donnée « biographique » au sens étymologique, c-a-d une information qui (d)écrit la vie ou plus exactement une tranche de vie, une caractéristique d'un individu. L'enjeu est donc ici la **connaissance** d'une ou plusieurs caractéristiques d'un individu **dans un contexte particulier**.

Dans le deuxième cas, la donnée se rapporte à un individu et constitue une caractéristique unique ou une valeur unique de certaines variables qui le distingue de manière certaine des autres individus au sein d'une population donnée. Ainsi une adresse IP identifie une personne de manière unique à un

moment donné6. Il s'agit d'un identifiant unique (Unique Identifier). Cet identifiant n'est guère problématique lorsqu'il s'agit d'identifier un individu dans un contexte particulier (numéro de compte dans une banque, numéro de patient dans un hôpital, numéro d'étudiant dans une université, numéro de citoyen dans une administration, numéro d'affilié dans un syndicat, etc). Toutefois, en pratique, ces identifiants sont rarement locaux mais deviennent rapidement globaux, c-à-d multicontextuels. On parle alors d'Identifiant Global Unique (Global Unique Identifier). Ce type d'identifiant permet la traçabilité d'une même personne au sein de plusieurs contexte différents. L'enjeu est donc ici une **connaissance multicontextuelle** d'un même individu.

Les données contactuelles constituent un troisième type de donnée. Une adresse email, une adresse postale, l'URL d'un « mur » sur un site social permettent à un tiers de communiquer un contenu à un individu identifié par une donnée de contact. Ainsi, par exemple, la connaissance d'une adresse email pourrait permettre d'identifier plusieurs pages WEB relatives au même individu. L'enjeu de ce dernier type de donnée est la **contactabilité**, ou la possibilité techniquement offerte à un tiers d'injecter un contenu informationnel (et notamment de la publicité) dans une boîte aux lettres ou sur un écran. Dans ce contexte, c'est naturellement de marketing dont il s'agit et, plus précisément du contrôle de l'individu par rapport à son **exposition publicitaire**.

Cette division fonctionnelle des données distingue en fait trois types de données à caractère personnel qui sont substantiellement différentes. Il s'agit, plus précisément, de propriétés des données à caractère personnel. Ainsi, une adresse email de type « john.smith@coe.int » cumule les trois propriétés décrites ci-dessus. On peut savoir que John Smith travaille au Conseil de l'Europe. En tapant son adresse mail sur un moteur de recherche, on pourra trouver des informations qui y sont associées et enfin, l'adresse mail va permettre de contacter John Smith, éventuellement à des fins publicitaires

De très (trop ?) longs débats ont eu lieu depuis longtemps sur le caractère de données à caractère personnel de l'adresse IP ou des cookies. Il est à souligner que l'importance apparente de ce débat est liée à une confusion présente au sein des les entreprises, notamment multinationales. L'article 8 de la CEDH ne protège pas la vie privée de l'homme identifié ou identifiable. Toute personne même non identifiée ou identifiable a droit à cette protection. Le droit à la protection des données à caractère personnel n'épuise pas le droit à la protection de la vie privée. Ainsi, par exemple, la surveillance omniprésente des personnes dans les lieux publics ou privés par des moyens de vidéo surveillance constitue bel et bien une intrusion dans la vie des personnes filmées, quand bien même elles demeureraient non identifiables grâce à un savant floutage de leur visage.

En d'autres termes, à notre sens, il n'existe pas de donnée concernant un individu qui ne l'identifie, soit de manière traçante, soit de manière biographique ou qui ne permette de le contacter.

Il est à noter que certains de ces problèmes sont déjà pris en considération par certaines directives européennes qui ne nous semblent pas avoir d'équivalent au sein du Conseil de l'Europe. Ainsi, par exemple, la directive CE 95/46 prévoit le droit de s'opposer au marketing direct sans aucune justification. La directive CE 2002/58 réglemente l'usage qui peut être fait du courrier électronique et soumet l'utilisation de celui-ci à des fins commerciales au consentement ou à la possibilité d'exercer un droit d'opposition dans le chef de la personne concernée. La directive CE 2006/24 détermine de manière exhaustive les données de trafic qui doivent être conservées par les opérateurs de télécommunication, par dérogation à la Directive 2002/58. Etc.

---

[6] Ceci est vrai en règle générale si l'utilisateur n'utilise pas de système NAT. Dans le cas d'un système NAT permettant le partage simultané d'une même adresse IP entre plusieurs personnes (élèves d'une école, membre d'une famille, hôtes d'un hotel, etc), l'adresse IP identifiie un groupe de personnes.

Il est à relever que ces dispositions du droit communautaire européen font preuve d'un plus grand pragmatisme et prétendent protéger la vie privée et les données à caractère personnel. On peut d'ailleurs noter que la protection du courrier électronique profitera tout autant aux personnes morales qu'aux personnes physiques.

En conclusion, il est devenu de moins en moins pertinent de se poser la question de savoir si telle ou telle donnée est une donnée à caractère personnel mais plutôt d'identifier les risques que fait courir l'utilisation des données issues des technologies de l'information et la communication dans un contexte particulier par un utilisateur donné et d'y apporter une réponse de principe.

A notre sens, les données les plus sensibles sont aujourd'hui les Identifiants Globaux Uniques hardware (numéro de série électronique) ou software (cookie) dans la mesure où, étant fermement attachés à un terminal de télécommunication, ils permettent la traçabilité d'un même utilisateur dans plusieurs contextes différents. L'utilisation des ces numéros uniques devrait être restreinte au terminal. Ils ne devraient pas devoir transiter jusque dans les réseaux de télécommunication, en l'absence de garanties appropriées.

Les données de trafic devraient elles aussi jouir d'un statut particulier. En droit européen, le principe d'anonymisation ou de destruction immédiate des données de trafic est inscrit à l'article 6 de la Directive 2002/54. Par dérogation à ce principe général, les opérateurs, sur base de la directive 2006/24 sont contraints de conserver un nombre limité de données pour une période limitée et aux seules fins de la poursuite et de la recherche des infractions pénales. Il est piquant de constater que Google collecte aujourd'hui en temps réel l'ensemble des données de trafic du Web sur une base individuelle et à des fins commerciales (le marketing direct a rapporté à Google plus de six milliards de US $ en 20097) alors que semblable collecte est expressément interdite aux opérateurs de télécommunication à des fins de détection et de poursuite par les forces de police des délits criminels. Qu'en d'autres termes, un acteur puissant d'Internet collecte quotidiennement et de facto bien plus de données personnelles à des fins commerciales que ne le peuvent et ne le font les services de polices, par le biais des opérateurs, à des fins de lutte contre les atteintes à la sécurité publique.

6. Le maître du fichier

Tant la Directive 95/46 que la Convention 108 distinguent deux personnes responsables du traitement des données : le responsable du traitement (maître du fichier) et le sous-traitant.

Cette catégorisation ne nous semble plus adéquate. Le monde des TIC s'est spécialisé et de nouveaux métiers se sont créés. D'autres métiers émergeront demain.

Pour parvenir à mener à bien cette régulation, il convient d'adapter le régime légal en fonction du métier de la société qui collecte, stocke ou transmet des données relatives aux individus.
Nous avons par ailleurs bien conscience que cette régulation se heurte actuellement à un problème de Droit International Privé. A l'instar du droit de la consommation, la protection des données (qui devient un aspect de plus en plus important de ce droit de la consommation) ne devrait il pas être

[7] Voir à ce sujet « *Bénéfices en forte hausse pour Google* » *in* « *Le Monde*, *16 octobre 2009*, *http://www.lemonde.fr/technologies/article/2009/10/16/benefices-en-forte-hausse-pour-google_1254699_651865.html*

celui de la personne concernée et non celui de l'établissement de la société qui collecte, stocke ou transmet ces données ? Ce point sera abordé en détail dans notre deuxième partie.

Sous la pression populaire, certains grands acteurs (FaceBook, Google) ont parfois modifié leurs politiques en matière de vie privée mais un tel mode de régulation par essai et erreur n'apparait pas satisfaisant. Les attaques de plus en plus subtiles contre la protection des données à caractère personnel et contre la vie privé des internautes sont motivées par des considérations économiques de grands acteurs de l'Internet et génèrent, par effet de bord, des problèmes dont le coût social est porté par la société dans son ensemble.

Sur ce point précis, nous constatons que le financement de nombreux outils de la société de l'information et de la communication (moteur de recherche, réseaux sociaux, courrier électronique,…) est basé sur la publicité. L'argument clé des publicitaires, à savoir la gratuité de l'Internet, se révèle, à l'analyse, bancal. Si c'est la publicité qui finance l'internet, il faut évidemment se demander qui finance la publicité. Bien loin de recevoir un Internet gratuit, le consommateur paie en fait deux fois. Il paie tout d'abord en nature en se faisant profiler, analyser et manipuler tant dans son conscient que dans son inconscient. Le consommateur paie une deuxième fois en achetant le produit ou le service ainsi promu et dont le coût se trouve inéluctablement inclus dans le prix final.

De nombreux auteurs ont mené une réflexion sur la marchandisation de la vie privée et des données à caractère personnel. Il semble aujourd'hui acquis, que la protection de la vie privée est une liberté fondamentale. Et c'est bien parce qu'il s'agit d'une liberté fondamentale que cette vie privée peut, dans une certaine mesure et sous certaine conditions se monnayer. A l'instar du droit à l'image monnayé par les vedettes du show biz, chaque individu devrait pouvoir non seulement refuser ou accepter l'exposition publicitaire mais aussi la monnayer contre des espèces sonnantes et trébuchantes. Il serait donc souhaitable que l'accès aux services de la société de l'information et de la communication ne soit plus conditionné par une obligation de fait de se soumettre à l'analyse comportementale et à l'injection de contenus publicitaires mais puisse être payée par le consommateur via une contribution financière Ces services sans publicités pourraient être rendus accessibles aux citoyens par les fournisseurs d'accès à Internet, moyennant une modeste contribution financière et forfaitaire incluse dans le coût de l'abonnement Internet. En effet, si l'on ramène grossièrement le bénéfice de Google au nombre d'internaute concernés, on se rend compte que l'accès aux services de Google pourrait s'effectuer pour un prix d'environ un euro par internaute et par mois, sans que le bénéfice de Google en soit affecté de manière significative.

7. Une "success story" ?

A notre sens, le réseau téléphonique mobile moderne demeure un exemple à suivre en matière de protection de la vie privée intégré au cœur de la technologie. D'une part, les terminaux de téléphonie mobile doivent (sous peine de ne pas être agrées et donc impossibles à vendre) inclure le Calling Line Identification Restriction. Cette fonctionnalité permet à tout utilisateur, même néophyte, de masquer son numéro d'appel à la personne à qui elle téléphone. Techniquement, il faut savoir que ce numéro est toujours techniquement transmis, ce qui permet, par exemple aux services d'urgence, dans les conditions prévues par ou en vertu de la loi, de procéder à l'identification du numéro appelant ces services.

Les appareils téléphonique mobiles possèdent eux aussi un numéro de série électronique appelé IMEI (*International Mobile Equipment Identity)*. Ce numéro de série est transmis à l'opérateur du réseau téléphonique et à lui seul. L'opérateur du réseau ne transmet pas techniquement ce numéro de série sur l'appareil mobile du destinataire de la télécommunication. Toutefois, en vertu de la

Directive 2006/24, les opérateurs doivent conserver cette donnée d'identification. Ces éléments techniques permettent à l'utilisateur un réel contrôle sur la téléphonie mobile. Il peut masquer son numéro d'appel et gère ainsi sa traçabilité et sa contactabilité. Sa communication est chiffrée et n'est pas facilement observable par un tiers.

On peut constater un certain consensus au sujet des principes de protection de la vie privée et des données à caractère personnelles (ontologie de la privacy : contrôle sur l'observabilité, la traçabilité et la contactibilité ; respect du principe de finalité (contextualisation des données)), de nombreuses recherches relatives au « privacy by design » sont en cours.

Nous pensons que face aux défis présents et à venir la loi doit s'adresser de manière différente à tous les acteurs de la société de l'information et de la communication, selon le rôle qu'ils jouent et le type de données qu'ils sont appelés à traiter. Sur les autoroutes de l'information, le code de la route ne suffit plus ; il faut produire des véhicules, de la technologie qui mette en œuvre ces principes de protection du conducteur. « If the technology is the problem, the technology may be the answer… »

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

T-PD-BUR(2010)09

LE BUREAU DU COMITE CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISE DES DONNES A CARACTERE PERSONNEL

(T-PD-BUR)

22ème réunion
15-17 novembre 2010
Strasbourg, salle G04

Rapport sur les lacunes de la Convention n° 108 pou r la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques

(Partie II)

CENTRE DE RECHERCHES INFORMATIQUE ET DROIT

Auteurs :

Cécile de Terwangne, Professeur à la Faculté de Droit de l'Université de Namur, Directrice de recherche au CRID

Jean-Philippe Moiny, aspirant du F.R.S.-FNRS
Chercheur au CRID

Avec la collaboration de :

Yves Poullet, Recteur de l'Université de Namur (FUNDP), Professeur à la Faculté de droit, Directeur de recherche au CRID

Jean-Marc Van Gyzeghem, Senior Researcher au CRID

Document du Secrétariat préparé par
la Direction Générale des affaires juridiques et des droits de l'Homme

TABLE DES MATIERES

INTRODUCTION

Le présent rapport vise à identifier les domaines dans lesquels des problèmes spécifiques se sont fait jour à l'occasion de l'application des principes de protection des données à caractère personnel lorsqu'il est fait usage des nouveaux développements technologiques.

La réflexion porte en somme sur la mesure dans laquelle les dispositions de la Convention n°108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ainsi que de son protocole additionnel du 8 novembre 2001 concernant les autorités de contrôle et les flux transfrontières de données répondent toujours de façon adéquate aux attentes et aux préoccupations actuelles liées aux développements technologiques récents. Ces dispositions garantissent-elles encore de manière satisfaisante la protection des données dès lors qu'il est fait recours au réseau Internet, aux multiples applications ayant vu le jour sur le Web 2.0, aux technologies de géolocalisation, à celles d'échange des données, aux puces RFID, aux identifiants biométriques, aux techniques de surveillance, etc. ?

A cette fin, le rapport se présente en deux parties distinctes. Une première partie, contenue dans un document joint, contient une description des modifications du « paysage technologique » depuis la date d'approbation de la Convention n° 108 tout en relevant les enjeux importants liés à ces modifications. Elle porte sur la « nouvelle vulnérabilité de l'individu face à l'évolution technologique ». La deuxième partie du rapport fait l'objet des présentes pages. Elle est consacrée à une analyse des dispositions de la Convention n° 108 au regard des enjeux de ces réalités nouvelles afin d'identifier les lacunes éventuelles du texte actuel face aux nouveaux dangers et aux nouvelles attentes en termes de protection des données.

Le présent rapport peut, d'une certaine manière, être considéré comme une mise à jour du rapport intitulé « L'autodétermination informationnelle à l'ère d'Internet », rapport sur l'application des principes de protection des données de la Convention n° 108 aux réseaux mondiaux de télécommunications, rédigé en 2004 par le Centre de Recherches Informatique et Droit (CRID) de l'Université de Namur (Belgique) à la demande du Conseil de l'Europe[8]. Dans cette mesure, certains passages ayant gardé toute leur pertinence sont repris du texte initial avec les nécessaires ajustements de forme. Ces passages sont indiqués en surligné jaune.

[8] Y. POULLET, J.-M. DINANT, avec la collab. de C. de TERWANGNE ET M.-V. PEREZ-ASINARI, « L'autodétermination informationnelle à l'ère de l'Internet », Rapport pour le Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD), Conseil de l'Europe, Strasbourg, 18 novembre 2004.

CONFRONTATION DES DISPOSITIONS DE LA CONVENTION N° 108 A L'ENVIRONNEMENT TECHNOLOGIQUE NOUVEAU

L'analyse porte à ce stade sur la confrontation des dispositions de la Convention n° 108 ainsi que de son protocole additionnel du 8 novembre 2001 concernant les autorités de contrôle et les flux transfrontières de données au nouvel environnement technologique tel que décrit dans la première partie de ce rapport. Cette confrontation permet de vérifier si ces textes répondent toujours adéquatement aux nouveaux défis et garantissent encore une protection adéquate aux individus à l'égard du traitement des données à caractère personnel. L'objectif de cette deuxième partie de l'analyse consiste donc à mettre au jour les éventuelles lacunes apparues dans la protection.

L'analyse, se centrant sur le texte même de la Convention, en suit logiquement la structure.

Il est clair qu'un ensemble de documents ayant fait l'objet de discussion ou adoptés dans diverses enceintes internationales sur le sujet ont nourri le propos des pages qui suivent. En particulier, ont été pris en compte des documents issus des organes du Conseil de l'Europe lui-même, de l'Union européenne (directives, avis du Contrôleur européen à la protection des données, documents du Groupe des autorités européennes de protection des données (Groupe dit de l'article 29)), de l'OCDE et de l'APEC qui a adopté le texte régional le plus récent en la matière. La Résolution de Madrid[9] a aussi alimenté opportunément la présente réflexion. Ce texte, issu d'un travail conjoint des autorités de protection des données de cinquante pays sous la houlette de l'Agence espagnole de la protection des données, réalise l'intégration des valeurs et principes de protection des données garantis sur les cinq continents. Il vise donc à offrir un modèle reprenant les standards universels de la protection des données. Enfin, la jurisprudence de la Cour européenne des droits de l'homme ainsi que de la Cour de Justice de l'Union européenne a également été prise en considération lorsqu'elle pouvait éclairer l'analyse.

1. Objet et but de la Convention

1.1. LE BUT DE LA CONVENTION : LA PROTECTION DES DONNEES

1.1.1. Protection des données et protection de la vie privée

Il est intéressant que la Convention n°108 ait, dès l'origine, assimilé la protection des données au respect pour toute personne physique « *de ses droits et libertés fondamentales*, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant »[10].

La Convention indique de la sorte expressément dans son article 1er que la protection des données ne se résume pas à la seule protection de la vie privée. D'autres droits et libertés entrent en ligne de compte, telle la liberté de se déplacer, celle de s'assurer, celle de se loger, celle de trouver un emploi,

9 Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data, disponible à l'adresse http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf.

10 Article 1er de la Convention n° 108 (c'est nous qui soulignons). Rapport explicatif concernant la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

celle de s'informer et de s'exprimer en toute transparence, etc. Ainsi, la création, au sein de réseaux inter-entreprises ou inter-administrations, de bases de données permettant un profilage *a priori* des utilisateurs de services peut amener à discriminer ceux-ci lors de la recherche d'un logement, de la recherche d'information, de la demande d'une couverture d'assurance ou de l'acquisition d'un ouvrage[11]. Autre exemple, le remplacement progressif des modes de paiement traditionnels par des paiements via des cartes de crédit dont les émetteurs sont en situation oligopolistique exigerait une réflexion sur l'impact que peuvent avoir sur les citoyens tantôt le retrait ou le blocage d'une carte de crédit en termes de liberté de mouvement, tantôt l'analyse des utilisations de la carte en termes de surveillance globale des activités de l'individu.

Si l'enjeu de la protection des données ne se réduit pas à la seule protection de la vie privée, le lien avec cette dernière est cependant étroit. La protection des données est une émanation du droit au respect de la vie privée pris dans la dimension d'autonomie personnelle[12] ou même de droit à l'autodétermination[13] qui y est liée, davantage que dans le sens d'exigence de confidentialité attaché traditionnellement à la notion de vie privée. La protection des données c'est le droit à l' « autodétermination informationnelle ». La Convention n°108 traduit incontestablement cette approche en renforçant les moyens de contrôle par les citoyens des traitements opérés sur leurs données par l'octroi d'un droit à l'information et d'un droit d'accès aux données détenues par autrui et en définissant des limites au droit de traiter des données dans le chef des acteurs tant publics que privés (finalité légitime, proportionnalité, sécurité,…). Des éléments d'une approche plus négative et restrictive, où la vie privée est considérée comme un concept défensif, se retrouvent toutefois dans le régime des données sensibles (article 6 de la Convention), régime d'interdiction de principe garantissant la protection des citoyens contre les atteintes à la confidentialité de telles données.

C'est en ce sens que l'Assemblée parlementaire du Conseil de l'Europe a veillé à compléter sa Résolution 428 (1970). En effet, le droit au respect de la vie privée garanti par l'article 8 de la Convention européenne des Droits de l'Homme avait été défini par l'Assemblée en janvier 1970 dans la déclaration sur les moyens de communication de masse et les droits de l'homme contenue dans cette Résolution comme « le droit de mener sa vie comme on l'entend avec un minimum d'ingérence ». Près de trente ans après l'adoption initiale de ce texte, l'Assemblée a précisé que « Pour tenir compte de l'apparition des nouvelles technologies de la communication permettant de stocker et d'utiliser des données personnelles, il convient d'ajouter à cette définition *le droit de contrôler ses propres données* »[14].

La Charte des droits fondamentaux de l'Union européenne, devenue juridiquement contraignante depuis l'entrée en vigueur du Traité de Lisbonne, a pris l'option – à tout le moins pédagogique – de distinguer les concepts de vie privée (article 7) et de protection des données (article 8)[15].

---

11 V. sur ce dernier point les pratiques de « *discriminative pricing* » d'Amazon, dénoncées par les associations de consommateurs américaines et abandonnées par la suite.

12 Pour la mise au jour de la dimension d'autonomie personnelle attachée au droit au respect de vie privée consacré à l'article 8 de la Convention européenne des droits de l'homme, voy. Cour eur. D.H., *Pretty c. Royaume-Uni*, arrêt du 29 avril 2002, req. n° 2346/02 ; *Van Kück c. Allemagne*, arrêt du 12 juin 2003, req. n° 35968/97 ; *K.A. et A.D. c. Belgique*, arrêt du 17 février 2005, req. n° 42758/98 et 45558/99.

13 Pour la reconnaissance explicite d'un droit à l'autodétermination ou l'autonomie personnelle contenu dans le droit au respect de la vie privée de l'article 8 CEDH, voy. Cour eur. D.H., *Evans c. Royaume-Uni*, arrêt du 7 mars 2006, req. n° 6339/05 (confirmé par la Grande Chambre dans son arrêt du 10 avril 2007) ; *Tysiac c. Pologne*, arrêt du 20 mars 2007, req. n° 5410/03 ; *Daroczy c. Hongrie*, arrêt du 1er juillet 2008, req. n° 44378/05.

14 Rés. 1165(1998) de l'Assemblée parlementaire du Conseil de l'Europe sur le droit au respect de la vie privée, adoptée le 26.06.1998 (c'est nous qui soulignons).

15 Article 7 : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications »

S'autonomisant du droit au respect de la vie privée, le droit à la protection des données suppose la prise en compte, d'une part, des déséquilibres de pouvoirs entre la personne concernée et celui qui traite les données, déséquilibres engendrés par les capacités de traitement des données à disposition de ce dernier et dramatiquement exacerbés aujourd'hui du fait des développements techniques et, d'autre part, de l'impact que les traitements de données peuvent avoir sur les divers droits et libertés mentionnés plus haut. Les technologies, plus par un choix de configuration que par nécessité, génèrent et conservent les « traces » de l'utilisation des services et autorisent, par des capacités de traitement sans commune mesure avec celles existant il y a dix ans (que dire d'il y a vingt-neuf ans…), une connaissance de l'individu et de ses comportements, individuels ou collectifs, personnels ou anonymes. En d'autres termes, leur utilisation accroit le déséquilibre existant dans la relation entre ceux qui disposent de l'information et les individus, personnes concernées ou non. Sur la base des renseignements collectés, des décisions collectives (par exemple, la fixation du taux de remboursement des coûts de traitement d'une maladie) ou individualisées (par exemple, le refus de l'octroi d'un crédit ou d'un service bancaire) seront prises.

En résumé, la Convention n° 108 n'est pas tombée dans l'écueil d'une réduction de la protection des données au champ de la protection de la vie privée, écueil particulièrement dommageable si ce champ n'est envisagé, comme parfois encore hélas, dans la ligne classique du « right to be left alone », que comme une exigence de confidentialité. Cela étant, **ne s'indiquerait-il pas de mieux mettre en évidence l'étendue des préoccupations exprimées par le concept de droit à la protection des données ? Doit-on relever comme une lacune le fait que la Convention ne mentionne pas explicitement dans la définition de la protection des données contenue à l'article 1er l'aspect de contrôle par l'individu des données à caractère personnel qui le concernent ?**

La mention explicite de cet aspect pourrait avoir des vertus pédagogiques particulièrement indiquées dans le cas où la Convention n° 108 est appelée à servir de balise pour des pays tiers au Conseil de l'Europe, pays qui n'auraient pas connaissance de l'évolution que la notion de « vie privée » a connue dans la jurisprudence de la Cour européenne des droits de l'homme, tout comme parmi les institutions du Conseil de l'Europe et au sein de l'Union européenne. C'est d'autant plus important que dans le Préambule de la Convention il est spécifié que les Etats signataires de la Convention reconnaissent « la nécessité de concilier les valeurs fondamentales du respect de la vie privée et de la libre circulation de l'information […] ». La vie privée est donc là la seule valeur avancée pour justifier le régime de protection imaginé. Il est en conséquence crucial que cette notion soit perçue dans sa signification « moderne » et spécifique à la matière.

L'évocation de ce contrôle ou de cette maîtrise informationnelle au nom de l'autodétermination permettrait de démontrer clairement que la Convention n'est pas qu'un instrument défensif, visant à garantir la confidentialité des données ou à interdire le traitement de certaines données sensibles, mais qu'elle traduit une approche plus positive en ce qu'elle est la manifestation du droit à l'autodétermination informationnelle.

Article 8 : « 1. Toute personne a droit à la protection des données à caractère personnel la concernant ; »

« 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. »

« 3. Le respect de ces règles est soumis au contrôle d'une autorité de protection des données. »

1.1.2. Protection des données et dignité humaine

Il n'est pas fait mention dans la Convention de la protection de la dignité humaine. **L'invocation de la dignité humaine entend rappeler que l'Homme est un sujet[16] et ne peut être ramené à un simple objet de la surveillance et du contrôle d'autrui**.

La Cour européenne des droits de l'homme n'a pas hésité à appuyer explicitement son raisonnement en matière de respect de la vie privée sur la dignité de l'homme. Elle a en effet énoncé que « la dignité et la liberté de l'homme sont l'essence même de la Convention. Sur le terrain de l'article 8 de la Convention en particulier […] »[17] La Cour de Justice des Communautés européennes (aujourd'hui Cour de Justice de l'Union européenne) a elle aussi mis en exergue la valeur de dignité attachée intrinsèquement aux individus, qu'il s'agit de protéger juridiquement. Dans une affaire mettant en cause un transsexuel, elle a proclamé : « Tolérer une telle discrimination reviendrait à méconnaître, à l'égard d'une telle personne, le respect de la dignité et de la liberté auquel elle a droit et que la Cour doit protéger. »[18]

La loi française relative à la protection des données proclame dès l'entame que « L'informatique doit être au service de chaque citoyen. […] Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits fondamentaux, ni à la vie privée, ni aux libertés individuelles ou publiques. »[19] On peut voir exprimé dans cette formule un souci fort proche du respect de la dignité humaine, l'idée que l'homme ne peut être soumis à la machine mais que celle-ci, au contraire, doit être à son service et qu'elle ne peut porter atteinte aux valeurs essentielles des individus.

La directive 95/46 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[20] garantit, elle, le droit de ne pas être soumis à une décision prise par une machine. Ce droit reconnu à toute personne de ne pas être soumise à une décision individuelle entièrement automatisée[21] l'est au nom de la dignité humaine.

Il sera proposé dans le chapitre consacré aux garanties complémentaires pour les personnes concernées de faire figurer cette manifestation de la prééminence à accorder à la dignité humaine. Cela étant, il pourrait être également envisagé de faire figurer cette dernière dans les valeurs sous-tendant les règles de protection des données énoncées dans la Convention.

Ce rappel de la dignité comme valeur fondatrice de la protection des données voire de la vie privée[22] est sans doute nécessaire au vu de certaines utilisations de la technologie. Les systèmes d'information réalisent de manière croissante une surveillance globale des populations et des

---

16 Cf. la célèbre phrase de Kant, parlant de la dignité humaine: " Il (l'homme) ne peut être regardé comme un moyen pour les fins d'autrui, ou même pour ses propres fins mais comme une fin en soi, c'est à dire qu'il possède une dignité par laquelle il force au respect de sa personne, et qui lui permet de se mesurer avec chacune d'elles et de s'estimer sur pied d'égalité. » (*Doctrine de la vertu*, p. 96-97) citée par J. FIERENS, « La dignité humaine comme concept juridique », *Journal des tribunaux*, 2002, p. 78.

17 Cour eur. DH, *Christine Goodwin c. RU*, arrêt du 11 juillet 2003, req. n° 28957/95, par. 90.

18 C.J.C.E., 30 avril 1996, (P. v. S. and Cornwall County Council*)*, par. 21-22.

19 Loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978, modifiée en 2004, article 1er.

20 Directive 95/46/CE du Parlement et du Conseil 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.*, n° L 281 du 23 novembre 1995, pp. 31 et s

21 Article 15 de la directive 95/46, voy. *infra*.

22 Sur cette relation, lire J.H. REIMAN, "The Right to Privacy ", in *Philosophical Dimensions of Privacy* 272, F.D. Schoeman ed., New York, 1984, 300 et ss.

individus, créant un système de transparence des comportements des personnes qui peut s'avérer contraire à la dignité humaine[23]. De même, le phénomène du profilage qui conduit à déduire des informations à l'insu des personnes concernées pour leur appliquer des décisions en tout genre peut porter sérieusement atteinte à la dignité des individus profilés.

L'atteinte à la dignité est d'ailleurs clairement et à plusieurs reprises invoquée dans la recommandation en projet concernant la protection des données dans le contexte du profilage[24]. Deux considérants sont très explicites : « 14. Considering that the use of profiles, even legitimately, without precautions and specific safeguards could severely damage human dignity, as well as other fundamental rights and freedoms, including economic and social rights; 20. Considering that the protection of human dignity and other fundamental rights and freedoms in the context of profiling can be effective if, and only if, all the stakeholders contribute together to a fair and lawful profiling of individuals; ».

1.1.3. Protection des données, support ou mise en cause d'autres libertés

Que la vie privée ou de manière plus large la protection des données soit une garantie de nos libertés, cela va de soi. Ainsi, pour parler de la liberté d'expression et d'association, comment imaginer que celles-ci puissent survivre si la personne se sait surveillée dans ses communications et ne peut à certains moments s'exprimer anonymement si la technologie garde systématiquement trace de ses messages ? La liberté de s'informer suppose que l'information ne soit pas filtrée, que l'on ne soit pas conduit, profilage aidant, à son insu ou malgré soi, vers l'information qu'autrui souhaite nous voir consommer. Pire, la même technique de profilage peut amener l'auteur du profilage à priver de certains services ou informations un consommateur pour lequel il estime qu'il est peu rentable de l'autoriser à y avoir accès. Ces exemples pourraient être multipliés vis-à-vis des différentes libertés consacrées par la Convention européenne des droits de l'homme. La protection des données est indiscutablement le support de nombre d'autres libertés et les garantit**.**

Il arrive cependant que le souci de protection des données heurte le développement d'autres libertés**.** En particulier, **la protection des données doit être mise en balance avec les impératifs de protection de la liberté d'expression et d'opinion.**

Le préambule de la Convention le rappelle implicitement : « *Réaffirmant en même temps leur engagement en faveur de la liberté d'information sans considération de frontières ; Reconnaissant la nécessité de concilier les valeurs fondamentales du respect de la vie privée et de la libre circulation de l'information entre les peuples* », sans qu'aucune disposition de la Convention n°108 ne consacre cependant explicitement la nécessité de cette mise en balance. La Convention se veut il est vrai l'expression de cette mise en balance. L'article 9 autorisant les exceptions et restrictions au régime de protection (sauf aux obligations liées à la sécurité des données) prévoit qu'une dérogation est admise si, prévue par la loi, elle est nécessaire dans une société démocratique à la protection des droits et libertés d'autrui. Au rang de ces droits et libertés figure assurément la liberté d'expression. Le régime des flux transfrontières (article 12 et Protocole additionnel) ne bénéficie pas de cette possibilité d'exception. Il est néanmoins permis à chaque Etat d'autoriser un transfert de données normalement interdit, lorsque des intérêts légitimes prévalent. A nouveau on imagine sans peine que la liberté d'expression figure parmi les intérêts légitimes évoqués. Si les régimes d'exception

[23] Cf. le cas du Londonien filmé 300 fois par jour par des caméras de vidéosurveillance ou le cas de l'employé portant un badge permettant de le localiser à tout moment pendant les heures de travail et d'ainsi déduire ses relations de travail ou autres avec d'autres employés eux aussi porteurs de badge.

[24] Draft Recommendation on the protection of individuals with regard to automatic processing of personal data in the context of profiling, adopted by the T-PD at the 26th Plenary meeting, Strasbourg, 4 June 2010, disponible à l'adresse http://www.coe.int/t/dghl/standardsetting/DataProtection/TPD%20documents/T-PD-BUR_2009_02rev6_en_Fin%20_2.pdf

permettent sans doute de résoudre les frictions existant entre la liberté d'expression et la protection des données, il ne serait toutefois peut-être pas superflu d'inviter expressément les Etats à veiller à concilier les deux intérêts contradictoires. La directive européenne 95/46, bien qu'offrant un régime dérogatoire dans la même ligne que la Convention n° 108, invite expressément les Etats à adopter des exemptions et dérogations pour les traitements « effectués aux seules fins de journalisme ou d'expression littéraire et artistique » pour « concilier le droit à la vie privée avec les règles régissant la liberté d'expression »[25].

Ce souci de ne pas attenter, par le biais de la protection des données, à la liberté d'expression et d'opinion a jusqu'à présent été rencontré par certaines dispositions protectrices des conditions de travail des journalistes notamment dans l'univers en ligne. Cependant, il apparaît de plus en plus qu'il est indispensable d'aménager un équilibre entre la protection des données et la liberté d'expression en général. Cette réflexion est particulièrement pertinente depuis l'avènement d'Internet, de ses forums de discussion, de ses blogs et de ses réseaux sociaux[26]. En effet, recourir à ces médias est un moyen courant aujourd'hui pour s'exprimer, faire part de ses activités et de ses relations avec des tiers. C'est à la fois Internet comme lieu et moyen d'expression en tant que citoyens et ce qu'on a appelé « *le Web 2.0 pour les loisirs* »[27]. Il est sur plusieurs points inenvisageable de respecter le régime ordinaire de la protection des données à l'occasion de ces communications.

L'application des lois de protection des données avec les multiples obligations qu'elle emporte vis-à-vis des tiers (obligation d'informer, etc.) soulève un problème délicat à l'égard de la liberté d'opinion et d'expression qui pourrait ainsi se voir restreindre.

L'affaire Linqvist tranchée par la Cour de Justice des Communautés européennes[28] illustre le propos. Peut-on sur Internet évoquer ses relations personnelles, associatives ou professionnelles sans devoir se soumettre aux exigences de la loi sur la protection des données à caractère personnel ? La Cour rappelle le devoir, compte tenu des circonstances, d'apprécier la proportionnalité de la restriction à l'exercice du droit à la liberté d'expression qu'entraîne l'application de règles visant à la protection des droits d'autrui. La formule est vague et renvoie à un jugement de proportionnalité. Ce jugement peut difficilement mettre sur le même pied l'expression journalistique qu'elle soit sous format traditionnel ou sur Internet, pour laquelle des règles ont progressivement été dégagées[29] et la libre expression de chacun dont l'existence renvoie nécessairement à celle d'autrui. Sur ce dernier point cependant, la CJCE a rendu récemment un arrêt accordant à toute communication au public de données à caractère personnel le régime dérogatoire qui avait été pensé pour la « presse »[30].

---

25 Article 9 de la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, *J.O.C.E.*, n° L 281 du 23 novembre 1995, pp. 31 et s.

26 V. Groupe 29, WP 163, avis 5/2009 sur les réseaux sociaux en ligne, adopté le 5 juin 2009.

27 Discours « l'Internet du futur: l'Europe doit jouer un rôle majeur» de Mme Reding, Commissaire européenne DG Société de l'Information et des Médias, à propos de l'Initiative «Futur de l'Internet» du Conseil Européen de Lisbonne (2 février 2009).

28 C.J.C.E., 6 novembre 2003, (Lindqvist), C-101-01, *Rec*. p. I-12971, par. 43 et 44. Voy. la note d'observations de C. de Terwangne qui aborde amplement cette question : C. de TERWANGNE, « Arrêt Lindqvist ou quand la Cour de Justice des Communautés européennes prend position en matière de protection des données personnelles », note sous C.J.C.E., 6 novembre 2003, *R.D.T.I.*, 2004, n° 19, pp. 67 et s.

29 A noter que les réglementations nationales varient sur la manière dont doit être atteint cet équilibre (Cf. à ce propos, la note de C. de TERWANGNE, précitée)

30 C.J.C.E. (gr. ch.), 16 décembre 2008, (Satakunnan Markkinapörssi Oy et Satamedia Oy), Affaire C-73/07, note C. de TERWANGNE, « Les dérogations à la protection des données en faveur des activités de journalisme enfin élucidées », *R.D.T.I.*, 2010, n° 38, pp. 132-146.

Les développements techniques apparus après l'adoption de la Convention n° 108 conduisent également à ce que **l'application des règles de protection des données porte atteinte au secret de la correspondance ou des communications**. C'est le recours au courrier électronique et autres échanges électroniques qui induit cette friction. Sous cette forme, la correspondance se transforme en traitement automatisé de données. Les règles de transparence, droit d'accès et droit de rectification sont dès lors applicable alors qu'elles ne le sont pas en présence de courrier classique papier (qui, faute de structuration des données, ne passerait pas même pour un fichier couvert par les règles de protection dans les Etats parties qui ont étendu le champ d'application de la Convention aux fichiers non automatisés). En conséquence, ces règles de protection permettent à des tiers mentionnés dans les échanges électroniques de prendre connaissance du contenu de ces échanges, ce qui réalise à l'évidence une atteinte au secret de la correspondance ou des communications. Un régime d'exceptions appropriées devrait prendre en compte cette confrontation entre protection des données et secret de la correspondance ou des communications.

L'utilisation des données de trafic réalise également une atteinte au secret des communications. Cette utilisation devrait être encadrée très strictement[31].

Certaines règles du régime de protection des données impliquent aussi un **risque d'atteinte à la liberté de la recherche scientifique**. La recherche, essentiellement médicale, utilise des données qui sont – la plupart du temps – codées de manière telle qu'il est difficile mais pas impossible de les lier à une personne physique déterminée. Les chercheurs scientifiques sont donc confrontés à devoir respecter les règles relatives à la protection des données à caractère personnel, règles qui sont bien souvent inapplicables pour eux.

Pensons ainsi aux divers droits de la personne concernée tel le droit d'accès aux données ou de rectification de celles-ci. Il est, en effet, impossible pour le chercheur ou son employeur de répondre à des demandes d'accès dès lors qu'il ne connaît pas les personnes physiques liées aux données (il ne travaille qu'avec des codes et ce n'est pas lui mais un tiers qui détient la clé du code). Si la définition de "données à caractère personnel" va jusqu'à englober toute donnée portant sur des individus identifiables par quelqu'un (dans l'exemple, le médecin à la source des données mais pas les chercheurs eux-mêmes qui ne disposent que de données codées), cette définition et, *a contrario*, la notion de données anonymes sous-jacente, peut s'avérer trop sévère et devenir une obstruction à la recherche. Il faudrait donc définir avec réalisme ces concepts.

1.2. CHAMP D'APPLICATION

1.2.1. Un élargissement ratione personae ?

Faut-il au delà de la protection des individus, prévoir une réglementation protectrice des profils[32] ? Le profilage s'entend de deux étapes : d'une part, la détermination d'une série de caractéristiques à propos d'un individu ou d'une collectivité d'individus en lien avec un ou des comportements opérés ou attendus et, d'autre part, le traitement subséquent de ces individus ou collectivités sur base de la reconnaissance de ces caractéristiques.

La question de l'encadrement juridique du profilage a débouché sur l'élaboration d'un projet de recommandation. Elle ne sera en conséquence plus retenue ici.

---

31 V. *infra* point 2.1.4.

32 A noter que cette réglementation existe en Suisse et partiellement en Norvège. Sur ces points, lire L. BYGRAVE, *Data Protection Law*, Kluwer Law International, Information Law Series, Den Haag, 2002, pp.185 et s.

1.2.2. Une restriction

La Convention 108 ne présente pas une restriction à son champ d'application qu'on retrouve dans toutes les législations des Etats membres de l'Union européenne (à l'invitation de la directive 95/46). Il s'agit des traitements **de données effectués « par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques »**[33]. Ces traitements sont donc exclus de la directive et de tous les textes nationaux qui l'ont transposée.

La loi canadienne sur la protection des renseignements personnels et les documents électroniques prévoit également une telle exclusion. Son article 4, § 2 (b) stipule que le régime de protection ne s'applique pas « *b*) à un individu à l'égard des renseignements personnels qu'il recueille, utilise ou communique à des fins personnelles ou domestiques et à aucune autre fin ».

L'APEC Privacy Framework a introduit une restriction du même type à son champ d'application par le biais d'une exception apportée à la définition de *personal information controller*. Ainsi, est exclu de cette définition tout individu « who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs »[34].

La Résolution de Madrid admet, elle, que les lois nationales prévoient une exclusion du champ d'application pour les traitements réalisés par une personne physique dans le cadre d'activités exclusivement en lien avec sa vie privée ('private life') et familiale (Article 3, § 2).

L'importance mais la difficulté d'application d'une telle exception dans le contexte technologique actuel, principalement le Web 2.0, fait l'objet de développements réservés au point 7, *infra*.

2. Définitions

2.1. LA NOTION DE DONNEE A CARACTERE PERSONNEL (ARTICLE 2. LITTERA A)

Aux termes de l'article 2, alinéa a. de la Convention, la donnée à caractère personnel doit s'entendre de « toute information concernant une personne physique identifiée ou identifiable ('personne concernée') ». Cette définition est désormais classique et reprise dans la plupart des instruments de protection des données. Il est à noter toutefois que le *Privacy Framework* de l'APEC se distingue de cette approche en ne visant par les données à caractère personnel que les données identifiantes (directement ou indirectement). Il est stipulé "The APEC Privacy Framework applies to personal information, which is information that can be used to identify an individual. It also includes information that would not meet this criteria alone, but when put together with other information would identify an individual."[35] Cette approche est plus restreignante.

2.1.1. L'identité : une notion ambiguë à la base de la définition de donnée à caractère personnel

La notion de donnée à caractère personnel repose sur l'identification ou l'« identifiabilité » des individus concernés par les données. En principe, la réglementation de protection des données n'est applicable que si la donnée traitée peut être référée à une personne déterminée. Or la notion

---

33 Art. 3.2 de la directive 95/46.

34 APEC Privacy Framework, November 2004, disponible à l'adresse <http://www.apec.org/content/apec/apec_groups/som_special_task_groups/electronic_commerce.html>, Part II Scope, § 10. Le commentaire de cette disposition apporte cet éclaircissement : « Individuals will often collect, hold and use personal information for personal, family or household purposes. For example, they often keep address books and phone lists or prepare family newsletters. The Framework is not intended to apply to such personal, family or household activities".

35 APEC Privacy Framework, Part II Scope.

d'identité est peu évidente lorsqu'on la confronte à certaines réalités nouvelles. Ainsi, l'étiquette RFID qui suit un vêtement[36] est-elle une donnée à caractère personnel alors qu'elle se rapporte, directement du moins, à un objet, de même que le numéro IP qui se rapporte en définitive à un ordinateur et non à un utilisateur précis ?

La notion d'identité est ambiguë (cf. ce qui est dit sur ce point dans la première partie de ce rapport présentée dans un document joint).

L'identité a la fâcheuse tendance d'être interprétée de manière restrictive par l'industrie. Une telle interprétation présente l'avantage de faire échapper aux règles de protection des données puisqu'elle évacue la présence de données à caractère personnel.
A titre d'exemple de cette interprétation restrictive, on peut citer le cas de la volonté de fusion entre les banques de données d'Abacus[37] et de DoubleClick. On ne peut d'ailleurs que s'étonner que la fusion entre les profils "anonymes[38]" de DoubleClick et la banque de données nominatives d'Abacus ait été techniquement possible. Cela signifie tout simplement que DoubleClick qui prétendait ne collecter aucune information relative à une personne identifiable possédait néanmoins un point d'ancrage permettant de faire le lien. Ce lien est bien probablement le fameux cookie identifiant que DoubleClick a installé sur des millions d'ordinateurs personnels[39]. Il suffit qu'un hyper lien invisible soit présent sur un formulaire nominatif en ligne pour que DoubleClick puisse faire ce lien.

Une tendance actuelle de l'industrie consiste[40] donc à considérer des points d'ancrages et de simples données biographiques y associées comme étant des données se rapportant à un individu non identifiable[41]. Des points de contact stables dans le temps sont généralement admis comme étant des données à caractère personnel. En d'autres termes, la surveillance et la traçabilité d'un individu

---

36 C'est l'exemple d'une des premières applications des RFID, les puces insérées dans les vêtements Benetton.

37 « a cooperative membership database, contains records from more than 1,100 merchandise catalogs, with more than 2 **billion** consumer transactions from virtually all U.S. consumer catalog buying households » lu sur http://www.abacus-direct.com en mai 2004

38 http://www.doubleclick.net/company_info/about_doubleclick/privacy : " *DoubleClick does not collect any personally-identifiable information about you, such as your name, address, phone number or email address.*

39 DoubleClick délivre plus d'un milliard de bannières publicitaires par jour.

40 La déclaration de confidentialité de Microsoft Update va dans le même sens. Après avoir déclaré que le site collecte les informations suivantes

1. Numéro de version du système d'exploitation
2. Numéro de version d'Internet Explorer
3. Numéro de version des autres logiciels pour lesquels Windows Update fournit des mises à jour
4. Numéro d'identification Plug and Play des périphériques
5. Paramètre régional et linguistique

la « privacy policy » de Microsoft disponible sur : http://v4.windowsupdate.microsoft.com/fr/default.asp spécifie que *« Le système d'exploitation Windows génère un identificateur global unique (GUID, Globally Unique IDentifier) qui est stocké sur votre ordinateur afin d'identifier celui-ci de façon unique. Le GUID ne contient aucune information permettant de vous identifier personnellement et ne peut pas être utilisé pour vous identifier.* »

41 La première étude de mise en application du Safe Harbor révèlait la façon dont les entreprises américaines ont tendance à définir la notion de données à caractère personnelle comme la donnée permettant l'identification directe par le maître du fichier des personnes concernées (J. DHONT, V.PEREZ, Y. POULLET avec la collaboration de J.REIDENBERG et L. BYGRAVE, *Safe Harbour Agreement Implementation Study*, étude disponible sur le site*:* http://europa.eu.int/com/internal_market/privacy/index_en.htm. ….)

ou des biens qu'il utilise ou possède ne sont pas majoritairement perçues comme une atteinte à la vie privée si la personne n'est pas identifiable et reste anonyme (c'est à-dire si on ne connaît pas son nom ou si on ne sait pas la contacter)[42]. Comme si nos comportements n'étaient pas constitutifs en soi de notre identité.

2.1.2. Le caractère « identifiable »

Un problème est à relever dans la portée du qualificatif « identifiable » attaché à une personne physique pour en faire une « personne concernée ». Le Rapport explicatif concernant la Convention n° 108 signale que l'on entendait viser par « personne identifiable » une personne qui peut être « facilement » identifiée, ce qui ne couvre pas l'identification de personnes « par des méthodes très complexes »[43]. Cette clarification n'est plus suffisante. Le critère de complexité des méthodes à utiliser pour identifier une personne n'est pas suffisamment éclairant. Aujourd'hui des méthodes « très complexes » d'un point de vue technique ne sont plus nécessairement hors de portée.

Le projet de Recommandation sur le profilage ne recourt plus au critère de complexité des méthodes d'identification mais plutôt à celui de l'ampleur des moyens à mettre en œuvre pour aboutir à l'identification des individus. Ainsi, ce texte énonce : "An individual is not considered "identifiable" if identification requires unreasonable time or manpower"[44].

Il conviendrait de trouver le critère adéquat, exercice essentiel puisque ce critère est la clé de la notion de données à caractère personnel et, par contraste, de données anonymes. Par exemple, si la personne qui détient l'identification du sujet d'une donnée est tenue par un secret professionnel et ne peut communiquer cette information sous peine de sanction pénale, la donnée sera-t-elle considérée comme identifiable ? Vraisemblablement non. Mais en sera-t-il de même si l'obligation de secret n'est plus pénale mais contractuelle ?

La notion de donnée à caractère personnel mérite assurément d'être clarifiée au regard des formes qu'elle a été appelée à prendre à la suite des développements technologiques. Il s'agit notamment de tenir compte des pratiques des prestataires de service sur Internet.

Dans le cadre de la réflexion, on notera que considérer une donnée comme le cookie, l'adresse IP ou un *Global Unique Identifier* comme « donnée à caractère personnel »[45] entraîne l'application des dispositions de la Convention et peut dès lors conduire à rechercher l'identité des personnes concernées, ne serait-ce que pour permettre l'exercice du droit d'accès, alors même que cela n'était pas nécessaire pour les besoins de l'activité du maitre du fichier. Par ailleurs, appliquer des dispositions comme l'obligation d'informer la personne concernée pourrait s'avérer impossible sans l'identifier.

Par contre, ne pas traiter l'adresse IP et le G.U.I. comme donnée à caractère personnel poserait problème au vu des risques que l'utilisation postérieure de ces données représente en termes de profilage de l'individu voire de possibilité de le contacter. A cet égard, on relève qu'avec la

---

42 Voir la Privacy Policy de DoubleClick : A la question : « Les utilisateurs ont-ils accès à leurs informations personnelles recueillies par le site Web ? », le site répond **: «** Aucune information d'identification personnelle n'est recueillie, aucune n'est donc accessible. »

43 Rapport explicatif, p. 14.

44 Draft Recommendation Appendix, 1. Definitions, a.

45 Le Groupe de l'article 29 a répété à plusieurs reprises que les adresses IP devaient selon lui être considérées comme des données à caractère personnel (Groupe de l'article 29, WP 136 ; WP 148 ; WP 150, avis 2/2008 sur la révision de la directive 2002/58/CE concernant la protection de la vie privée dans le secteur des communications électroniques, 15 mai 2008.

combinaison d'outils de surveillance du trafic sur le web, on peut facilement cerner le comportement d'une machine et derrière celle-ci de son utilisateur. On reconstitue ainsi la personnalité de l'individu pour lui appliquer certaines décisions. Sans même s'enquérir de l'« identité » de l'individu, c'est-à-dire de son nom et son adresse, on peut caractériser ce dernier en fonction de critères socio-économiques, psychologiques, philosophiques ou autres et lui appliquer certaines décisions dans la mesure où le point de contact de l'individu (l'ordinateur de l'individu) ne nécessite plus nécessairement la révélation de son identité au sens étroit du terme. En d'autres termes, la possibilité d'agir vis-à-vis d'un individu ne nécessite plus nécessairement la possibilité de connaître son identité.

L'important désormais dans le nouveau contexte technologique, c'est l'individualisation davantage que l'identification. Doit-on en arriver à faire évoluer la définition de donnée à caractère personnel ou lui adjoindre une définition qui ne couvre plus les données relatives à une personne que l'on peut identifier mais bien que l'on peut individualiser ?

Il est intéressant de noter que, même si elles donnent une définition semblable de la donnée à caractère personnel, les Lignes directrices de l'OCDE apportent une clarification de la notion dans l'Exposé des motifs qui évacue le caractère identifiable de la personne concernée. Ainsi, il y est dit : « En principe, les données à caractère personnel transmettent une information qui, par des liaisons directes (numéro matricule civil, par exemple), peut être rattachée à une *personne physique particulière*. » (c'est nous qui soulignons).

De la même manière, la directive 2002/58 Vie privée et communications électroniques donne une définition des données de trafic et des données de localisation (V. ci-dessous) qui dans les deux cas évite l'évocation d'un rapport à un individu identifié ou identifiable. Par application de ces définitions, il suffit qu'un lien puisse être fait avec un terminal, un objet, et qu'à travers celui-ci une personne, le possesseur de ce terminal, même non identifiée puisse être atteinte ou caractérisée pour que la directive 2002/58 s'applique[46].

2.1.3. Les données biologiques et biométriques

La Cour européenne des droits de l'homme a relevé que des empreintes digitales, des profils ADN et des échantillons cellulaires, constituent tous « des données à caractère personnel au sens de la Convention du Conseil de l'Europe de 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel »[47]. Cette position n'est pas évidente. Du sang ou un échantillon buccal serait donc une donnée à caractère personnel ? On pourrait plutôt penser qu'un échantillon cellulaire contient des données sans en être lui-même.

Il serait opportun d'éclairer la notion de donnée à caractère personnel en présence de données biologiques et biométriques.

---

[46] Voy. Y. POULLET, « Pour une troisième génération de réglementation de protection des données », in *Défis du droit à la protection de la vie privée, Perspectives du droit européen et nord-américain – Challenges of Privacy and Data Protection Law, Perspectives of European and North American Law*, M.V. Perez-Asinari et P. Palazzi (ed.), coll. Cahiers du CRID, n° 31, Bruxelles, Bruylant, 2008, p. 51.

[47] Cour eur. D.H. (Gr. Ch.), *S. et Marper c. Royaume-Uni*, arrêt du 8 décembre 2008, req. n° 30562/04 et 30566/04, par. 68.

2.1.4. Les données de trafic et de localisation : un régime spécifique ?

Faut-il appréhender les données de trafic et de localisation comme des données à caractère personnel appelant une réglementation spécifique et dès lors comme devant faire l'objet d'une définition reprise dans la liste de l'article 2 ?

Ces données sont définies par la directive européenne 2002/58 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques[48], comme suit :

- « données de trafic : toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation » ;
- « données de localisation : toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public. ».

Le statut particulier des données de localisation et de trafic s'explique par le caractère dangereux du traitement systématique de telles données qui révèlent les déplacements, l'entourage habituel, les habitudes de consommation et de vie[49]. En outre, l'utilisateur des services de communications électroniques, sauf dans le cas de services à valeur ajoutée, se trouve dans une position de relative faiblesse, dans la mesure où l'utilisation du réseau suppose implicitement la génération, le stockage et la transmission de nombreuses données techniques dont le sens et l'utilisation potentiels lui échappent et dont il ne peut suivre facilement la trace (l'opacité du fonctionnement des réseaux).

A titre d'illustration des enjeux liés aux données de géolocalisation, l'OCDE propose l'exemple suivant : « *Un opérateur mobile utilise un système GPS (Global Positioning System) ou un système de triangulation (à partir des signaux émis par le terminal) pour localiser les utilisateurs mobiles. L'entreprise vend les informations concernant l'abonné et sa localisation à des entreprises de marketing qui les utilisent pour adresser à l'abonné mobile des publicités ou messages personnalisés. L'abonné mobile n'a pas compris que dans ce système ses données personnelles sont communiquées à autrui, et il n'a pas donné son accord à cet effet. Il peut arriver que des messages d'information lui soient facturés (par exemple facturation de SMS envoyés concernant les ventes proposées à proximité, ou du temps de connexion sur Internet pour l'affichage des messages « pop-up »). Il est troublé par le fait qu'on puisse savoir où il est, et inquiet que l'information puisse être interceptée (volée ou achetée) par des [personnes mal intentionnées]*[50] ».

Il est en fait également possible de localiser un individu en recourant aux traces qu'il laisse, traces par exemple liées à l'usage d'une carte de crédit, ou de tickets électroniques d'accès aux transports en commun. Ces traces ne sont toutefois pas comprises comme des données de localisation au sens où on l'entend ici.

---

48 La recommandation n° R(99) 5 du Comité des Ministres du Conseil de l'Europe sur la protection de la vie privée sur Internet ne prévoit ni définition, ni réglementation particulière de ce type de données.

49 Voy. dans le même sens, Groupe de l'article 29, Avis 5/2005 sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée, WP 115, 25 novembre 2005, p. 3 : « La sensibilité particulière du traitement de ces données, qui met en jeu la question essentielle de la liberté de circuler anonymement, a conduit le législateur européen […] à adopter un régime particulier qui impose de recueillir le consentement de l'utilisateur ou de l'abonné préalablement au traitement des données de localisation nécessaires à la fourniture d'un service à valeur ajoutée et d'informer les personnes concernées des conditions de ce traitement ».

50 OCDE, « Orientations de l'OCDE pour les politiques pour la prise en compte des questions de protection et d'autonomisation des consommateurs dans le commerce mobile », Réunion ministérielle de l'OCDE Le futur de l'économie Internet, Séoul, juin 2008, p. 22.

Par contre, ce sont bien des données de localisation qui sont utilisées pour offrir des services de repérage des personnes inscrites (groupes d'amis ou inconnus intéressés à rencontrer des personnes géographiquement proches) qui se sont multipliés tels *Find a friend*, nécessitant la localisation continue des personnes inscrites.

Au vu des enjeux des données de localisation, la Directive 2002/58 limite *a priori* les traitements de telles données, à une seule exception près : avec le consentement dûment informé et révocable à tout moment de la personne concernée.

L'OCDE estime qu'il serait judicieux que les entreprises « donnent aux consommateurs des indications claires sur toutes les informations de localisation qui sont recueillies et sur l'usage auquel ces informations sont destinées », de même qu'elles « donnent aux consommateurs la possibilité de restreindre l'échange de données avec des tiers (à l'exception des situations d'urgence), et de revenir sur leur décision concernant ceux avec lesquels ces données peuvent être échangées »[51].

Aux États-Unis, la possibilité dont dispose un opérateur de communiquer à des tiers des informations de géolocalisation relatives aux abonnés est limitée par les dispositions légales relatives à l'utilisation des informations de réseau propriétaires concernant la clientèle (Customer Proprietary Network information ou CPNI). Ainsi, l'article 222 de la Loi fédérale sur les communications interdit la communication ou l'utilisation des informations de localisation de terminaux sans fil, obtenues par un opérateur dans le cadre de sa prestation de services de télécommunications, sans le consentement préalable expresse de l'abonné. On ne peut se passer du consentement de l'abonné que dans des situations d'urgence particulières (afin de permettre de répondre à un appel d'urgence d'un abonné). De plus, la Loi CAN SPAM (Controlling the Assault of Non-Sollicited Pornography and Marketing) interdit l'envoi de messages commerciaux de service mobile directement sur des terminaux sans fil via Internet sans l'autorisation préalable expresse du destinataire.[52]

2.2. LES NOTIONS DE FICHIER (ARTICLE 2, LITTERA B) ET DE TRAITEMENT AUTOMATISE (ARTICLE 2, LITTERA C)

Le traitement tel que défini ne couvre pas la collecte des données. Cette opération de base est explicitement exclue de la définition de traitement dans le Rapport explicatif (p. 14). Or, il est important que cette opération doive répondre aux exigences contenues dans le régime de protection. Il est vrai que l'article 5 prévoit que l'obtention des données doit être réalisée de manière loyale. Par ailleurs, lorsque l'on collecte des informations sur la toile ou via un des protocoles d'Internet, il y a toujours enregistrement, au moins sur la mémoire RAM de l'ordinateur. Etant donné que l'enregistrement des données constitue à lui seul un traitement, on se trouvera bien en présence d'un traitement de données par le seul fait de la collecte.

Faut-il vraiment en conséquence voir dans cette omission volontaire une lacune ?

Signalons que la Cour européenne des droits de l'homme a expressément inclus la collecte de données, séparément de leur enregistrement, dans les opérations portant atteinte à la vie privée. Elle a ainsi relevé dans son arrêt *Antunes Rocha* que « la collecte, la mémorisation et l'éventuelle communication de données relatives à la « vie privée » d'un individu entrent dans le champ d'application de l'article 8 § 1 de la Convention (*Leander c. Suède*, arrêt du 26 mars 1987, série A n° 116, p. 22, § 48 ; *Rotaru c. Roumanie* [GC], n° 28341/95, § 43, CEDH 2000-V). Même des données de nature publique peuvent relever de la vie privée lorsqu'elles sont, d'une manière systématique, recueillies et mémorisées dans des fichiers tenus par les pouvoirs publics (*Rotaru* précitée, *ibidem*) » et qu' « qu'il y a eu une ingérence dans la « vie privée », au sens de l'article 8, de la requérante,

---

51 *Ibidem*, p. 23.

52 Cité dans OCDE, « Orientations de l'OCDE pour les politiques pour la prise en compte des questions de protection et d'autonomisation des consommateurs dans le commerce mobile », Réunion ministérielle de l'OCDE Le futur de l'économie Internet, Séoul, juin 2008, p. 27.

ingérence causée par la collecte de renseignements effectuée à son sujet par les autorités, indépendamment de la question de savoir quelle forme a revêtu cette collecte. »[53]

S'indique-t-il d'ajouter d'autres opérations à la liste de la définition du traitement automatisé ? Qu'en est-il de la communication de données, de leur rapprochement ou de leur interconnexion ?

Quant à la notion de « fichier automatisé », elle recouvre une réalité différente de ce qui est entendu par « fichier » dans le texte de la directive 95/46. Le « fichier automatisé » de la Convention 108 signifie « tout ensemble d'informations faisant l'objet d'un traitement automatisé », tandis que le « fichier » de la directive recouvre « tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ». Dans le cas visé par la directive, la structuration des données est une condition indispensable pour être en présence d'un fichier. Cette condition n'apparait pas du tout dans la définition de la Convention. En outre, c'est dans un contexte totalement non technique que la notion de fichier de la directive trouve à s'appliquer, à l'inverse de la notion de la Convention.

Le recours à deux termes identiques de portée différente au sein de deux textes qui doivent tous deux servir de référence pour une série d'Etats risque d'amener à des confusions et n'est certes pas souhaitable.

2.3. LE « MAITRE DU FICHIER » (ARTICLE 2, LITTERA D)

L'article 2, littera d, de la Convention 108 définit le maitre du fichier comme étant *"la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui est compétent selon la loi nationale, pour décider quelle sera la finalité du fichier automatisé, quelles catégories de données à caractère personnel doivent être enregistrées et quelles opérations leur seront appliquées".*

En parlant de « maître du fichier », la Convention 108 *"vise exclusivement la personne ou l'organe responsable en dernier ressort du fichier et non pas les personnes qui procèdent aux opérations de traitement conformément aux instructions du maître du fichier"*[54]

Il convient de revoir cette définition de « maître du fichier ».

On constate, à la lecture de cette définition, que la Convention 108 a considéré que le "Maître de fichier" avait une fonction de décision à plusieurs niveaux: d'une part il doit déterminer la finalité du fichier qu'il "crée" et, d'autre part, les données qui le nourriront ainsi que les opérations qui leur seront appliquées. L'accent a donc été mis sur le rôle ultime de cet acteur.

Il semble cependant que cette vision ne corresponde plus réellement à l'environnement actuel. Il est, en effet, intéressant de souligner qu'à l'heure actuelle le rôle de "maître du fichier" n'est plus attaché au seul fichier traité mais à l'ensemble du traitement qui est devenu l'élément central. Il semble donc cohérent de faire glisser la notion de maître de fichier vers celle de responsable de traitement. Ainsi que le souligne de Groupe de travail "article 29" sur la protection des données, le fait de passer de la notion de fichier à celle de traitement à permis de glisser d'une *"définition statique liée à un fichier à une définition dynamique associée à l'activité de traitement"*[55].

Cette modification permettrait également d'intégrer de manière plus efficace le principe selon lequel cet acteur serait responsable de toute la chaîne constituant un traitement ce qui offrirait une plus grande protection à la personne concernée. En effet, la personne concernée aurait un seul et même

---

53 Cour eur. D.H., *Antunes Rocha c. Portugal*, arrêt du 31 mai 2005, Req. n° 64330/01, par. 65.

54 Rapport explicatif de la Convention 108, point 32.

55 Groupe de l'article 29, Avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant», p. 13.

interlocuteur qui aurait un contrôle à partir du recueil des données jusqu'à leur destruction, en ce compris l'anonymisation.

Par ailleurs, la pratique indique que, dans certaines situations, le "maître du fichier" est bicéphale ou même tricéphale, situation qui n'est pas rencontrée par la Convention 108 dans sa version actuelle. Pensons ainsi à l'hypothèse du *cloud computing* ou de plateforme de *e-Health*. Il serait peut-être utile de prévoir l'hypothèse d'un travail conjoint d'une ou plusieurs personnes, comme cela est le cas dans la Directive 95/46, même si cela soulève inévitablement une question de droit applicable (v. ci-dessous).

Il y a lieu ensuite de **clarifier le critère qui est repris dans le texte actuel de la Convention :** « compétent […] pour décider quelle sera la finalité du fichier automatisé, quelles catégories de données à caractère personnel doivent être enregistrées et quelles opérations leur seront appliquées » (art. 2, littera d). Cette clarification peut se faire dans l'esprit de ce qui est indiqué dans le Rapport explicatif de la Convention dans lequel il est spécifié que la Convention « vise exclusivement la personne ou l'organe responsable en dernier ressort du fichier et non pas les personnes qui procèdent aux opérations de traitement conformément aux instructions du maître du fichier »[56]. Le critère du « responsable en dernier ressort du fichier » est assurément un bon critère car il rejoint ce qui a émergé de la pratique, qui est que l'on souhaite voir le responsable du traitement dans la personne qui exerce le vrai contrôle du traitement des données, qui dispose d'un véritable pouvoir de décision quant au traitement.

Dans la Résolution de Madrid il a été clairement opté pour un critère unique conduisant à désigner celui qui détient le pouvoir de décision sur le traitement des données. Ce texte précise que par "Responsible person" il faut entendre « any natural person or organization, public or private which, alone or jointly with others, decides on the processing » (Article 2, d.).

L'APEC Privacy Framework retient également un critère unique pour désigner la personne de reference en matière de traitement. Il s'agit précisément du critère du conrôle évoqué ci-dessus. Ce texte désigne par « Personal information controller » "a person or organization who controls the collection, holding, processing or use of pesonal information" (Part II, Définitions, § 10).

Cette clarification permettrait de rencontrer la critique qui, dans le cadre de la directive 95/46, s'est élevée à propos de la coexistence de deux critères. Recourir à plusieurs critères de détermination du responsable du traitement peut évidemment conduire à identifier plusieurs personnes comme responsable et par là-même peut conduire à des problèmes d'application concurrente de plusieurs lois nationales si le critère de la loi applicable est lié au responsable du traitement et à son établissement (comme c'est le cas pour la directive 95/46)[57]. Or, l'on retrouve dans la définition retenue dans la version de 1981 de la Convention 108 un triple critère censé refléter l'exercice de la responsabilité du fichier : il est question de la compétence pour décider de la finalité du fichier automatisé ainsi que pour décider des catégories de données et des opérations à appliquer.

Dans un second temps, **on peut s'interroger sur l'intérêt d'intégrer d'autres notions dans la Convention qui correspondraient aux acteurs classiques ou nouvellement apparus qui jouent un rôle en la matière.**

Ces acteurs sont tout d'abord les **sous-traitants**, notion qui désigne la personne, au sens large, qui travaille sous les instructions du maître du fichier/responsable de traitement pour effectuer les tâches que ce dernier n'est pas à même d'effectuer. On pense notamment aux tâches de sécurité. Le

---

56 Rapport explicatif, pp. 14-15.

57 Pour un exemple d'une critique en ce sens, v. D. KORFF, *Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments*, EC Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, WP 2, 20 January 2010, pp. 60 et s.

sous-traitant est donc la personne extérieure au maître du fichier, en charge des aspects délégués (généralement techniques) d'un traitement de données. Les sous-traitants jouent un rôle prépondérant dans le contexte du *cloud computing*, notamment.

La directive 95/46 définit le sous-traitant comme « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. » (article 2, e.)

La Résolution de Madrid, pour sa part, dispose : « "Processing service provider" means any natural person or organization, other than the responsible person that carries out processing of personal data on behalf of such responsible person. » (Article 2, e.)

Là où elle existe, cette notion n'est pas sans soulever des difficultés d'application. Il n'est en effet pas toujours évident de distinguer les notions de maître du fichier/responsable du traitement et de sous-traitant. C'est particulièrement vrai lorsqu'on se trouve en présence d'une organisation complexe comme une entreprise multinationale ou un groupement d'entreprises.

Parmi les nouveaux intervenants[58], on trouve les **opérateurs de réseaux**, en ce compris les fournisseurs d'accès à Internet. Ils sont les interfaces obligées entre l'utilisateur du réseau en tant que personne concernée et les multiples acteurs d'Internet qui pourront traiter les données générées consciemment ou non par l'utilisation du réseau. A eux pourraient incomber certains devoirs comme celui de prévenir des risques liés à l'utilisation du réseau, celui de garantir la sécurité de leurs services, celui de permettre des restrictions à l'identification de la ligne appelante, etc.

Les **fournisseurs d'équipements techniques** (notamment de logiciels de navigation) interviennent aussi dans le nouveau paysage. Il pourrait être envisagé de les rendre destinataires d'obligations en termes de normes techniques et de les rendre responsables du respect de telles normes (v. *infra* le point sur la prise en compte du respect de la vie privée dès la conception/Privacy by Design).

3. Principes de protection

3.1. ARTICLE 5 : QUALITE DES DONNEES, INADEQUATION DE L'INTITULE

L'article 5 de la Convention, intitulé « Qualité des données », est la disposition centrale comportant l'essentiel des principes de protection. L'intitulé de cet article est assurément inadéquat. En effet, le contenu de cette disposition dépasse la qualité des données proprement dite. Seuls les points c. et d. correspondent à une question de qualité des données (qui doivent être adéquates, pertinentes et non excessives par rapport aux finalités, et qui doivent être exactes et à jour). Ainsi, la règle concernant la collecte loyale et licite (littera a.) et celle relative au principe de finalité (induisant l'exigence d'utilisations compatibles des données et de conservation limitée) (littera b. et e.) ne peuvent être vues comme l'expression d'exigences de qualité des données. D'ailleurs, le Rapport explicatif de la Convention le stipule clairement : « Deux règles principales sont exprimées par les différentes dispositions de cet article. D'une part, l'information elle-même doit être correcte, pertinente et non excessive par rapport à sa finalité. D'autre part, son utilisation (collecte, enregistrement, diffusion) doit également être correcte »[59].

---

[58] V. Y. POULLET, « Pour une troisième génération de réglementation de protection des données », in *Défis du droit à la protection de la vie privée*, *Perspectives du droit européen et nord-américain – Challenges of Privacy and Data Protection Law*, *Perspectives of European and North American Law*, M.V. Perez-Asinari et P. Palazzi (ed.), coll. Cahiers du CRID, n° 31, Bruxelles, Bruylant, 2008, p. 54.

[59] Rapport explicatif, précité, p. 17.

Dans l'hypothèse où la Convention doit servir de modèle international de régime de protection des données, il est important que le texte soit clair et parlant ; la vocation éducative du texte n'est pas à négliger.

Les Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel contiennent, à côté du principe de la qualité des données, le principe de la spécification des finalités et celui de la limitation de l'utilisation. Les Principes directeurs de l'ONU pour la réglementation des fichiers informatisés contenant des données à caractère personnel[60], quant à eux, distinguent le principe de licéité et de loyauté, le principe d'exactitude et le principe de finalité.

3.2. PRINCIPE DE PROPORTIONNALITE

On ne trouve pas de formulation explicite dans la Convention du principe de proportionnalité, principe selon lequel l'atteinte aux intérêts de la personne qu'induit le traitement de ses données ne peut être disproportionnée par rapport à l'intérêt que le traitement des données représente pour son responsable. La seule manifestation expresse de ce principe se situe dans l'exigence de données « non excessives », données que, même pertinentes, on ne peut traiter car cela porterait excessivement atteinte à la personne concernée par rapport à l'intérêt que représente leur traitement pour le responsable de celui-ci. On peut également voir dans l'obligation de restreindre la collecte aux seules données adéquates et pertinentes une manifestation du principe de proportionnalité dans la mesure où par cette exigence, on veille à ce que l'atteinte soit réduite à ce qui est strictement nécessaire. Le CEPD s'est exprimé dans ce sens dans un de ses avis où il a insisté sur l'importance de maintenir un équilibre approprié entre les droits fondamentaux de la personne concernée et les intérêts des différents acteurs en présence, ce qui suppose que la quantité de données à caractère personnel traitées soit la plus limitée possible.

La doctrine a estimé que **l'exigence de finalités « légitimes » énoncée à l'article 5, b. de la Convention correspondait à cette exigence de proportionnalité**. Pour être légitime une finalité ne peut causer un préjudice plus grand que l'intérêt que représente le traitement.

La loi canadienne sur la protection des renseignements personnels et les documents électroniques contient une formulation intéressante sur les finalités de traitement acceptables. Aux termes de son article 5, § (3), toute organisation privée « ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances ». Il est donc fait appel à une mise en balance des intérêts en présence, effectuée au niveau d'un individu abstrait et non l'individu impliqué dans une situation donnée. Il est clair en effet que pour estimer des finalités acceptables la personne raisonnable pèsera le pour et le contre du traitement, les implications que ce traitement pourrait avoir sur sa situation et ses intérêts. Il convient de relever que, contrairement à l'exemple canadien, la balance d'intérêts qui doit présider à la vérification de la proportionnalité ne devrait pas être limitée à un point de vue privé mais devrait également comprendre un point de vue supérieur, intégrant les intérêts de la société dans son ensemble.

I**l serait sans doute judicieux et à tout le moins pédagogique de faire apparaître clairement dans le texte de la Convention l'exigence du respect du principe de proportionnalité**. Il est en effet devenu crucial aujourd'hui d'inscrire cette obligation qui peut servir de rempart face aux risques de certains développements techniques (notamment les traitements insoupçonnés qui foisonnent sur Internet) et au recours très (abusivement ?) répandu au consentement des personnes concernées pour traiter leurs données. Si la présence d'un consentement permet de présumer la légitimité d'un traitement, la mise en balance des intérêts en présence et la vérification de l'équilibre atteint offre une

[60] Assemblée générale de l'ONU, Résolution 45/95 du 14 décembre 1990.

sauvegarde bienvenue quand on songe aux défauts trop souvent attachés au consentement (information insuffisante de la personne concernée, manifestation du consentement déduite de la non-modification de conditions par défaut, etc.).

Cette exigence ne devrait pas être limitée aux finalités du traitement mais valoir également pour chaque opération effectuée sur les données.

En présence de données génétiques et d'empreintes digitales, la Cour européenne des droits de l'homme a réclamé une « mise en balance attentive des avantages pouvant résulter d'un large recours à ces techniques, d'une part, et des intérêts essentiels s'attachant à la protection de la vie privée »[61].

La CJUE a dès son premier arrêt en la matière établi que l'article 8 CEDH devait se lire en filigrane de la directive 95/46, ce qui implique de vérifier, en présence d'un traitement de données, s'il respecte le principe de proportionnalité contenu au paragraphe 2 de cette disposition[62].

3.3. LE CONSENTEMENT ET LES BASES DE LEGITIMITE D'UN TRAITEMENT

3.3.1. Le consentement

La Convention n° 108 ne réserve pas de place officielle au consentement de la personne concernée. A l'inverse de l'article 8 de la Charte des droits fondamentaux de l'Union européenne et de la directive 95/46, ainsi que de la Résolution de Madrid, elle ne consacre pas le consentement comme fondement de la légitimité des traitements de données.

Faut-il y voir une lacune alors que les critiques s'élèvent face au recours systématique au consentement comme fondement de la légitimité de certains traitements opérés dans le cadre de l'utilisation par la personne concernée des services du Web 2.0 et autres[63] ?

La forme et les conditions du consentement sont également source de grande préoccupation, des situations telles que la non-opposition aux conditions d'utilisation des données proposées par le fournisseur de service sur une page internet « subalterne », le non « décochage » de cases pré-cochées, la non-modification des paramètres par défaut, sont avancées comme correspondant à des consentements.

L'opacité des réseaux, le fait que de nombreux traitements de données échappent aux personnes concernées et le fait que nombre d'individus ne prennent pas la juste mesure des implications que les traitements présentent, conduisent à s'inquiéter de ces consentements présupposés.

---

61 Cour eur. DH (Gr. Ch.), *S. et Marper c. Royaume-Uni*, 4 décembre 2008, req. nos 30562/04 et 30566/04, § 112.

62 C.J.C.E., arrêt du 20 mai 2003, (Österreichischer Rundfunk e.a.), C-465/00, C-138/01 et C-139/01 : « Aussi, pour les besoins de l'application de la directive 95/46, […] importe-t-il de vérifier, en premier lieu, si une réglementation telle que celle en cause dans les affaires au principal prévoit une ingérence dans la vie privée et, le cas échéant, si cette ingérence est justifiée au regard de l'article 8 de la CEDH. » (§ 72) ; la Cour indique qu'il faut examiner si la disposition autrichienne en cause « est conforme à l'article 8 de la CEDH, au regard de l'exigence de proportionnalité, par rapport aux objectifs poursuivis » (§ 80). « Il convient, en ce sens, de mettre en balance l'intérêt de la république d'Autriche à garantir une utilisation optimale des fonds publics […] avec la gravité de l'atteinte au droit des personnes concernées au respect de leur vie privée » (§ 84).contribution

63 Article 29 Working Party and Working Party on Police and Justice, WP 168, The Future of Privacy – Joint contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data, adopted on 1 December 2009, §§ 65-68.

Dans la mesure où les réseaux modernes sont interactifs, le consentement peut plus facilement être réclamé comme fondement de légitimité des traitements et être préféré à d'autres fondements plus traditionnels comme la balance d'intérêts.

Cette considération amène certains à considérer dès lors que le consentement peut suffire pour légitimer un traitement. A cet égard, on rappelle que le développement par le World Wide Web Consortium (W.3.C.) de la *Platform for Privacy Preferences* (P.3.P.)[64] reposait également sur la possibilité pour l'internaute de négocier avec le fournisseur de services qui ne répondait pas à ses *Privacy Preferences* et d'aboutir alors à un accord qui serve de fondement légitime au traitement considéré. Même si cette négociation n'a jamais été déployée à une grande échelle, notamment par le biais d'agents électroniques, P3P reste révélateur de la volonté de l'industrie de se donner les moyens de négocier avec la personne concernée l'utilisation qui pourrait être faite de ses données. La protection de la vie privée pourrait ainsi, dans une certaine mesure, se négocier[65].

Or, la question de la protection de la vie privée n'est pas une simple affaire privée mais met en jeu des considérations d'ordre social et exige une possibilité d'intervention et un contrôle marginal par les autorités publiques[66].

3.3.2. Les autres bases de légitimité des traitements de données

La Convention ne prévoit pas les hypothèses dans lesquelles les traitements de données sont jugés légitimes. Elle se limite à exiger que les finalités poursuivies soient légitimes mais ne clarifie pas les cas où la légitimité du traitement est reconnue. Les auteurs de la directive 95/46 ont réalisé l'exercice d'envisager *a priori* les cas de traitements admis car légitimes. Ils ont élaboré la liste de ces cas reprise à l'article 7 de la directive, afin de simplifier la vie des utilisateurs de données à caractère personnel et de leur offrir une certaine sécurité juridique. Il s'agit d'hypothèses dans lesquelles la règle de proportionnalité est *a priori*, abstraitement, respectée. Cela n'empêche pas de vérifier concrètement si l'équilibre des intérêts en présence est atteint, au nom de l'exigence de finalité légitime contenue à l'article 6, b. de la directive (l'équivalent de l'article 5, b. de la Convention 108).

Est-il nécessaire d'introduire dans la Convention une liste des hypothèses dans lesquelles les traitements de données sont considérés comme légitimes ?

3.4. LES TRAITEMENTS « INCOMPATIBLES »

Le principe de **« compatibilité »** des opérations effectuées sur les données exige que toute utilisation des données soit compatible avec la finalité pour laquelle les données ont été enregistrées. On s'accorde pour estimer que l'exigence de compatibilité implique que ce qui est fait avec les données ne heurte pas les prévisions raisonnables de la personne concernée.

---

64 Outre l'opinion émise par le Groupe de l'article 29 (Opinion 11/98 à propos de la Platform for Privacy Preferences (P3P) et des Open Profiling Standards (OPS), opinion disponible à http://europa.eu.int/comm/dg15/fr/media/dataprot/wpdoes/wp11.fr.pdf), lire sur ce protocole, J. CATLETT, « Technical Standards and Privacy : An open Letter to P3P Developers », disponible à l'adresse : *http://www.junkblusters.com/standards.html*.

65 Sur la contractualisation du traitement des données ainsi opérée par la technologie, lire P.M. SCHWARTZ, « Beyond Lessig's Code for Internet Privacy : Cyberespace, Filters, Privacy control and Fair Information Practices », *Wisconsin Law Review*, 2000, pp. 749 et s. ; M. ROTENBERG, « What Larry doesn't Get the Truth », *Stan. Techn. L. Rev.*, 2001, 1, disponible sur le site : http://www.sth.Stanford .edu/STLR/Articles/01_STLR_1 .

66 A ce propos, les réflexions de SCHWARTZ, article cité note précédente.

L'APEC Privacy Framework apporte la précision suivante à propos de la notion d'utilisation compatible : « The fundamental criterion in determining whether a purpose is compatible with or related to the stated purposes is whether the extended usage stems from or is in furtherance of such purposes. The use of personal information for "compatible or related purposes" would extend, for example, to matters such as the creation and use of a centralized database to manage personnel in an effective and efficient manner; the processing of employee payrolls by a third party; or, the use of information collected by an organization for the purpose of granting credit for the subsequent purpose of collecting debt owed to that organization. »[67]

L'accélération du progrès technologique, les potentialités infinies de traitements nouveaux offertes par les logiciels et les données disponibles sur le réseau justifient la nécessité de s'interroger sur cette question de la régulation des utilisations et traitements ultérieurs et de leur compatibilité avec les finalités initiales d'enregistrement et sur les moyens de faire respecter le principe d'interdiction de traitements incompatibles.

Ainsi, les RFID conçus au départ par les entreprises de biens de consommation comme un outil de lutte contre les vols dans les grands magasins sont devenues un outil puissant d'analyse des comportements des consommateurs, leur profilage etc. La mise à disposition par un auteur scientifique de son curriculum vitae et de ses publications aux fins de faire connaître son œuvre peut servir à le classer politiquement ou philosophiquement. La publication des décisions jurisprudentielles dans de vastes bases de données a un but scientifique et aide à faire connaître le droit. La possibilité de recherche par le nom des parties ou le type d'affaires peut permettre de créer des listes noires (ainsi, la liste des employés ayant intenté un recours contre leurs employeurs ou ayant été licenciés par eux).

La régulation qui pourrait être proposée doit tenir compte de l'intérêt que peuvent présenter les traitements ultérieurs[68]. Sans doute dans toute la mesure du possible, le codage voire l'anonymisation des données devrait être requis (principe de minimisation des données, voy. *infra*) ou le consentement devrait-il être demandé. A défaut, on devrait pouvoir admettre que le maître du fichier qui souhaite lancer un traitement ultérieur soit tenu de motiver soigneusement au regard de la balance d'intérêts la légitimité d'y procéder et tenu d'en informer les personnes concernées au moins collectivement.

Le régime que l'APEC Privacy Framework réserve aux utilisations ultérieures des données non compatibles avec les finalités de la collecte est le suivant : ces utilisations incompatibles sont en principe exclues à l'exception des cas où l'on a le consentement des individus dont les données ont été collectées, des cas où cela est nécessaire pour fournir un service ou un produit demandé par l'individu, et des cas couverts par une loi ou tout autre instrument légal.[69]

La Résolution de Madrid, quant à elle, ne retient que l' « unambiguous consent » comme situation dans laquelle on peut effectuer un traitement de données non compatible avec les finalités pour lesquelles ces données ont été collectées.[70]

Quant aux solutions techniques, on peut, par exemple dans le cadre des moteurs de recherche, songer à donner à l'usager du réseau, les moyens de définir lui-même ce qu'il entend par finalités « compatibles ». Ainsi, les systèmes techniques « no-robot » apposés sur des pages web interdisent

---

[67] Principle IV. Uses of Personal Information, § 19.

[68] Ainsi une base de données de soins de santé peut ayant servi à une première finalité thérapeutique être utilisée par la suite à des finalités de recherche scientifique, une banque peut proposer à un moment donné un service nouveau à ses clients fondé sur une exploitation plus performante des données relatives à ses clients.

[69] Principle IV Uses of Personal Information, § 19.

[70] Article 7, § 2.

leur prise en compte par les engins de recherche. Autre exemple de solutions techniques : à propos de l'utilisation marketing des données collectées sur le net, des infomédiaires proposent leurs services pour sélectionner les utilisations possibles des données des internautes à des fins de marketing, etc.

3.5. PRINCIPE DE MINIMISATION DES DONNEES

Par l'exigence qu'elle contient de limiter le traitement des données aux seules données adéquates, pertinentes et non excessives, la Convention 108 oblige à réduire la collecte de données à caractère personnel. On peut voir dans cette exigence une facette du principe de minimisation des données. Mais celui-ci va plus loin. Il invite en effet à minimiser (c.à.d. limiter au strict minimum) ou éliminer la collecte d'informations à caractère personnel dès que cela est possible.

C'est surtout par le biais du recours à des techniques d'anonymisation ou de pseudonymisation ou par des techniques favorables à la vie privée (*Privacy Enhancing Technologies* – PET) qu'on envisage la mise en œuvre de ce principe de minimisation. Mais, outre les limites que de telles techniques ont démontrées[71], on peut très efficacement honorer ce principe en recourant à des solutions à caractère relativement peu technologique. Ainsi, on peut exiger que les paramètres par défaut de diverses applications renforcent la protection de la vie privée au niveau des quantités de données personnelles traitées, plutôt que ne la fragilise. Cela peut conduire à ce que, par défaut, un navigateur limite au maximum les informations qui sont envoyées aux sites web dans le sillage des visites effectuées par un utilisateur, ou un réseau social ne rende pas les informations qu'il contient visibles du monde entier, par exemple.

L'ensemble des autorités nationales de protection des données des Etats membres de l'Union européenne ont demandé que cet aspect du principe de minimisation soit désormais consacré dans la législation[72]. Le Contrôleur européen à la Protection des Données a fait de même[73]. La Commission européenne a pour sa part adopté des actions pour promouvoir les technologies renforçant la vie privée (PETs) qui permettent de réduire le traitement de données à caractère personnel[74].

La résolution de Madrid a, quant à elle, rattaché au principe de proportionnalité l'exigence de limiter au minimum nécessaire les données faisant l'objet d'un traitement[75]

---

71 « Les autres moyens de renforcer la protection des données, et notamment les moyens techniques tels que le cryptage, l'anonymisation, les outils de gestion des identités et autres technologies renforçant (soi-disant) la protection de la vie privée (PET), sont encore très peu développés, souvent peu mis en application et peu efficaces, et trop souvent appliqués d'une façon inappropriée qui les rend inefficaces. Certains d'entre eux ne sont rien de plus que des cache-misère. D'autres (comme l'anonymisation) sont de plus en plus contournées par les avancées technologiques. Et souvent, ils ne résolvent pas les problèmes au bon moment, en particulier au moment de la conception, ou ne sont pas conviviaux. Dans le nouvel environnement technique, nous devrons accorder davantage d'attention à ces mesures et poser sur elles un regard plus critique. » (*Etude comparative sur les différentes approches des nouveaux défis en matière de protection de la vie privée, en particulier à la lumière des évolutions technologiques*, précitée, p. 19)

72 Groupe de l'article 29, Avis 2/2008 sur la révision de la directive 2002/58 concernant la protection de la vie privée dans le secteur des communications électroniques, WP 150, 15 mai 2008 ; Article 29 Working Party and Working Party on Police and Justice, WP 168, The Future of Privacy – Joint contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data, adopted on 1 December 2009, §53.

73 EDPS Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, 18 March 2010. Notamment: "the EDPS recommends the Commission to […] propose to include a general provision on Privacy by Design in the legal framework for data protection." (point 38)

74 Communication de la Commission européenne sur les technologies renforçant la protection de la vie privée, 2 mai 2007, COM(2007)228 final.

75 Madrid Resolution, Article 8, § 2 : « In particular, the responsible person should make reasonable efforts to limit the processed personal data to the minimum necessary »

4. Données sensibles

L'identification de catégories particulières de données auxquelles on réserve une protection plus élevée est liée aux risques accrus de porter préjudice aux individus sur la base du traitement de ces données. C'est principalement le risque de discriminations illégitimes ou arbitraires qui est lié à ces données. Les Principes directeurs de l'ONU pour la réglementation des fichiers informatisés contenant des données à caractère personnel[76] mettent d'ailleurs bien en évidence ce risque. Ils contiennent en effet une disposition consacrée aux données sensibles qu'ils ont intitulée « Principe de non-discrimination »[77]. La résolution de Madrid indique elle aussi très clairement le lien entre le régime spécial accordé aux données sensibles et le risque de discrimination illégitime. Ce texte ajoute cependant le risque de telles données d'affecter la sphère la plus intime des sujets de données, ainsi que, tout simplement, le risque sérieux que ces données présentent, en cas d'abus, pour la personne concernée[78].

La définition des données sensibles présentée à l'article 6 de la Convention est extrêmement large du fait qu'elle qualifie comme telles les données « *révélant* l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions,… » (c'est nous qui soulignons). Cela signifie que tombent dans cette catégorie, par exemple, les noms patronymiques qui révèlent indubitablement l'origine raciale, de même que toute photo d'une personne ; l'achat d'un ouvrage sur le Coran sur un site web peut quant à lui révéler les convictions religieuses, etc. Or, il est inconcevable de traiter systématiquement les noms, les photographies et certains achats comme des données sensibles bénéficiant d'un régime de protection particulièrement sévère. Ce ne sera que quand c'est justement l'élément sensible de la donnée qui est retenu par le responsable du traitement (sélection des personnes d'origine africaine ou arabe ou juive ou japonaise, sur la base de leurs noms ; ou sélection des personnes de type tutsi ou rom ou aborigène sur la base de leurs photos) que le régime protecteur, principalement justifié par le risque élevé de discrimination à partir des données traitées, se justifie.

D'une part, il est louable de retenir les données « révélant » des caractéristiques sensibles des personnes. Cela permet en effet de considérer comme sensible des cas dans lesquels n'apparaît aucune donnée *a priori* sensible. Ainsi, les recherches sur Google de sites de voyage à Rome pratiquées par un internaute, son achat de livres religieux, sa lecture d'une encyclique pontificale, etc. pourraient être traitées comme révélant une opinion religieuse.

D'autre part, **retenir justement tout ce qui révèle une caractéristique sensible en arrive à faire entrer dans cette catégorie de données énormément de données qui dans bien des cas ne sont pas traitées pour l'aspect sensible qu'elles véhiculent**. Cela est excessif et risque d'ôter son sens à la notion de données sensibles au niveau de l'application concrète. Une solution serait peut-être de revoir la définition en apportant la nuance suivante : seraient retenues comme données sensibles « les données à caractère personnel traitées pour l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions qu'elles révèlent, … ».

---

76 Résolution 45/95 de l'Assemblée générale des Nations Unies du 14 décembre 1990.

77 Article 5, Principe de non-discrimination : Sous réserve des cas de dérogations limitativement prévus sous le principe 6, les données pouvant engendrer une discrimination illégitime ou arbitraire, notamment les informations sur l'origine raciale ou ethnique, la couleur, la vie sexuelle, les opinions politiques, les convictions religieuses, philosophiques ou autres, ainsi que l'appartenance à une association ou un syndicat, ne devraient pas être collectées.

78 Avant de présenter une liste non exhaustive de données considérées comme sensibles, l'article 13, § 1, de la Résolution de Madrid indique « The following personal data shall be deemed to be sensitive : a. Data which affect the data subject's most intimate sphere ; or b. Data likely to give rise, in case of misuse, to : i Unlawful or arbitrary discrimination ; or ii A serious risk to the data subject ».

Il convient de s'interroger sur la pertinence d'ajouter deux catégories particulières de données à la liste des données sensibles au vu des risques nouveaux suscités par le développement technologique :

- les « numéros d'identification » (avec ou sans lien avec l'identité au sens étroit) qui permettent de coupler de multiples bases de données ou données et se généralisent tant dans le secteur tant privé que public ;

- les données biologiques ou biométriques. La Cour européenne des droits de l'homme a exposé clairement en quoi ces données soulevaient une préoccupation particulière au regard de la protection de la vie privée. Elle a ainsi estimé[79] que, vu les usages futurs que l'on pouvait envisager pour les échantillons cellulaires, la conservation systématique de pareils éléments était suffisamment intrusive pour entraîner une atteinte au droit au respect de la vie privée. En outre, « En dehors de leur caractère éminemment personnel, la Cour note que les échantillons cellulaires contiennent beaucoup d'informations sensibles sur un individu, notamment sur sa santé. De surcroît, les échantillons renferment un code génétique unique qui revêt une grande importance tant pour la personne concernée que pour les membres de sa famille »[80]. Quant aux profils ADN, pour la Cour[81], ils contiennent une quantité importante de données à caractère personnel uniques qui, même si objectives et irréfutables, permettent aux autorités d'aller bien au-delà d'une identification neutre (les profils ADN peuvent notamment être utilisés pour effectuer des recherches familiales en vue de découvrir les relations génétiques pouvant exister entre des individus). Concernant les empreintes digitales (on pourrait vraisemblablement étendre ce raisonnement aux autres identifiants physiques tels l'iris, la silhouette, etc.), la Cour a également relevé[82] que « Chacun admet que, de par les informations que les échantillons cellulaires et profils ADN contiennent, la conservation de ces éléments a un impact plus grand sur la vie privée que celle d'empreintes digitales. […] Toutefois, les empreintes digitales contiennent des informations uniques sur l'individu concerné et leur conservation sans le consentement de celui-ci ne saurait passer pour une mesure neutre ou banale. Dès lors, la conservation d'empreintes digitales peut en soi donner lieu à des préoccupations importantes concernant le respect de la vie privée et constitue donc une atteinte au droit au respect de la vie privée. »

Dans son analyse réalisée pour le Conseil de l'Europe en 1999, S. Simitis estimait déjà que les données génétiques méritaient de figurer dans la liste des données sensibles. Il signale ainsi : « Rien n'illustre mieux la nécessité de mettre à jour les listes que les données génétiques. On n'en parlait pratiquement pas lorsque les premières listes ont été établies. Mais aujourd'hui, il n'y a aucun doute qu'aucune autre catégorie de données ne donne d'informations aussi complètes sur les personnes concernées. Les risques du traitement de données à caractère personnel n'avaient donc jamais été aussi évidents auparavant. Qu'il s'agisse de la possibilité de trouver un emploi, des chances d'obtenir une assurance maladie ou des limites de la marchandisation croissante des individus, l'accessibilité des données génétiques détermine la réponse. Aucune liste de données sensibles ne peut donc négliger les données génétiques sans que l'on s'interroge sur son sérieux. »[83]

---

79 Cour eur. D.H., *Van der Velden c. Pays-Bas*, déc. du 7 décembre 2006, req. n° 29514/05

80 Cour eur. D.H., *S. et Marper c. Royaume-Uni*, précité, par. 72.

81 Cour eur. D.H., *S. et Marper c. Royaume-Uni*, précité, par. 75.

82 Cour eur. D.H., *S. et Marper c. Royaume-Uni*, précité, par. 86

83 S. Simitis, « Les données sensibles revisitées (1999) », Examen des réponses au questionnaire du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE 108), Strasbourg, 24-26 novembre 1999.

5. Sécurité

5.1. OBLIGATIONS DE SECURITE

L'article 7 de la Convention envisage la sécurité dans un sens très limité : essentiellement la destruction des données et l'atteinte à la confidentialité. Il serait utile que la sécurité porte sur les 3 aspects de la sécurité au sens large « intégrité, disponibilité et confidentialité » et que soient repris les 9 principes directeurs de l'OCDE pour la sécurité des systèmes d'information établis en 1992 (principes de responsabilité, de sensibilisation, d'éthique, de multidisciplinarité, de proportionnalité, d'intégration, d'adaptation, de réévaluation, de démocratie).

Par ailleurs, l'absence de sécurité du réseau et la multiplication des agissements illicites possibles rendent nécessaires l'obligation des fournisseurs de services de communications électroniques de prévenir les utilisateurs du réseau, des risques liés à l'utilisation de leur service.

Enfin, on insistera sur l'importance de l'autorégulation en la matière : développement de normes en la matière ; méthodes d'audit ; systèmes d'agrément de S.I., etc. La sécurité organisationnelle et technique des systèmes d'information doit devenir partie intégrante de la politique de protection des données.

L**es mesures de sécurité doivent non seulement empêcher les accès non autorisés mais également permettre aux personnes concernées de contrôler les accès aux données** qui ont eu lieu. Seul cet accès aux données sur les personnes ayant accédé aux données permet en effet à la personne concernée de vérifier l'effectivité des mesures de sécurité et lui permet d'exercer son contrôle ou sa maîtrise sur ses propres informations. C'est en ce sens qu'a jugé la Cour européenne des droits de l'homme dans l'affaire *I c. Finlande*, condamnant cet Etat pour avoir laissé un hôpital public mettre en place un système de sécurité des données qui ne conserve en mémoire que les traces des cinq derniers accès aux données et qui, de surcroît efface toute trace d'accès une fois les données versées aux archives[84].

La Cour de Justice des Communautés européennes a, pour sa part, signalé dans son arrêt *Rijkeboer*[85] que la protection des données implique que la personne concernée puisse s'assurer que ses données à caractère personnel sont adressées à des destinataires autorisés. Afin de pouvoir effectuer les vérifications nécessaires, la personne concernée doit disposer d'un droit d'accès à l'information sur les destinataires ou les catégories de destinataires des données ainsi qu'au contenu de l'information communiquée non seulement pour le présent, mais aussi pour le passé. Cela implique l'obligation de conservation pendant une certaine durée des renseignements relatifs aux personnes destinataires des données ainsi qu'aux données précisément consultées ou transmises.

La Cour de Strasbourg a, dans le cours de son argumentation dans l'arrêt *I c. Finlande*, mis en exergue que la confidentialité de certaines données (par exemple les données médicales) présentant une importance plus grande pour les individus concernés imposait dans ces cas des mesures plus strictes. **L'exigence de sécurité est en effet modalisable en fonction de la nature des données, des**

84 " […] the impugned health records system was such that it was not possible to retroactively clarify the use of patient records as it revealed only the five most recent consultations and that this information was deleted once the file had been returned to the archives. Therefore, the County Administrative Board could not determine whether information contained in the patient records of the applicant and her family had been given to or accessed by an unauthorised third person" (Cour eur. D.H., *I. v. Finlande*, 17 July 2008, appl. n° 20511/03, par. 41)

85 C.J.C.E., 7 mai 2009, (Rijkeboer), aff. C-553/07.

circonstances qui entourent leur traitement et des risques que celui-ci fait courir aux personnes concernées. Dans la même ligne, la directive 2002/58 sur la protection de la vie privée dans les communications électroniques dispose, dans son article 4 consacré à la sécurité du traitement : « […] Compte tenu des possibilités techniques les plus récentes et du coût de leur mise en œuvre, ces mesures garantissent un degré de sécurité adapté au risque existant. »

L'APEC Privacy Framework indique de même une possibilité de nuancer le degré d'exigence de sécurité. Son Principe VII *Security Safeguards* stipule : "22. Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. *Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment*." (c'est nous qui soulignons). La Résolution de Madrid a adopté la même modulation des exigences de sécurité : « These measures depend on the existing risk, the possible consequences to data subjects, the sensitive nature of the personal data, the state of the art, the context in which the processing is carried out, and where appropriate the obligations contained in the applicable national legislation. » (Article 20, § 1, *in fine*)

5.2. CONFIDENTIALITE

La question de la confidentialité des données s'inscrit traditionnellement dans celle de la sécurité.

Les communications électroniques empruntant désormais la forme de traitements de données (relatives aux personnes impliquées dans la communication), **l'obligation de garantir la confidentialité des données converge avec l'exigence de confidentialité des communications.** Cette convergence d'exigences de confidentialité se comprend donc par le fait que désormais la technologie interactive du réseau permet à la personne utilisatrice de cette technologie de communiquer avec les autres personnes connectées au réseau, et ce pour des finalités personnelles.

L'obligation de confidentialité doit porter tant sur le contenu des communications que sur les données techniques accompagnant les communications, données de trafic et données de localisation.[86] Ces données attestent de l'existence ou de la tentative d'établissement des communications, indiquent l'émetteur et le destinataire, la date et l'heure, la taille des données transmises, la nature d'éventuels fichiers joints, la position géographique des utilisateurs, etc.

La confidentialité des données de communication doit toutefois se voir imposer des limites. La Cour européenne des droits de l'homme a mis au jour l'obligation pour les législateurs de prévoir un cadre législatif permettant de concilier la confidentialité des services Internet avec la défense de l'ordre, la prévention des infractions pénales et la protection des droits et libertés d'autrui. Dans l'affaire tranchée par la Cour[87], une annonce à caractère sexuel avait été publiée au sujet d'un jeune garçon sur un site de rencontres par Internet. Or, la législation finlandaise de protection de la confidentialité des communications en vigueur à l'époque n'avait pas permis à la police et aux tribunaux d'obliger le fournisseur d'accès à identifier l'auteur de l'annonce. La Cour a conclu à la violation de l'article 8 CEDH dans la mesure où le respect de la confidentialité l'a emporté sur le bien-être physique et moral de l'enfant, la Finlande manquant ainsi à protéger le droit de l'intéressé au respect de sa vie privée.

---

86 Voy. Directive 2002/58, art. 5, paragraphe 1er. Dans le même sens voy. Cour eur. D.H., *Copland c. Royaume-Uni*, arrêt du 3 avril 2007, § 44

87 Cour eur. DH, *K.U. c. Finlande*, arrêt du 2 décembre 2008

5.3. VIOLATIONS DE LA SECURITE/COMPROMISSIONS DES DONNEES

La Madrid Privacy Declaration, déclaration de la société civile adoptée le 3 novembre 2009 visant à l'établissement de « Standards mondiaux de respect de la vie privée dans un monde globalisé **»** incite notamment les États « (7) à **assurer que les citoyens sont rapidement avisés lorsque leurs informations personnelles sont abusivement divulguées ou utilisées de manière incompatible avec les finalités de leur collecte** ».

Il s'agit ainsi d'aviser les personnes concernées lorsqu'un tiers non autorisé, un pirate par exemple, a accédé à des données à caractère personnel en s'introduisant illégalement dans un serveur. Entrent également dans le champ de cette obligation des situations dans lesquelles les données à caractère personnel ont été perdues (par exemple, sur des CD-Rom, des clés USB ou d'autres appareils portatifs), ou communiquées par inadvertance ou malveillance par un utilisateur autorisé, en violation du principe de finalité ou de son devoir de confidentialité (par exemple, un fichier de données bancaires transmis aux autorités fiscales d'un pays tiers par un employé licencié, à titre de vengeance ; la publication accidentelle sur un site internet de la liste des personnes affiliées à un parti politique ; l'envoi par une société pharmaceutique d'un mail d'alerte à propos d'un médicament laissant apparaître le nom et les coordonnées de toutes les personnes consommant ce médicament,…).

Les avantages liés à une telle obligation d'informer sur les violations de la sécurité et compromissions des données sont importants sur le plan de la protection des données : « Les notifications des violations de la sécurité peuvent aider les personnes à prendre les mesures qui s'imposent pour réduire les dommages susceptibles de résulter d'une telle compromission. En outre, l'obligation de notifier les violations de la sécurité incitera les sociétés à améliorer la sécurité des données et les rendra davantage comptables des données à caractère personnel dont elles sont responsables. »[88]

Venue des Etats-Unis où une grande majorité des Etats ont adopté une législation à ce propos, cette préoccupation relative aux *privacy breaches* a désormais reçu un écho dans la législation communautaire européenne. Ainsi, la directive 2002/58 sur la protection de la vie privée dans les communications électroniques a été amendée par la Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 en vue notamment d'y introduire une disposition spécifique aux «violation de données à caractère personnel»[89]. Désormais, les fournisseurs de service de communications électroniques accessibles au public ont l'obligation de signaler aux abonnés ou aux particuliers les atteintes subies par leurs données[90].

---

88 Deuxième avis du contrôleur européen de la protection des données relatif au réexamen de 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 (directive «vie privée et communications électroniques»), *J.O.U.E.*, 6 juin 2009, C 128/28, par. 10.

89 Par violation de données à caractère personnel on entend (article 2, i. de la directive 2002/58 telle qu'amendée) : « une violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés de données à caractère personnel transmises, stockées ou traitées d'une autre manière en relation avec la fourniture de services de communications électroniques accessibles au public dans la Communauté. »

90 Article 4, § 3. de la directive 2002/58 telle qu'amendée : « En cas de violation de données à caractère personnel, le fournisseur de services de communications électroniques accessibles au public avertit sans retard indu l'autorité nationale compétente de la violation.

Lorsque la violation de données à caractère personnel est de nature à affecter négativement les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier, le fournisseur avertit également sans retard indu l'abonné ou le particulier concerné de la violation.

La notification d'une violation des données à caractère personnel à l'abonné ou au particulier concerné n'est pas nécessaire si le fournisseur a prouvé, à la satisfaction de l'autorité compétente, qu'il a mis en œuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données

Cette limitation de l'obligation d'informer les personnes des violations de sécurité aux seuls fournisseurs de service de communications électroniques accessibles au public (soit les sociétés de télécommunications et les fournisseurs d'accès internet) a été critiquée. Il a été demandé tant par le Contrôleur européen à la protection des données[91] que par le Groupe de l'article 29 d'étendre aux fournisseurs de services de la société de l'information la portée de l'obligation de notifier les violations de sécurité (les exemples cités ci-dessus illustrent la pertinence d'un tel élargissement). Cette obligation devrait donc idéalement s'adresser aux banques en ligne, aux entreprises qui ont développé des activités sur le réseau, aux prestataires de services de soins de santé en ligne, etc. Pour ces autorités, « élargir la portée de l'obligation aux prestataires de services de la société de l'information en général augmenterait leur responsabilité et contribuerait à sensibiliser le public. Cela permettrait incontestablement de réduire les risques en matière de sécurité. »[92]

La limitation des destinataires des notifications de violations de la sécurité aux abonnés a de même été critiquée. C'est en effet toute personne concernée par une compromission de ses données à la suite d'une violation de la sécurité qui devrait bénéficier de l'information de cette compromission.

La Résolution de Madrid fait figurer dans sa disposition sur les Mesures de sécurité (article 20), un devoir d'information des sujets de données, à charge des personnes impliquées à tous les stades du traitement des données, de toute atteinte à la sécurité qui pourrait affecter significativement les droits financiers et non financiers des individus. Les personnes concernées doivent aussi être informées des mesures prise pour résoudre l'atteinte.

L'OCDE, à l'occasion de l'adoption de ses *Orientations pour les politiques concernant les questions émergentes de protection et autonomisation des consommateurs dans le commerce mobile*[93], a estimé que dans le cadre du développement du commerce mobile, il serait nécessaire d'introduire des mesures additionnelles de protection à côté de celles contenues dans les Lignes directrices sur la vie privée de 1980 et celles de 2002 régissant la sécurité des systèmes et réseaux de l'information. Au rang de ces mesures figure l'invitation adressée aux opérateurs mobiles de mettre en place des politiques et mesures de sécurisation des données destinées à prévenir les transactions non autorisées et les compromissions de données, et de proposer aux consommateurs des moyens rapides et efficaces de recours quand leurs données sont compromises et/ou qu'ils subissent un préjudice financier.

---

concernées par ladite violation. De telles mesures de protection technologiques rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès.

Sans préjudice de l'obligation du fournisseur d'informer les abonnés et les particuliers concernés, si le fournisseur n'a pas déjà averti l'abonné ou le particulier de la violation de données à caractère personnel, l'autorité nationale compétente peut, après avoir examiné les effets éventuellement négatifs de cette violation, exiger du fournisseur qu'il s'exécute.

La notification faite à l'abonné ou au particulier décrit au minimum la nature de la violation de données à caractère personnel et les points de contact auprès desquels des informations supplémentaires peuvent être obtenues et recommande des mesures à prendre pour atténuer les conséquences négatives possibles de la violation de données à caractère personnel. La notification faite à l'autorité nationale compétente décrit en outre les conséquences de la violation de données à caractère personnel, et les mesures proposées ou prises par le fournisseur pour y remédier. »

91 Deuxième avis du contrôleur européen de la protection des données relatif au réexamen de la directive 2002/58/CE, précité, par. 22 et s.

92 Groupe de l'article 29, WP 150, avis 2/2008 sur la révision de la directive 2002/58/CE concernant la protection de la vie privée dans le secteur des communications électroniques (« directive vie privée et communications électroniques »), 15 mai 2008.

93 OCDE, Séoul, juin 2008.

Les Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information[94] ont instauré un **principe de réaction**, stipulant que « les Parties prenantes doivent agir avec promptitude et dans un esprit de coopération pour prévenir, détecter et répondre aux incidents de sécurité. ». L'interconnectivité des systèmes et des réseaux d'information accentue la propension des dommages à se répandre rapidement et massivement, à la suite d'un incident de sécurité. C'est à ce risque accru que répond le *principe de réaction*.

6. Garanties complémentaires pour la personne concernée

6.1. OBLIGATION DE TRANSPARENCE/D'INFORMATION

La Convention prévoit à son article 8 des « garanties complémentaires pour la personne concernée ». Ces garanties sont appelées, dans les lois nationales, à correspondre à des droits subjectifs. La Convention ne formule aucune obligation spécifique pour les maitres du fichier si ce n'est celles de répondre et donner effet aux droits des personnes concernées.

Or, le système de protection ne s'accommode plus de garanties qui reposent essentiellement sur la seule initiative de la personne concernée. Il est impératif, vu l'environnement particulièrement opaque des systèmes d'information actuels, de mettre à charge des responsables de traitement des obligations de transparence active. La personne concernée ne peut s'intéresser à et s'informer sur un traitement dont elle ne soupçonne pas l'existence. Combien de personnes concernées « standard » songeront que les mots introduits dans un moteur de recherche sont enregistrés pendant des mois et reliés à un pointeur identifiant[95] ? Ou que des caméras les filment alors qu'elles sont miniaturisées et, vu leur puissance, posées à bonne distance ? Ou que leur entreprise conserve toutes les traces d'utilisation de clés/cartes magnétiques pour contrôler leurs déplacements ? Ou que le portique qu'elles franchissent lit la puce RFID qui se trouve dans leur passeport ? Les exemples de telles situations où les personnes concernées ne se doutent pas, tant qu'on ne les en a pas informées, que leurs données sont traitées, sont malheureusement multipliables à l'envi aujourd'hui. **Il importe donc que soit clairement énoncée[96] une obligation d'information des personnes sur lesquelles on traite des données, à mettre à charge des personnes qui effectuent ce traitement**.

La Déclaration de Madrid d'ailleurs inscrit expressément dans le régime protecteur universel qu'elle vise à voir établir, un ensemble d'obligations à mettre à charge de ceux qui collectent des données. La société civile, à travers les signataires de la Déclaration, affirme ainsi « (1) Réaffirmer son adhésion à un cadre mondial pour des pratiques loyales de traitement des données, *imposant des obligations*

---

94 Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité, 25 juillet 2002.

95 Voy. *supra*, la notion de donnée à caractère personnel.

96 On pourrait estimer que l'obligation d'information se trouve en filigrane de l'article 8, *littera* a, la latitude étant laissée aux Etats de donner forme à l'obligation contenue dans cette disposition qui exige que « Toute personne doit pouvoir connaître l'existence d'un fichier automatisé de données à caractère personnel, ses finalités principales, ainsi que l'identité et la résidence habituelle ou le principal établissement du maître du fichier ». Le Rapport explicatif énonce en effet que le libellé de l'alinéa tient compte de la variété des règles de droit interne donnant effet au principe qui y est inscrit. Ainsi, « dans certains Etats, le nom du maître du fichier est inscrit dans un répertoire public. Dans d'autres Etats n'ayant pas un tel système de publicité, la loi pourra prévoir que le nom du maître du fichier sera communiqué à la personne qui le demandera. » (p. 19). Outre le fait que l'hypothèse d'un devoir d'information systématique (et non via une déclaration inscrite dans un registre public) n'est pas citée dans les exemples de mise en œuvre du principe contenu à l'alinéa a., la formulation de ce principe n'est assurément pas suffisamment indicative d'un devoir de transparence spontané qui est pourtant indispensable dans la réalité technique actuelle.

à ceux qui collectent et traitent des informations personnelles et donnant des droits à ceux dont les informations personnelles sont recueillies ».[97]

Le dernier instrument juridique adopté pour l'heure à un niveau international/régional, l'APEC Privacy Framework prévoit une telle obligation d'information à charge des *personal information controllers*, il s'agit du *Principle of Notice*.[98] Le commentaire de ce principe l'éclaire de la sorte: « 15-17. The Notice Principle is directed towards ensuring that individuals are able to know what information is collected about them and for what purpose it is to be used. By providing notice, personal information controllers may enable an individual to make a more informed decision about interacting with the organization. One common method of compliance with this Principle is for personal information controllers to post notices on their Web sites. In other situations, placement of notices on intranet sites or in employee handbooks, for example, may be appropriate."

La Résolution de Madrid prévoit, elle, un « Openness Principle » (Article 10). Ce principe correspond à un devoir d'information dans le chef du responsable du traitement qui est particulièrement détaillé.

Il s'agit par ailleurs de proposer une amélioration de la situation des personnes concernées afin de leur assurer la possibilité d'une « autodétermination informationnelle » au moment où cette maîtrise tend à diminuer au vu de la double opacité à la fois du fonctionnement des terminaux et du réseau. La reconnaissance de droits nouveaux est l'indispensable corollaire de la perte de contrôle par les utilisateurs des systèmes d'information de leur maîtrise de l'environnement informationnel.

6.2. DROIT D'ACCES

Le droit d'accès qui est prévu par la Convention pourrait être enrichi à plusieurs points de vue.

Tout d'abord, **l'accès des personnes concernées pourrait, au-delà de la communication des données elles-mêmes, couvrir aussi l'accès à l'origine des données**[99]. Cette information est en effet cruciale car c'est souvent la source des données qui intrigue et interpelle les personnes concernées (comment ont-ils obtenu ces informations, qui les leur a communiquées ?). Par ailleurs, les renseignements sur l'origine des données permettent de vérifier la licéité de la communication ou de la collecte de celles-ci et éventuellement d'introduire un recours à l'encontre du premier détenteur des données (ce qui permet « d'arrêter l'hémorragie » si celui-ci diffuse illicitement les données en question). Enfin, en cas de problèmes liés à la qualité des données et de nécessité de correction, il devient possible de faire effectuer ces corrections à la source, ce qui évite la propagation ultérieure d'erreurs.

Le droit d'accès pourrait aussi être enrichi par le **droit pour chacun d'accéder à la logique** qui sous-tend tout traitement automatisé de données le concernant (v. ci-dessous point 6.5).

Ensuite, il faudrait garantir que la personne concernée puisse bénéficier des mêmes facilités techniques pour exercer ses droits (ici droit d'accès mais aussi de correction et d'opposition) que celles dont jouissent les responsables de traitement[100]. Il s'agit donc de lui permettre de s'adresser

---

97 Déclaration de Madrid, précitée (c'est nous qui soulignons).

98 Principle II Notice.

99 Un tel droit d'accès est garanti par la directive 95/46, à l'article 12 : « Les États membres garantissent à toute personne concernée le droit d'obtenir du responsable du traitement: a) sans contrainte, à des intervalles raisonnables et sans délais ou frais excessifs: […] la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine des données […]. » Il est aussi prévu dans la Résolution de Madrid (Article 16, § 1)

100 Y. POULLET, « Pour une troisième génération de réglementation de protection des données », in *Défis du droit à la protection de la vie privée*, *Perspectives du droit européen et nord-américain – Challenges of*

au responsable du traitement par la voie du réseau si le traitement a lieu sur Internet. C'est le **droit à la réciprocité des avantages**, qui oblige celui qui utilise des technologies à mettre à disposition de l'internaute des moyens électroniques pour faire valoir ses intérêts ou ses droits qui peuvent être mis à mal par l'utilisation de ces moyens électroniques.

Il faudrait de même, pour faciliter l'exercice du droit d'accès (ainsi que des autres droits), que l'on **permette de réutiliser les données identifiantes** utilisées par le responsable du traitement (en certains cas même non nominatives) pour exercer son droit, plutôt que d'exiger que l'on s'identifie, en présentant la preuve de son identité. En effet, l'identité ainsi attestée ne correspondra dans bien des cas pas aux données identifiantes conservées (un cookie par exemple, qui n'a pas besoin d'aller jusqu'à identifier civilement une personne concernée mais réalise pour autant l'individualisation nécessaire).

6.3. DROIT D'OPPOSITION

A l'instar des autres instruments internationaux (Lignes directrices de l'OCDE, Principes directeurs de l'ONU[101] et APEC Privacy Framework), **la Convention n'a pas prévu de droit d'opposition pour la personne concernée**. La directive européenne 95/46 cependant a dès 1995 inscrit ce droit au tableau des droits subjectifs destinés à permettre aux individus d'exercer une maitrise sur le sort réservé à leurs données, de mettre en œuvre leur autodétermination informationnelle. La directive 2002/58 vie privée et communications électroniques a, elle aussi, repris ce droit sous différentes formes (v. ci-dessous). La Résolution de Madrid, enfin, fait également figurer ce droit dans le catalogue de droits du sujet de données.

Ce droit se justifie lorsque le traitement des données ne repose pas sur le consentement des personnes concernées. Celles-ci, qui n'ont pu exprimer leur point de vue à l'entame du traitement, retrouvent par le biais de ce droit la possibilité de faire valoir leurs arguments auprès du maitre du fichier pour le convaincre de renoncer à traiter leurs données. Ce droit est particulièrement important dans les hypothèses où le responsable a effectué lui-même, *a priori*, la mise en balance des intérêts en présence et a estimé que le résultat était équilibré et qu'il pouvait légitimement traiter les données. Grâce au droit d'opposition, la personne concernée retrouve l'occasion de contester le résultat de la mise en balance, à tout le moins dans son cas.

Il est clair que dans le contexte technologique actuel où les traitements de données à l'insu ou sans recourir au consentement des personnes concernées se développent à foison, il est important de rééquilibrer la situation des intervenants en garantissant un droit aux personnes concernées de se manifester et de refuser les enregistrements et utilisations de leurs données quand elles viennent à en prendre connaissance. Il se peut aussi que les personnes avaient bien été informées des traitements envisagés mais n'ont pris la pleine mesure du sort réservé à leurs données ou des implications que ces traitements pouvaient avoir sur d'autres intérêts qu'après un certain temps. Dans de tels cas également, le droit d'opposition offre une solution opportune.

Ce droit est reconnu par le Groupe de l'article 29 comme faisant partie du noyau dur de la protection des données et est dès lors repris dans la liste des principes de protection qui doivent figurer au menu de tout régime de protection des données qui se veut « adéquat ». Ainsi le document de travail n° 12 consacré à l'élaboration des conditions de reconnaissance de l'adéquation des régimes

---

Privacy and Data Protection Law, *Perspectives of European and North American Law*, M.V. Perez-Asinari et P. Palazzi (ed.), coll. Cahiers du CRID, n° 31, Bruxelles, Bruylant, 2008, pp. 57 et s.

[101] On pourrait voir une certaine forme de droit d'opposition dans le « *droit d'obtenir les* rectifications ou *destructions adéquates en cas d'enregistrements illicites*, *injustifiés* ou inexacts », droit rattaché au *Principe de l'accès par les personnes concernées* (Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel, précités).

de protection des pays tiers à l'Union européenne mentionne dans la liste des conditions minimales pour que soit reconnu un niveau de protection adéquat : « Dans certains cas, [toute personne concernée] doit également pouvoir s'opposer au traitement des données qui la concernent. »[102]

Le droit d'opposition est particulièrement pertinent dans un domaine dans lequel il est massivement recouru à la balance des intérêts pour justifier les traitements de données plutôt qu'au consentement préalable des personnes concernées, le domaine du marketing direct. Ce domaine est d'ailleurs épinglé par le Groupe de l'article 29 comme nécessitant la reconnaissance du droit d'opposition : « Lorsque les données sont transférées à des fins de marketing direct, la personne concernée doit être en mesure de "s'opposer" à ce que les données la concernant soient, à un moment ou à un autre, utilisées à une telle fin. » [103]
Lorsque le marketing prend des formes particulièrement intrusives ou coûteuses pour les consommateurs visés (par la voie d'automates d'appel[104], de fax ou de courriers électroniques), ce n'est plus un droit d'opposition qu'il faudrait garantir (opt-out) mais l'obtention du consentement des consommateurs fichés (opt-in)[105].

Le modèle économique du fonctionnement du Web suscite une réflexion sur la place à accorder au droit d'opposition et l'impact que celui-ci peut avoir. Ce modèle est basé sur une gratuité de façade de la plupart des services offerts, financés par une publicité ciblée nourrie d'immenses quantités de données à caractère personnel recueillies loyalement ou de manière opaque. Le droit d'opposition pourrait permettre à un individu de refuser ce modèle qui conduit au traitement, au croisement, à l'interconnexion de ses données, et de lui préférer un modèle payant qui lui rende la maitrise des informations qu'il communique.

Dans la même ligne mais hors d'un modèle économique basé sur le traitement intensif de données à des fins de marketing direct, l'opposition au traitement de ses données pourrait également conduire à obliger le concepteur d'un service imposant à l'utilisateur le traitement de ses données, de développer une version de son service fonctionnant sans traitement de données à caractère personnel. A titre d'exemple, on peut envisager les cartes électroniques d'usage des moyens de transport public. Celui qui ne souhaite pas laisser les traces de tous ses déplacements entre les mains d'un opérateur, devrait pouvoir s'y opposer, ce qui implique pour l'opérateur en question l'obligation de mettre en place une version « non-identifiante » du service. Cette version devrait être accessible à des conditions qui n'ôtent pas tout intérêt pour ses candidats-utilisateurs. Le cas du billet électronique pour circuler dans le métro à Paris illustre cette hypothèse d'offre conjointe d'un service « identifiant » et d'un service « non identifiant »[106].

Dans un autre domaine que le marketing ou la prospection directe, la règle posée par la directive 2002/58 qui permet à l'utilisateur d'une ligne appelante ou connectée d'empêcher la présentation de l'identification de la ligne appelante ou connectée, constitue une autre illustration du principe d'opposition[107].

---

102 Groupe de l'article 29, WP 12, Transferts de données personnelles vers des pays tiers: Application des articles 25 et 26 de la directive relative à la protection des données, 24 juillet 1998.

103 Groupe de l'article 29, WP 12, Transferts de données personnelles vers des pays tiers: Application des articles 25 et 26 de la directive relative à la protection des données, 24 juillet 1998.

104 Systèmes automatisés d'appel et de communication sans intervention humaine.

105 V. Directive 2002/58 Vie privée et communications électroniques, article 13 sur les communications non sollicitées à des fins de prospection directe.

106 V. *infra*, point 6.7. Droit à l'anonymat.

107 Article 8 de la directive 2002/58 : « Présentation et restriction de l'identification de la ligne appelante et de la ligne connectée § 1. Dans les cas où la présentation de l'identification de la ligne appelante est offerte, le fournisseur du service doit offrir à l'utilisateur appelant, par un moyen simple et gratuit, la possibilité d'empêcher la présentation de l'identification de la ligne appelante, et ce, appel par appel. […] § 4. Dans les

Ce texte contenait jusqu'il y a peu une autre manifestation du droit d'opposition. Aux termes de l'article 5, § 3 de cette directive, toute personne devait être clairement informée de toute utilisation à distance de son terminal (via des cookies ou des spywares, par exemple) et pouvoir facilement et gratuitement *s'y opposer*. Aujourd'hui, le stockage d'informations ou l'accès à des informations déjà stockées dans l'équipement terminal d'un utilisateur n'est permis qu'à condition que ce dernier *ait donné son accord*, après avoir été dûment informé, notamment sur les finalités du traitement.

Par ailleurs, permettre la désactivation des puces RFID par l'acquéreur des objets auxquels elles sont attachées[108], est également une expression du principe d'opposition.

En présence de traitements de données de trafic ou de localisation, le droit d'opposition trouverait aussi à s'appliquer[109].

6.4. DROIT DE NE PAS ETRE SOUMIS A UNE DECISION INDIVIDUELLE PRISE PAR UNE MACHINE

Il n'est pas souhaitable qu'une décision qui s'impose à un individu dépende des seules conclusions d'une machine[110]. Or, la technique est de plus en plus souvent utilisée aujourd'hui pour s'en remettre à un « ordinateur » et aux algorithmes qu'il applique pour décider du traitement à réserver à un individu (le considérer ou non comme fraudeur fiscal, ou comme cible de marketing, ou comme voyageur candidat terroriste,…). Ainsi, « les nouvelles technologies entraînent dans leur sillage de nouvelles menaces: face à la multiplication des analyses de plus en plus automatisées de données toujours plus nombreuses et accessibles, les individus risquent d'être réduits à de simples objets, qui seront traités (ou qui pourront même faire l'objet de discrimination) sur la base de «profils» informatiques, de probabilités et de prévisions, sans possibilité de s'opposer aux algorithmes sous-jacents. À défaut de maintenir une protection des données très stricte, les décisions qui ont un «impact significatif» (par exemple, la décision de vous refuser un poste ou de ne pas même vous accorder un entretien d'embauche; d'être arrêté à une frontière et éventuellement de se voir refuser l'entrée dans un pays; d'être soumis à une surveillance intrusive, et éventuellement d'être arrêté, etc.) seront de plus en plus souvent motivées «par le fait que l'ordinateur a dit non» (même si les responsables ou le personnel prenant la décision ne peuvent la justifier complètement) » [111].

A l'exemple de la directive 95/46 (article 15)[112], **il conviendrait d'interdire qu'une décision individuelle affectant une personne de manière significative soit prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité**. A moins que l'on préfère opter pour la voie suivie par la Résolution de Madrid qui ne présente pas ce droit de manière autonome mais le prévoit d'une certaine façon, sous la forme du droit de s'opposer aux

---

cas où la présentation de l'identification de la ligne connectée est offerte, le fournisseur de service doit offrir à l'abonné appelé, par un moyen simple et gratuit, la possibilité d'empêcher la présentation de l'identification de la ligne connectée à l'utilisateur appelant. »

108 V. *infra*, droit de ne pas être pisté.

109 Voy. notamment les articles 6 et 9 de la directive 2002/58 ainsi que OCDE, « Orientations pour les politiques concernant les questions émergentes de protection et autonomisation des consommateurs dans le commerce mobile », Séoul, juin 2008, pp. 22-23.

110 Cf. *supra* ce qui est dit à propos de la dignité humaine.

111 LRDP Kantor Ltd, en association avec Centre for Public Reform, *Étude comparative sur les différentes approches des nouveaux défis en matière de protection de la vie privée, en particulier à la lumière des évolutions technologiques*, Rapport final, Note de synthèse, disponible sur http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_fr.pdf, janvier 2010, p. 2.

112 V. l'analyse de cette disposition par L. BYGRAVE, « Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling », *Computer Law & Security Report*, 2001, volume 17, pp. 17–24.

décisions qui produisent des effets juridiques basées exclusivement sur un traitement automatisé de données à caractère personnel (article 18, § 3).

Une telle interdiction devrait bien évidemment connaître des limitations ou exceptions là où cela se justifie en considération du contexte et des risques en jeu. Ainsi, dans le monde commercial, il était courant de recourir à des évaluations automatisées du profil du consommateur lorsqu'il s'agit de contrats d'octroi de prêt ou de souscription d'une assurance. Le recours à la technique du profil déborde désormais largement ces contextes commerciaux restreints et se nourrit de quantités impressionnantes de données glanées de toutes parts, ainsi qu'il est dit ci-dessus. Il y a peut-être une distinction à faire selon le contexte.[113] Il est également fait recours à un traitement purement automatisé pour décider de la réussite ou de l'échec à certains examens (comme pour l'examen théorique pour le permis de conduire, par exemple, ou des examens de concours administratifs). Les exceptions que l'on estimerait justifiées devraient toutefois être accompagnées de mesures garantissant la sauvegarde de la dignité de l'homme face à la machine, en prévoyant à tout le moins le droit pour l'intéressé de faire valoir *utilement* son point de vue.

6.5. DROIT DE CONNAITRE LA LOGIQUE QUI SOUS-TEND TOUT TRAITEMENT DES DONNEES

Dans le contexte technique actuel, il est un droit qui ne se trouve pas dans la Convention mais qui présente un grand intérêt, notamment face au déploiement exponentiel du phénomène de profilage. **Il s'agit du droit d'avoir connaissance de la logique qui sous-tend tout traitement automatisé des données**[114]. Cette garantie consacrée par la directive 95/46 a un potentiel d'application qui a fait dire à Marc Rotenberg (de l'EPIC – Electronic Privacy Information Center – Washington) qui l'évoquait : "There is a giant sleeping in the EU directive. That is the right to know the logic of a data processing"[115].

Ce droit a été mis en exergue dans le projet de recommandation relative au profilage. Il est relevé dans les considérants de ce texte : "17. […] considering that every person should know the logic involved in profiling; whereas this right should not affect the rights and freedoms of others, in particular, not adversely affect trade secrets or intellectual property or the copyright protecting the software;". Ce texte en projet consacre en conséquence le droit d'accès à cette information (point 5. 1. b. de l'annexe).

A côté de ce droit d'accéder à la logique d'un traitement mais dans le même but de permettre aux personnes concernées de contrôler les fondements de décisions prises à leur encontre, impliquant le traitement de leurs données, il a été suggéré par le professeur canadien Pierre Trudel, autorité reconnue en la matière, que, **dans le contexte spécifique des réseaux, contexte permettant une interactivité et un dialogue accrus, le cadre juridique fasse désormais obligation aux organismes de communiquer aux personnes concernées les données entrées en ligne de compte dans une décision individuelle**[116]. Cela permettrait de s'assurer de l'exactitude des données : « Lors de toute utilisation de renseignements personnels, les organismes publics[117] doivent valider auprès de

---

113 V. le projet de recommandation sur le profilage.

114 La directive européenne qui consacre ce droit à son article 12 ajoute " au moins dans le cas des décisions automatisées ».

115 Marc Rotenberg at the International Conference on Privacy and Data Protection "Re-inventing Data Protection?", Brussels, 12 and 13 October 2007.

116 P. Trudel, « Hypothèses sur l'évolution des concepts du droit de la protection des données personnelles dans l'Etat en réseau », in *Défis du droit à la protection de la vie privée*, *Perspectives du droit européen et nord-américain – Challenges of Privacy and Data Protection Law*, *Perspectives of European and North American Law*, M.V. Perez-Asinari et P. Palazzi (ed.), coll. Cahiers du CRID, n° 31, Bruxelles, Bruylant, 2008, p. 547.

117 La réflexion a été développée dans le contexte spécifique de l'Etat en réseau mais pourrait être envisagée pour l'ensemble des acteurs intervenants sur des réseaux. (Note ajoutée par nous)

l'intéressé les informations auxquelles ils ont eu accès. Lorsque cela est nécessaire pour assurer la qualité des données, les informations doivent être rendues disponibles afin que les personnes concernées puissent en vérifier la teneur et, le cas échéant, exercer leur droit de rectification. »[118] C'est donc un devoir de mise à disposition spontanée des données ayant servi à prendre une décision qui est prôné. Dans cette conception, ce n'est plus la logique (le programme d'ordinateur ou le raisonnement, les critères) appliquée aux données qui doit être communiquée mais les données qui ont été prises en considération elles-mêmes.

6.6. DROIT DE NE PAS ETRE PISTE, SUIVI A LA TRACE

A la suite du développement de l' « Internet des objets », un nouveau droit a fait son apparition dans la doctrine et dans les documents officiels adoptés par certaines organisations, dans lequel on pourrait voir une nouvelle conception du *right to be left alone*[119]. Il s'agit du droit de ne pas être pisté, de ne pas être suivi à la trace *(right not to be tracked).* Ce droit venant en réponse surtout face au développement exponentiel de l'usage des puces RFID, on a aussi parlé du « droit au silence des puces ». Ce droit « exprime l'idée que les individus devront pouvoir se déconnecter de leur environnement réseau à tout moment»[120].

Dans sa Recommandation sur l'utilisation des puces RFID, la Commission européenne recommande différentes lignes de conduite afin d'exploiter les applications RFID de façon licite, éthique et socialement et politiquement acceptable, en respectant le droit à la vie privée et en assurant la protection des données à caractère personnel. Le point 11 de cette Recommandation spécifie : « Les détaillants doivent désactiver ou retirer, au point de vente, les étiquettes de leur application à moins que les consommateurs, après avoir pris connaissance de la politique d'information visée au point 7, acceptent que les étiquettes restent opérationnelles. Par désactivation des étiquettes, on entend tout processus qui interrompt les interactions d'une étiquette avec son environnement et qui n'exige pas de participation active du consommateur. La désactivation ou le retrait des étiquettes par le détaillant doivent être effectués sur-le-champ et sans coût pour le consommateur. Les consommateurs doivent pouvoir vérifier que la désactivation ou le retrait sont effectifs. »[121]

Le Contrôleur européen à la protection des données recommande, face à l'usage des RFID dans le monde commercial, que soit mis en place un principe de *opt-in* suivant lequel toutes les étiquettes RFID attachées à des produits de consommation seraient désactivées par défaut au point de vente[122].

6.7. DROIT A L'ANONYMAT

Il est symptomatique que nombre d'actions que l'on effectue sur Internet laissent entre les mains de différentes personnes des traces de ce que l'on a fait. A l'inverse de ce qui se passe dans le monde physique réel, il n'est pas question de se promener sur les inforoutes, d'entrer dans les magasins

---

118 P. Trudel, *op. cit.*, p. 547.

119 La première formulationdéfinition de la *privacy* a été l'occasion de cette désormais célèbre formule de « *right to be left – ou let – alone » (*WARREN & BRANDEIS, « The Right to Privacy », 4 *Harv. L. Rev.* 193 (1890)).

120 Communication de la Commission au Parlement européen, au Conseil, Comité économique et social européen et au Comité des régions - L'internet des objets : un plan d'action pour l'Europe, COM (2009) 278 final, 18.6.2009, Line of Action 3 - The 'silence of the chips'.

121 Recommandation 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, C (2009) 3200 final, *J.O.U.E.*, 16.5.2009, L 122/47.

122 European Data Protection Supervisor, Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, 18 March 2010, nr. 56-70.

virtuels, de lire le journal, d'être intéressé par une annonce commerciale,… sans que cela se sache. On ne peut manquer de s'interroger sur cette transparence permanente qui ne serait sans doute pas tolérée dans le monde réel.

Nombre de textes à caractère non contraignant préconisent le « droit » du citoyen[123] à disposer de l'anonymat lorsqu'il utilise les services offerts par les technologies nouvelles. La Recommandation n° R(99) 5 du Comité des Ministres du Conseil de l'Europe[124] énonce le même principe: « *L'accès et l'utilisation anonymes des services et des paiements constituent la meilleure protection de la vie privée* » et souligne à ce propos l'intérêt des *Privacy Enhancing Technologies* disponibles sur le marché.

La **notion d'anonymat devrait sans doute être redéfinie** et, dans la foulée, d'autres termes comme la « non identifiabilité » devraient être préférés dans la mesure où cette notion d'anonymat demeure ambiguë. Ce qui est recherché est bien souvent, non un anonymat absolu, mais une « non identifiabilité » fonctionnelle de l'auteur d'un message vis-à-vis de certaines personnes[125].

Celui qui utilise les moyens modernes de communication devrait avoir le choix de rester non identifiable au regard, tantôt de tiers intervenant dans l'acheminement du message ou de prestataires intervenant dans cette chaîne de communication, tantôt du ou des destinataires de la communication et disposer gratuitement, ou au moins à des prix abordables, des moyens d'exercer son choix.

L'anonymat ou la « non identifiabilité fonctionnelle» requis ne sont cependant pas absolus. Au droit à l'anonymat des citoyens, s'oppose l'intérêt supérieur de l'Etat qui pourra imposer des limitations lorsque celles-ci constituent des mesures nécessaires « *pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique la prévention, la recherche, la détection et la poursuite de (certaines) infractions pénales* ». L'équilibre entre le légitime contrôle des infractions et la protection des données pourrait être trouvé dans des systèmes de « pseudo-identité » attribuée à un individu par un fournisseur de service spécialisé auprès duquel dans les seuls cas prévus par la loi et moyennant les modalités fixées par celle-ci pourrait s'opérer le lien entre l'identité réelle d'un usage et son pseudonyme.

La Déclaration de Madrid invite à approfondir l'étude des techniques pouvant intervenir dans la réalisation de l'anonymat. Elle recommande « des recherches approfondies sur le caractère adéquat des techniques de 'désidentification' de données afin de déterminer si ces méthodes permettent de sauvegarder effectivement la vie privée et l'anonymat » (point 8).

Garantir le droit à l'anonymat aux individus ce n'est pas seulement veiller à ce que leur soient offerts des outils de « désidentification » des données pour permettre une navigation anonyme sur les réseaux notamment. C'est aussi garantir aux citoyens le droit d'opter pour une alternative aux services offerts qui n'impose pas une identification des usagers. Cela devrait par exemple être le cas en présence de cartes d'usage des transports en commun. On observe dans certaines agglomérations

---

123 A ce propos, lire notamment S. RODOTA, "Beyond the E.U. Directive : Directions for the Future", in *Privacy : New Risks and opportunities*, Y. POULLET, C. de TERWANGNE et P. TURNER (ed.), coll. Cahiers du CRID, n° 13, Bruxelles, Bruylant, pp. 211 et s.

124 Lignes directrices pour la protection des personnes à l'égard de la collecte et du traitement de données à caractère personnel sur les « inforoutes », texte disponible sur le site du Conseil de l' Europe. Dans le même sens, la recommandation 3/97 du groupe dit de l'article 29 intitulée : « l'anonymat sur Internet ». Cf. également l' avis de la Commission belge de la vie privée pris d'initiative sur le commerce électronique (Avis n° 34/2000 du 22 novembre 2000, avis disponible sur le site de la Commission belge de la vie privée : http://www.privacy.fgov.be) rappelle à bon escient qu'il existe des mécanismes qui permettent d'authentifier l'émetteur d'un message sans nécessairement l'obliger à s'identifier.

125 Sur ce point, lire J. GRIJPINK et C. PRINS, "Digital Anonymity on the Internet, New Rules for anonymous electronic Transactions ?", 17 *CL&SR*, 2001, p. 378 et ss.

le passage à des systèmes de cartes magnétiques pour accéder au réseau de métro ou de bus. Il conviendrait que l'adoption de tels systèmes, dans l'hypothèse où ils impliquent l'identification de l'abonné ou du détenteur de la carte, s'accompagne de la possibilité pour celui qui ne souhaite pas laisser une trace de tous ses déplacements dans les mains de l'organisme de transport, d'acquérir un titre de transport anonyme, éventuellement moyennant paiement d'un tarif spécifique (si c'est justifié par des coûts liés à l'offre de cette alternative) raisonnable.

7. Article 9 – Exceptions et restrictions

A l'instar de ce qui a été dit *supra* sur la restriction du champ d'application de la Convention, une **exception générale devrait être ajoutée**, selon nombre d'auteurs, **en ce qui concerne les traitements de données à caractère personnel à « but familial/personnel ou domestique ».** Le raisonnement est juste : on ne peut au nom de la protection des données d'autrui violer l'intimité de celui qui traite des données pour son propre compte. La portée de cette exception doit cependant tenir compte, comme le montre l'affaire *Linqvist* tranchée par la CJCE déjà citée, du fait que des réflexions privées postées sur un site web sortent indéniablement de la sphère privée ou domestique des intéressés et sont rendues accessibles à un nombre indéterminé et illimité de personnes.

La pertinence et la portée d'une telle exception ont pris une grande importance avec le développement du Web 2.0 et l'utilisation exponentielle du Web, de ses blogs, ses réseaux sociaux, son Twitter, par des particuliers qui fournissent désormais eux-mêmes des contenus (dans lesquels figurent souvent des données à caractère personnel sous forme d'informations, de photos ou de vidéos). L' « Internet des loisirs » dont il a été question *supra* illustre parfaitement ce mélange de finalités personnelles et familiales et de l'utilisation d'un mode public d'expression qui vient contredire la vocation « privée » des données partagées. Cette réalité a pour conséquence qu'il n'est pas évident d'accepter ou de refuser purement et simplement l'application d'une telle exception dans le nouvel environnement technologique.

"The overall problem is that the granting of a full exemption from data protection requirements to anyone who uploads materials to the Internet as a private individual would lead to easy circumvention of the rules and, in an age of user-generated content, would fundamentally undermine data protection (and privacy) itself; yet the full imposition of the law to all such individuals would seem excessive and, because of the sheer numbers, would be largely unenforceable. The question - the challenge - is then perhaps whether a middle way be found?"[126]

Le point 2 devrait prévoir des exceptions liées à la nécessité de garantir la liberté d'expression ou d'opinion (principe du juste équilibre entre la protection des données et la liberté d'opinion et/ou d'expression). La formulation d'une telle exception devra être délicatement soupesée étant donné que le régime spécifique réservé à la presse dans nombre de pays de par le monde, régime au titre duquel on trouve des exceptions partielles ou totales aux principes de protection des données (dans les pays européen et au Canada, par exemple), doit être repensé dans le contexte d'Internet. Le déploiement du Web 2.0 a vu la dilution de la notion de presse et l'estompement de celle de journaliste, la diffusion et le commentaire de nouvelles et d'informations d'intérêt public n'étant plus l'apanage, dans ce nouvel environnement, des journalistes ou des journaux.[127]

Le point 3 à propos des statistiques ou recherches n'envisage que les risques liés à la protection des données individuelles à la base de la recherche ou de la statistique. Or, la statistique et la recherche

[126] D. KORFF, *Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments*, EC Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, WP 2, 20 January 2010, p. 8.

[127] Voy. les développements sur cette question en marge de l'arrêt très interpellant de la CJCE :

scientifique nécessitent certaines précautions même lorsqu'elles travaillent sur des données anonymes ou rendues anonymes dans la mesure où elles introduisent la possibilité d'appliquer les profils ainsi créés à des individus.

8. Responsabilité

La Convention 108 ne contient aucune disposition concernant la responsabilité du respect des règles de protection qu'elle édicte.

A l'inverse, les Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données à caractère personnel de 1980 énoncent le *Principe de la responsabilité* selon lequel : « Tout maître de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus ». Il s'agit donc dans un premier temps de spécifier que c'est au maitre du fichier qu'incombe de garantir le respect des principes de protection.

Le temps écoulé depuis l'adoption de ce texte a montré combien il était **important de responsabiliser davantage les maitres de fichier**. C'est en effet la clé d'une véritable prise en compte des exigences de protection des données au sein des organisations. « Ensuring compliance before the fact is less expensive, and imposes less burden on data subjects than having to pursue enforcement actions in court or otherwise. »[128]

Dans un très récent document qu'il a adopté, le Groupe de l'article 29 invite la Commission européenne à réécrire le principe de responsabilité qui se trouve dans la directive 95/46 et à insister sur le fait qu'assumer la responsabilité du respect des règles protectrices implique de prendre des mesures concrètes. Le Groupe de l'article 29 propose en conséquence que la responsabilité aille désormais de pair avec l'obligation de pouvoir démontrer qu'on a bien pris de telles mesures : « […] un principe légal de responsabilité exigerait expressément des responsables du traitement des données qu'ils mettent en oeuvre des mesures appropriées et efficaces en vue de garantir le respect des principes et obligations prévus par la directive, et qu'ils soient en mesure d'en faire la preuve sur demande. En pratique, ceci se traduirait par des programmes évolutifs visant à appliquer les principes relatifs à la protection des données en vigueur (parfois appelés «programmes de conformité»). »[129] Egalement : « **le principe de responsabilité exigerait des responsables du traitement des données qu'ils mettent en place les mécanismes internes nécessaires pour démontrer leur conformité** aux parties prenantes externes, notamment aux autorités nationales chargées de la protection des données. Au final, la nécessité de prouver que les mesures appropriées ont été prises pour assurer la conformité facilitera considérablement l'exécution des règles applicables.»[130]

La Résolution de Madrid contient une disposition allant clairement dans ce sens. Son article 11 intitulé « Accountability principle » prévoit pour la personne responsable, à côté de l'obligation de prendre toutes les mesures nécessaires pour se conformer aux règles de protection, l'obligation de mettre en place les mécanismes internes permettant de démontrer qu'il s'est précisément conformé à ces règles. Cet *accountability principle* s'accompagne par ailleurs d'un régime de responsabilité (*Liability*) devant permettre d'indemniser les personnes concernées pour tout dommage matériel ou moral encouru du fait du non-respect des règles de protection.

---

[128] OECD Directorate for Science, Technology And Industry, Committee For Information, Computer and Communications Policy, Working Party on Information Security and Privacy, Report on Compliance with, and Enforcement of, Privacy Protection Online, DSTI/ICCP/REG(2002)5/FINAL, 12 February 2003.

[129] Groupe de l'article 29, Avis n° 3/2010 sur le principe de la responsabilité, WP 173 du 13 juillet 2010, point 3.

[130] Groupe de l'article 29,WP 168, point 79.

La réflexion pourrait également être menée dans le cadre de la Convention 108.

9. Prise en compte du respect de la vie privée dès la conception (Privacy by design)

"You need to start to think to privacy when you think to the idea you will design, not at the time of implementing it."[131]

Le principe de « prise en compte de la vie privée dès la conception » (*Privacy by Design*) apparaît de plus en plus comme une exigence incontournable aujourd'hui pour réaliser efficacement la protection de la vie privée et des données. Cette **exigence d'intégration de la préoccupation de protection de la vie privée au sein même des systèmes, produits et services créés et dès les premiers stades de leur conception** a été évoquée à de multiples reprises lors de l'Internet Governance Forum de septembre 2010[132]. Aux yeux d'acteurs de tous horizons géographiques, il s'agit là d'une contribution adéquate à la protection des données et de la vie privée.

A plusieurs occasions, la Commission européenne a souligné la nécessité d'un tel principe, notamment dans le cas d'applications particulières (comme pour l'Internet des Objets : « Le développement des TIC a montré par le passé que [les questions de confiance et de vie privée] sont parfois négligées durant la phase de conception, et qu'intégrer par la suite des éléments afin de les prendre en compte entraîne des difficultés et des coûts et peut réduire considérablement la qualité des systèmes. Il est donc primordial que l'approche de la conception initiale des éléments de l'IdO intègre le respect de la vie privée et la sécurité ainsi que l'ensemble des exigences des utilisateurs. »[133]). Le Groupe de l'article 29 ainsi que le Contrôleur européen à la protection des données ont également indiqué la nécessité d'une consécration légale de cette exigence.

L'OCDE a de son côté beaucoup œuvré pour inciter au recours aux technologies pour favoriser la protection des données. La Déclaration ministérielle de 1998 a établi que les technologies protectrices de la vie privée pouvaient jouer un rôle décisif en permettant aux internautes d'exercer un contrôle accru sur les informations personnelles les concernant et d'exercer leur liberté de choix eu égard aux utilisations qui sont faites de leurs données. Les gouvernements des pays membres de

---

131 Joseph ALHADEFF, vice president for Global Public Policy and Chief Privacy Officer for Oracle Corporation (Washington), at the Internet Governance Forum, Workshop "The Future of Privacy", Vilnius, 14 September 2010.

132 Hugh STEVENSON, Deputy Director for International Consumer Protection Office of International Affairs, U.S. Federal Trade Commission: "The first is we [the US Federal Trade Commission] encourage businesses to integrate privacy and security into their systems at the outset. I think that's responsive to one of the comments here on the important of incentives of privacy and system design. […]" ; Ellen BLACKLER, Executive Director, AT&T; Rosa BARCELO, conseillère juridique auprès du Contrôleur européen à la Protection des Données : "Another right we will support is the right to privacy by design. This right will be required, not only the data protection principles taken into account in the technology but also in the whole organisation, in the beginning from the moment when the standards are written to the end of the process" ; Joseph ALHADEFF, vice president for Global Public Policy and Chief Privacy Officer for Oracle Corporation (Washington); the Internet Architecture Board, (IAB); Jon PETERSON (Neustar), Hannes TSCHOFENIG (Nokia Siemens Network), Bernard ABOBA (Microsoft), "Position Paper: Improving Privacy on the Internet and the Role of the Standards Community" for the "Future of Privacy" workshop: "From the long experience of the Internet Engineering Task Force (IETF), the authors believe that an important initial step is to consider privacy while designing protocols and architectures, rather than as something to bold on as an afterthought. […] Technical work needs to be backed-up by laws and appropriate disincentives to violate them. Providing the right incentives for companies to consider privacy friendly design will be a game changer."; etc.

133 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, L'internet des objets – Un plan d'action pour l'Europe, 18 juin 2009, COM(2009) 278 final.

l'OCDE se sont engagés à veiller à encourager l'utilisation de technologies permettant d'améliorer la vie privée. Ils ont demandé à l'OCDE de coopérer avec l'industrie et les entreprises dans le cadre de leurs travaux en vue d'assurer la protection de la vie privée sur les réseaux mondiaux. [134]

Il convient de noter ici une réflexion concernant un des aspects de la prise en compte de la vie privée au sein même de la configuration technique des produits. C'est l'observation soulevée par les auteurs d'une étude commandée par la Commission européenne sur les nouveaux défis pour la protection de la vie privée à la lumière des évolutions technologiques. Ces auteurs relèvent que imposer un paramétrage par défaut protecteur de la vie privée aux acteurs proposant des sites de réseaux sociaux ou des blogs permettrait de répondre au problème des limites de l'exception pour usage à des fins personnelles (cf. ce qui est dit *supra* sur ces limites en cas d'utilisation de moyens d'expression publics comme Internet). Pour ces auteurs, « Il devrait être possible d'appliquer les règles de protection des données de façon plus souple aux activités relativement insignifiantes sur l'Internet. Le fait de vouloir soumettre les particuliers qui utilisent normalement l'Internet au plein effet de toutes les règles qui s'appliquent aux «contrôleurs» pose problème. Et nous pensons que la meilleure façon de résoudre ce problème consiste à réglementer les services qu'utilisent ces particuliers: les sites de réseaux sociaux, les sites hébergeant des «blogs», etc. Ces hôtes devraient être obligés à doter leurs sites et leurs services de paramètres par défaut et d'outils respectueux de la vie privée. Les utilisateurs ordinaires qui utilisent ces sites sans modifier les paramètres par défaut devraient pouvoir être sûrs qu'ils n'enfreignent aucune loi sur la protection des données; si les paramètres par défaut ne protègent pas la vie privée et les données à caractère personnel, le site qui a défini ces paramètres doit en assumer la responsabilité principale. » [135]

Au-delà de l'obligation générale de prise en compte et d'intégration des exigences de la protection des données (transparence sur les données recueillies, sur ce qui en est fait, sur qui a eu accès, recueil d'un consentement éclairé,…) dans les produits et services, deux facettes particulières de cette obligation ont été mises en exergue :

9.1. PRINCIPE DE MINIMISATION DES DONNEES

Voir ce qui a été dit sur ce point *supra* dans le point 3. sur les principes de protection, le principe de minimisation des données étant présenté comme un éventuel nouveau principe de protection.

9.2. ETUDES D'IMPACT SUR LA VIE PRIVEE

Il a également été demandé que, avant de développer et lancer un produit ou service (comme les puces RFID), les concepteurs soient tenus de procéder à une évaluation des incidences que le produit ou service en question risque d'avoir sur la vie privée et la protection des données[136]. Pour la

---

134 OCDE, Déclaration ministérielle relative à la protection de la vie privée sur les réseaux mondiaux, 19 octobre 1998. V. Egalement Forum de l'OCDE sur les technologies protectrices de la vie privée (TPVP), 8 octobre 2001 ; OCDE, *Protection de la vie privée en ligne Orientations politiques et pratiques de l'OCDE* , Paris, 2003, pp. 273-383.

135 LRDP Kantor Ltd, en association avec Centre for Public Reform, *Etude comparative sur les différentes approches des nouveaux défis en matière de protection de la vie privée, en particulier à la lumière des évolutions technologiques*, Rapport final, disponible sur http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_fr.pdf, janvier 2010, § 35.

136 Not. le Contrôleur à la protection des données (v. son Avis au JO C 101, 23.4.2008, pp 1-12), la Commission européenne (Recommandation 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, C(2009) 3200).

Commission européenne, le niveau de détail de l'évaluation doit être approprié aux risques que l'application peut présenter pour la vie privée.

On pourrait retrouver dans ces études d'impact sur la vie privée la manifestation de la mise en balance des droits et intérêts qui devrait précéder le lancement de tout traitement de données (cf. *supra* le point 3.2.). Cette obligation de mettre par écrit la mise en balance garantit que l'on a effectivement procédé à une prise en considération de tous les intérêts en jeu et permettrait de contester plus facilement, le cas échéant, le résultat de cette mise en balance.

Des études d'impact pourraient au minimum être rendues obligatoires en présence de produits, services ou systèmes d'information qui risquent d'avoir un impact significatif sur la population.

Dans cette ligne, en Australie, « The Government now proposes that the Privacy Commissioner will be able to direct federal government agencies (but not companies) to provide to the Commissioner a PIA [Privacy Impact Assessment] on a 'new project or development' that the Commissioner considers will have a 'significant impact' on the handling of personal information, and to report to the Minister (query whether also the public) if the agency fails to do so (AusGov, 2009: 47-4)." [137]

Il est intéressant de relever la façon de procéder des auteurs de la Résolution de Madrid sur ces points. Ce texte rassemble dans une disposition intitulée « Proactive measures » un ensemble de mesures organisationnelles, techniques ou autres, dessinant un « new and modern framework » et destinées à contribuer à la protection. Parmi ces mesures proactives, on trouve l'adaptation de la technologie aux lois de protection des données[138] et la réalisation d'études d'impact sur la vie privée[139], mais aussi la mise en œuvre de procédures pour prévenir et détecter les failles de sécurité de même que pour y répondre, la désignation de « data protection or privacy officers », la mise en œuvre de programmes de formation au sein des organisations, la réalisation d'audits pour vérifier le respect des règles de protection et l'adoption de codes de conduite.

10. Protection spécifique des données des mineurs

La Convention 108 ne contient aucune disposition spécifique pour protéger les données relatives à des mineurs. Or, du fait des risques particuliers qu'ils encourent sur Internet ainsi que liés à l'usage de leurs téléphones mobiles, **les mineurs méritent peut-être une protection ajustée**. Ils sont les cibles d'actions de marketing, d'invitations à devenir membres de tels réseaux sociaux ou de tels groupes, abonnés de tels services, utilisateurs de telles applications… Mais en même temps, ils manquent de discernement et d'esprit critique, ne prennent pas la mesure des implications de leurs décisions, prennent des décisions impulsives centrées sur le court terme,…

[137] G. GREENLEAF, Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, Country Study B.2 – Australia, January 2010, available at http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_B2_australia.pdf, p. 33.

[138] "States should encourage, through their domestic law, the implementation by those involved in any stage of the processing of measures to promote better compliance with applicable laws on the protection of privacy with regard to the processing of personal data. Such measures could include, among others: […] e. The adaptation of information systems and/or technologies for the processing of personal data to the applicable laws on the protection of privacy with regard to the processing of personal data, particularly at the time of deciding on their technical specifications and on the development and implementation thereof." (Article 22)

[139] "Article 22. […] f. The implementation of privacy impact assessments prior to implementing new information systems and/or technologies for the processing of personal data, as well as prior to carrying out any new method of processing personal data or substantial modifications in existing processing."

Dans ses *Orientations pour les politiques concernant les questions émergentes de protection et autonomisation des consommateurs dans le commerce mobile*[140], l'OCDE a traité particulièrement la question des risques accrus d'exploitation commerciale des mineurs dans le contexte du commerce mobile. En matière de « Protection des données nominatives des enfants », l'OCDE formule la recommandation suivante :

« Les pays pourraient explorer les moyens d'adapter les lois et règlements en vigueur protégeant les enfants en ligne dans l'environnement mobile. Ainsi, aux États-Unis, des lois fédérales limitent le recueil, l'utilisation et la communication d'informations potentiellement nominatives émanant ou concernant des enfants de moins de 13 ans dans les services en ligne. Elles prévoient notamment une information sur les politiques en matière de vie privée, la vérification de l'accord parental pour le recueil d'informations nominatives auprès des enfants (avec un certain nombre d'exceptions limitées), la vérification et la suppression par les parents des données personnelles émanant de leurs enfants et l'obligation de procédures destinées à protéger la sécurité des données. »[141]

La difficulté concernant le consentement des mineurs au traitement de leurs données avait déjà été soulevée dans le rapport de 2004 sur « L'autodétermination informationnelle à l'ère d'Internet »[142]. Ainsi il y était relevé que Le consentement par des individus mineurs au traitement des données à caractère personnel les concernant pose des problèmes délicats. Le consentement doit émaner d'une personne capable au sens de la loi. Le consentement exprimé par un mineur ne suffit pas sans l'autorisation parentale, ce qui n'empêche pas de devoir associer ce mineur au consentement dans la mesure de ses capacités de compréhension voire d'exiger à côté du consentement parental son consentement exprimé de manière autonome.

Récemment, le développement de services interactifs sur Internet a donné à ces principes une actualité. Les enfants sont une des cibles privilégiées pour les « vendeurs » de tous poils présents sur Internet et nombre de méthodes de collecte d'informations sont utilisées pour les amener à fournir des informations personnelles : jeux-concours, formulaires d'adhésion, etc.

La vérification du consentement parental à la délivrance de telles informations apparaît donc nécessaire. La loi américaine, le « Children's Online Privacy Protection Act » (COPPA) de 1998[143] exige que le fournisseur de services collectant des informations auprès de mineurs soient soumis au principe du « Verifiable Parental Consent » défini comme « tout effort raisonnable (prenant en considération la technologie disponible), comprenant une demande pour l'autorisation pour la collecte, l'utilisation et la communication futures de données relatives à l'enfant, et telles que décrites dans la notice d'information, de manière à garantir que les parents d'un enfant reçoivent notification de ces pratiques de collecte, utilisation et communication et puissent autoriser la collecte, l'utilisation, la communication et ses utilisations ultérieures avant que l'information ne soit collectée auprès de l'enfant ».

---

140 OCDE, Séoul, juin 2008.

141 *Ibidem*, p. 24.

142 Précité.

143 Sect. 1302(9). Le texte de la loi américaine est disponible sur le site de la Federal Trade Commission http://www.ftc.gov/ogc/coppa1.htm. Quelques exceptions à cette exigence sont prévues par la loi.

11. Protection spécifique en présence de traitements présentant des risques particuliers au regard des droits et libertés

Les développements techniques observés depuis l'adoption de la Convention 108 ont démontré que certains traitements présentent des dangers particuliers pour les personnes concernées.

Il peut s'agir de traitements envisagés au sein du secteur public, qui présentent les dangers cumulés de couvrir l'ensemble de la population d'un pays, ou des parties substantielles de cette population, et d'être revêtus d'un caractère obligatoire, ne laissant pas la place à des refus de laisser traiter ses données en avançant une justification légitime. Les risques d'interconnexion de fichiers sont particulièrement présents au sein du secteur public dès lors que l'on recourt au même numéro unique d'identification pour plusieurs fichiers. Ces risques viennent donc augmenter la dangerosité de fichiers ou traitements de données qui présentent les caractéristiques sus-mentionnées et pour lesquels l'usage d'un numéro d'identification non spécifique est envisagée.

Des traitements du secteur privé peuvent également présenter des risques particuliers, comme l'introduction d'un nouvel outil technique (par exemple les étiquettes RFID, les nouveaux systèmes de surveillance de masse, la reconnaissance faciale, l'imagerie corporelle, les identifiants biométriques,…) risquant de porter atteinte aux intérêts, droits et libertés des personnes visées par cet outil.

Il serait bon de prévoir une mesure de précaution préalable à la mise en œuvre de tels traitements. Cette mesure pourrait prendre la forme d'un contrôle préalable effectué par l'autorité de protection des données ou de l'exigence pour l'organisme, l'institution ou l'acteur privé auteur du projet de traitement de réaliser une étude d'impact sur la vie privée (cf. *supra* point 9.2.).

12. Recours

A l'instar de réflexions qui se sont fait jour ces dernières années, il convient de **réfléchir à l'opportunité d'introduire dans la Convention 108 la possibilité pour des personnes morales d'intenter une action en justice en réponse à des violations de règles de protection des données**.[144]

« […], il faut comprendre que dans le domaine de la protection de la vie privée et des données, le préjudice subi par une personne donnée ne suffit généralement pas à pousser celle-ci à faire appel aux tribunaux. La plupart du temps, les personnes concernées n'intentent pas d'action en justice de leur propre initiative après avoir reçu des pourriels ou vu leur nom inclus à tort dans un fichier. Cet amendement permettrait aux associations de consommateurs et aux syndicats qui défendent les intérêts des consommateurs à un niveau collectif d'intenter une action en justice en leur nom. »[145]

De même, « permettre, comme on l'a mentionné plus haut, à des entités juridiques, telles les associations de consommateurs et les FSCEP [fournisseurs de services de communications électroniques accessibles au public], d'intenter une action en justice renforce la position des

[144] V. notamment LRDP Kantor Ltd, en association avec Centre for Public Reform, *Etude comparative sur les différentes approches des nouveaux défis en matière de protection de la vie privée, en particulier à la lumière des évolutions technologiques*, Rapport final, disponible sur http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_fr.pdf, janvier 2010, §§ 109-111.

[145] Deuxième avis du contrôleur européen de la protection des données relatif au réexamen de 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 (directive «vie privée et communications électroniques»), *J.O.U.E.*, 6 juin 2009, C-128, p. 39, § 89.

consommateurs et favorise le respect général de la législation sur la protection des données. Si le risque de poursuites judiciaires est plus élevé pour les compagnies qui violent le droit, il est probable que celles-ci investiront davantage pour se conformer la législation relative à la protection. »[146]

Au-delà de la question de l'efficacité de la défense des droits des individus, la décision de reconnaître la capacité d'ester en justice pour les personnes morales dans cette matière aurait indéniablement pour conséquence une amélioration du respect des principes de protection sur le terrain.

Le **recours à l'arbitrage** pourrait également être envisagé au vu des réels avantages qu'il offre aux personnes lésées (coût moins élevé que nombre de recours juridictionnels, rapidité de décision,…).

13. Droit applicable en matière de protection des données et de vie privée – Flux transfrontières de données

13.1. UN CONTEXTE TRIPLEMENT « ECLATE »

En préliminaire à la question du droit applicable, il importe de relever les caractéristiques du nouveau contexte technique qui ont une incidence sur la résolution de cette question. Ces caractéristiques tiennent au fait que le contexte se présente comme triplement éclaté.

L'utilisation quotidienne et massive d'Internet (*webmails*, réseaux sociaux, plateformes d'*e-commerce*, etc.) engendre d'innombrables flux transfrontières de données. Les développements en informatique, tels que le « *cloud computing* », permettent une véritable délocalisation de la ressource informatique et informationnelle ; la donnée – financière, personnelle, commerciale, etc. – est traitée là où son traitement sera le plus efficace – économiquement et techniquement –, et elle est accessible à n'importe quel endroit du globe via Internet. Depuis longtemps maintenant, les services de la société de l'information[147] sont offerts en ligne, à tout le monde, à partir d'un ou plusieurs pays, et se déclinent en autant de variétés qu'il y a de besoins et de clientèles : individus agissant à des fins privées ou professionnelles, entreprises, petites, moyennes ou grandes, associations sans but lucratif, administrations publiques, syndicats, politiciens en campagne, hôpitaux, universités, etc. S'observe ainsi un double éclatement quant aux services en question : d'une part, quant à la *localisation* de leur contexte (localisation des prestataires, des destinataires, des moyens de traitement, de l'accessibilité au service, etc.), et d'autre part, concernant leur *nature*, en fonction des acteurs et des données qu'ils impliquent (acteurs publics, personnes physiques agissant à des fins privées, multinationales, etc.).

Inévitablement, un tel contexte interpelle quant aux questions de compétence internationale des juridictions ou autorités publiques (polices – judiciaire, financière, etc. –, autorités de protection des données, etc.), ainsi que quant à l'identification du droit qui régit les diverses configurations factuelles envisageables[148]. Dans l'établissement et l'interprétation des règles de droit tranchant ces questions, divers objectifs cruciaux sont à concilier, parmi lesquels comptent le principe de territorialité, l'harmonie internationale, la

---

146 *Ibidem*, § 92.

147 En droit communautaire, ils sont définis comme «Tout service presté normalement contre rémunération, à distance par voie électronique et à la demande individuelle d'un destinataire de services», article 1er, 2), *a*) de la directive (CE) no 98/48 du Parlement européen et du Conseil du 20 juillet 1998, portant modification de la directive 98/34/CE prévoyant une procédure d'information dans le domaine des normes et réglementations techniques, *J.O.* L 217, du 5 août 1998.

148 A cet égard, le propos est principalement focalisé sur la question de la détermination du droit applicable.

nécessitée de garantir la protection effective des droits – fondamentaux ou non – de certains et le besoin de sécurité juridique.

La Convention 108 et son protocole – traités internationaux contraignants – régissent le traitement automatisé de données à caractère personnel et les flux transfrontières de données y liés. Au regard de l'internationalité de la situation précédemment exposée, la Convention rapproche les législations de quarante-trois Etats[149] sur les quarante-sept Etats Membres du Conseil de l'Europe. Tandis que le protocole, nettement plus récent (2001), a été signé par quarante-et-un Etats dont trente ont procédé à sa ratification[150]. En outre, tous les Etats membres du Conseil de l'Europe sont liés par l'article 8 de la CEDH, particulièrement pertinent en l'espèce. Il faut relever au passage que des Etats non membres du Conseil de l'Europe peuvent adhérer à la Convention n°108 (article 23) et, ensuite, au protocole additionnel (article 3, § 2).

Vingt-sept des quarante-trois Etats membres à la Convention n°108 sont également membres de l'Union européenne où, principalement, les directives 95/46 et 2002/58 harmonisent leurs législations en matière de traitement de données à caractère personnel[151]. Sont à ajouter à ces Etats l'Islande, la Norvège et le Liechtenstein qui, en vertu de l'accord sur l'Espace Economique Européen, sont également tenus de respecter ces directives.

Pour le surplus, les règles contraignantes régissant la protection des données sont d'origine strictement nationale. Le cas échéant, les lignes directrices de l'Organisation de Coopération et de Développement Economiques – non contraignantes –, sur la protection de la vie privée et les flux transfrontières de données de caractère personnel, peuvent constituer une source d'inspiration au-delà des textes précités. Enfin, les règles relatives à la protection des données se voient réserver explicitement une place au sein des règles de l'Organisation Mondiale du Commerce (OMC). Ainsi, le commerce international des services peut être restreint pour des motifs liés à la protection des données ; l'article XIV, c), ii) de l'Accord Général sur le Commerce des Services prévoit que ledit accord n'empêchera pas l'application de mesures, par les Etats membres, nécessaires « à la protection de la vie privée des personnes pour ce qui est du traitement et de la dissémination de données personnelles, ainsi qu'à la protection du caractère confidentiel des dossiers et comptes personnels ». Le cas échéant, une mauvaise application de cette exception pourrait être identifiée par un groupe spécial (*panel*) et donner lieu au déclenchement de sanctions propres à l'OMC.

Une troisième forme d'éclatement, liée au contexte souvent international des développements technologiques (en particulier Internet et les services y liés) s'observe donc : l'éclatement des ordres et cultures juridiques amenés à appréhender des situations identiques ou similaires.

Dans un tel contexte, la souplesse d'un texte international tel que la Convention n°108 est utile pour garantir la coexistence des différentes strates de réglementation et permettre la juste et adéquate appréhension par le droit des situations complexes et évolutives que présentent les technologies actuelles (et futures). Ce sont les Etats qui – le cas échéant sous le contrôle d'un juge international – spécifient la protection des personnes concernées et en assurent l'effectivité via leurs législateurs, juridictions et autorités nationales de protection des données. Il s'avère opportun de s'interroger sur l'intérêt d'une éventuelle harmonisation des

[149] La Turquie et la Russie ont signé la Convention 108 du Conseil de l'Europe mais ne l'ont pas ratifiée, tandis que Saint-Marin et l'Arménie ne l'ont pas signée.

[150] Le protocole n'a pas encore été signé par l'Arménie, l'Azerbaïdjan, la Géorgie, Malte, Saint-Marin et la Slovénie. Ne l'ont pas encore ratifié la Belgique, le Danemark, la Finlande, la Grèce, l'Islande, l'Italie, la Moldavie, la Norvège, le Royaume-Uni, la Russie et la Turquie.

[151] V. également la Charte européenne des droits fondamentaux.

règles de droit international privé en la matière, et de déterminer quel rôle pourrait avoir le Conseil de l'Europe à cet égard.

13.2. REGIME DES FLUX TRANSFRONTIERES DE DONNEES [FTD] : ABSENCE DE REGLE DE DROIT APPLICABLE A LA PROTECTION DES DONNEES

Au niveau du Conseil de l'Europe, les flux transfrontières de données sont régis par les articles 12 de la Convention et 2 du Protocole.

Ainsi, entre Etats parties à la Convention, la seule fin de protection de la vie privée ne peut en principe donner lieu à l'interdiction ou à la soumission à une autorisation administrative des flux transfrontières de données à destination du territoire d'une autre Partie. Exceptionnellement, la Convention le permet (article 12, al. 2, a) et b)) : « dans la mesure où sa législation prévoit une réglementation spécifique pour certaines catégories de données à caractère personnel ou de fichiers automatisés de données à caractère personnel, en raison de la nature de ces données ou de ces fichiers, sauf si la réglementation de l'autre Partie apporte une protection équivalente » ; ou « lorsque le transfert est effectué à partir de son territoire vers le territoire d'un Etat non contractant par l'intermédiaire du territoire d'une autre Partie, afin d'éviter que de tels transferts n'aboutissent à contourner la législation de la Partie visée au début du présent paragraphe ». Dans la première hypothèse, un Etat peut limiter les FTD relatifs à certaines catégories de données ou de traitements, si l'Etat de destination ne garantit pas une protection « équivalente ». Quant à la deuxième hypothèse, consacrant une disposition anti-contournement, les FTD à destination d'Etats tiers ne sont qu'indirectement pris en compte.

Les Etats membres de l'Union européenne quant à eux « ne peuvent restreindre ni interdire la libre circulation des données à caractère personnel entre États membres pour des raisons relatives à la protection assurée en vertu » de la directive 95/46 (article 1er, § 2, de la directive 95/46). La règle est donc plus stricte entre Etats membres de l'Union européenne.

Le Protocole additionnel à la Convention 108 vise quant à lui les FTD à destination d'un Etat (ou d'une organisation) tiers à la Convention (non « soumis à la juridiction d'une Partie à la Convention »). Il ne permet de tels flux qu'à condition que l'Etat (ou organisation) tiers « assure un niveau de protection adéquat » (article 2, § 1er du protocole). Cette exigence n'est toutefois pas requise pour un transfert de données dans deux hypothèses. D'une part, « si le droit interne le prévoit : pour des intérêts spécifiques de la personne concernée, ou lorsque des intérêts légitimes prévalent, en particulier des intérêts publics important » (article 2, § 2, a), du Protocole). Le consentement de la personne concernée pourrait ainsi entrer en ligne de compte, comme la directive 95/46, abordée dans la suite des développements, le prévoit. L'on s'inquiètera toutefois en passant du risque qu'*en pratique*, ce consentement ne soit qu'une clause contractuelle parmi d'autres, réputée contractuelle par la simple utilisation du service offert… D'autre part, la nécessité d'une protection adéquate tombe « si des garanties pouvant notamment résulter de clauses contractuelles sont fournies par la personne responsable du transfert, et sont jugées suffisantes par les autorités compétentes, conformément au droit interne » (article 2, § 2, b), du Protocole).

Les Etats membres de l'Union européenne sont également tenus d'appliquer les règles de la directive 95/46 relatives aux flux à destination d'Etat tiers à l'Union européenne, susceptibles donc d'être également parties à la Convention n°108. L'article 25 de la directive 95/46 érige également en principe la nécessité d'une protection adéquate dans l'Etat tiers de destination des données, et l'article 26 énumère quant à lui une série d'exceptions à ce principe, dont le consentement indubitable de la personne concernée et les garanties contractuelles. Dans ce cadre, il est important de souligner, à propos des Etats tiers à l'Union européenne mais partie à la Convention n°108, que la

non adhésion à son protocole additionnel pourrait constituer – à défaut de règles similaires en droit interne – une lacune décisive dans la protection offerte[152]. L'absence de « mécanismes procéduraux institués pour garantir que les principes fondamentaux de protection des données sont véritablement appliqués » pourrait aussi être déterminante[153]. Bref, un Etat partie à la Convention n°108 du Conseil de l'Europe – voire même également au Protocole – n'est pas de ce simple fait considéré comme garantissant une protection adéquate. Même si, en pratique, il en ira vraisemblablement de la sorte dans de nombreux cas.

En passant, il est intéressant de noter qu'en l'état, l'analyse d'adéquation à réaliser en vertu de la directive 95/46 ne permet pas de prendre en compte, dans l'Etat tiers de destination, les règles portant sur les traitements « mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal[154]. Ce qui est par contre possible dans le contexte du protocole additionnel de la Convention n°108[155].

Quoi qu'il en soit, l'objectif poursuivi par la Convention n°108 dans la régulation des flux transfrontières est de « concilier les conditions nécessaires à une protection des données efficace avec le principe de la libre circulation des informations sans considération de frontières, qui est consacré par l'article 10 de la Convention européenne des Droits l'Homme » (rapport explicatif, § 62). Il s'agit notamment d'éviter que cette dernière soit remise en cause par « des formes de protectionnisme » (rapport explicatif, § 20). Ainsi, entre Etats contractants, il n'est « pas permis d'ériger des obstacles aux [FTD], que ce soit sous forme *d'interdictions ou d'autorisations spéciales* » (rapport explicatif, § 67) (italiques ajoutés par nous). Ces termes indiquent que la Convention prohibe un certain « contrôle administratif ».

Toutefois, d'une part, il ne s'agit pas d'empêcher les Etats de « prendre d'autres mesures pour s'informer de la circulation de données entre son territoire et celui d'un autre Etat contractant, par exemple au moyen de déclarations obligatoires par les maîtres de fichiers » (rapport explicatif, § 67). Et d'autre part, comme précédemment évoqué, il est permis aux Etats de retrouver ce contrôle pour des catégories spécifiques de données à caractère personnel ou de traitements[156].

---

152 Groupe de l'article 29, WP 12, Transferts de données personnelles vers des pays tiers: Application des articles 25 et 26 de la directive relative à la protection des données, 24 juillet 1998, p. 9.

153 *Ibid*.

154 L'article 3, § 2, 1er tiret de la directive 95/46 exclut ces matières du champ d'application de cette directive.

155 Au niveau de l'Union européenne, la décision 2008/977/JAI vise le traitement de données en matière de coopérations policière et judiciaire pénales, par les autorités compétentes, voy. article 1er, § 2, de la Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008, relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale. Elle ne peut évidemment pas concerner l'hypothèse où des autorités compétentes étrangères obtiendraient des données à caractère personnel relatives à des ressortissants de l'Union européenne à partir de bases de données gérées par des prestataires de services situés dans l'Etat tiers en question, sous sa juridiction. Or cette question pourrait utilement être prise en compte dans une analyse d'adéquation. Il en serait par exemple ainsi de la *third party doctrine* aux Etats-Unis. Cette doctrine pourrait être considérée dans une analyse d'adéquation opérée sur la base de la Convention du Conseil de l'Europe.

156 Si ce contrôle est permis entre Etats contractants à la Convention, nous considérons qu'il est *a fortiori* permis dans le contexte du Protocole additionnel, vis-à-vis des Etats tiers. Le Protocole interdit d'autoriser les flux lorsqu'il n'y a pas garantie d'une protection adéquate dans l'Etat destinataire. Il n'interdit pas de prohiber certains flux spécifiques de données même lorsque l'Etat tiers destinataire garantit une protection adéquate.

Le système de règles mis en place présente ainsi une complexité, somme toute, relative. Mais il convient d'ajouter qu'au-delà de ce que prévoient les dispositions exposées, la Convention n°108 et son Protocole *n'encadrent pas l'incidence que pourrait avoir l'applicabilité du droit d'un Etat contractant, plutôt que celle d'un autre Etat, à un traitement de données à caractère personnel*. Cette remarque est valable tant dans le contexte des FTD à destination d'Etats tiers, que dans celui des FTD à destinations d'autres Etats contractants. Au sujet de ces derniers, le rapport explicatif de la Convention (§ 10) reconnaît ainsi qu' « il est parfois difficile de déterminer quel Etat a juridiction et quelle loi nationale est applicable », soulignant que « le «noyau dur» [de la Convention] aboutira à une harmonisation des lois entre les Parties et, par conséquent, comportera une diminution des possibilités de conflits de lois ou de juridiction » (§ 20). Ainsi, **la Convention n°108 et son Protocole** n'éliminent pas ces conflits ; ils **ne déterminent ni le droit applicable en matière de protection des données, ni les juridictions compétentes pour trancher les litiges en cette matière**. Or l'éclatement du contexte des technologies précédemment évoqué, renforce l'importance de ces règles. En ces matières – droit applicable et juridiction compétente –, c'est l'ordre juridique de l'Union européenne qui paraît le plus avancé quant à son harmonisation.

13.3. DROIT APPLICABLE A LA PROTECTION DES DONNEES : ARTICLE 4 DE LA DIRECTIVE 95/46 ET REGLEMENT 864/2007 (« ROME II »)[157]

En matière de droit applicable à la protection des données, l'article 4 de la directive 95/46 constitue la disposition allant le plus loin quant à l'harmonisation des règles déterminant quel droit de la protection des données est applicable à un traitement de données à caractère personnel[158]. Cette disposition détermine les hypothèses dans lesquelles les Etats membres doivent appliquer leur droit national. Elle détermine, en combinaison avec les articles 25 et 26 régissant les FTD, l'applicabilité spatiale de la protection européenne des données[159].

Toutefois premièrement, elle ne détermine, *a priori, que* les hypothèses où les Etats membres *doivent* appliquer leur législation nationale. Autrement dit, si un Etat membre n'est pas tenu d'appliquer son droit national, la directive ne détermine pas quel droit il doit appliquer. Sauf à l'interpréter comme consacrant une véritable règle bilatérale de conflit de loi désignant quel droit, de l'ordre juridique de l'Union européenne est applicable à une situation donnée. Ou sauf à appliquer un raisonnement unilatéraliste. Etant entendu que dans ces deux cas, ne seraient désignés que les droits applicables dans les hypothèses couvertes par le champ d'application spatial de la directive 95/46[160].

---

157 Règlement (CE) n°864/2007 du Parlement Européen et du Conseil du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles (Rome II), *JO* L 199 du 31.7.2007.

158 A propos du droit applicable à la protection des données et, en particulier, de l'article 4 de la directive 95/46, voy. not. C. KUNER, « Data Protection Law and International Jurisdiction on the Internet (Part 1) », *International Journal of Law and Information Technology*, 2010, n°18 (2), pp. 176-193 ; C. KUNER, « Data Protection Law and International Jurisdiction on the Internet (Part 2) », *International Journal of Law and Information Technology*, 2010, n°18 (3), pp. 227-247 ; J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *Revue Européenne de Droit de la Consommation*, 2010, n°2, pp. 255-270; F. RIGAUX, « Libre circulation des données et protection de la vie privée dans l'espace européen », in *La protection de la vie privée dans la société de l'information, L'impact des systèmes électroniques*, P. Tabatoni (dir.), t. 2, P.U.F., Paris, 2000, pp. 25-40 .

159 Au sujet de la détermination de son applicabilité territoriale par le droit communautaire dérivé, v. S. FRANCQ, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, Bruylant, L.G.D.J., Bruxelles, Paris, 2005.

160 Dans ce cas, pour les situations relevant du champ d'application spatial de la directive 95/46, celle-ci déterminerait *in fine* pour chaque opération de traitement quel droit est applicable. Si cette disposition est

Quid alors de l'éventuelle applicabilité des droits nationaux au-delà des hypothèses exclues du champ spatial de la directive 95/46 ? Comme le relève le Groupe 29 : « certaines situations ne relèvent pas du champ d'application de la directive. C'est le cas lorsque les activités de responsables du traitement des données établis en dehors de l'UE concernent des résidents de l'UE, ce qui donne lieu à la collecte et à un traitement supplémentaire de données à caractère personnel. C'est le cas par exemple des commerçants en ligne et d'autres fournisseurs qui utilisent des publicités «couleur locale», des sites web qui *ciblent directement* les citoyens de l'UE (dans leur langue notamment). Si ces activités sont menées sans utiliser d'équipements installés dans l'UE, la directive 95/46/CE ne s'applique pas »[161] (italique ajouté par nous). *Quid* du rôle du droit national dans ces cas ?

Deuxièmement, selon les traitements de données et selon les établissements du responsable de traitement, un même responsable de traitement pourrait être tenu de respecter différents droits nationaux. Son application peut donc se révéler complexe. Par ailleurs, les éléments de rattachement pris en compte, à savoir le critère d'utilisation de moyens (équipements) sur le territoire de la Communauté aux fins du traitement en question, et le lieu d'établissement dans le cadre des activités duquel a lieu le traitement concerné, causent des difficultés d'interprétation et d'application majeures dans le contexte éclaté exposé à titre introductif. L'on lira ainsi dans une étude récente commandée par la Commission européenne que les « règles de l'article 4(1)(a) sont tout simplement confuses et impossibles à appliquer dans le nouvel environnement technique mondial »[162]. Par ailleurs, la prise en compte de la localisation des équipements utilisés aux fins de traitement ne s'avère pas nécessairement pertinente au regard de l'évolution technologique[163]. Et l'étude de poursuivre : « les dispositions de la directive relatives au droit applicable sont effectivement impossibles à appliquer aux entreprises et aux organisations de pays tiers qui exercent leurs activités en Europe (en particulier si elles sont actives sur l'Internet – comme elles le sont, ou le seront, certainement presque toutes) »[164].

Troisièmement enfin, et ce point est lié au précédent, la mise en œuvre de l'article 4 de la directive 95/46 dépend *in fine* de sa transposition par les Etats membres. L'article 4 de la directive 95/46 ne résout donc pas intégralement la question du droit applicable à la protection des données au sein de l'ordre juridique de l'Union européenne.

---

transposée à la lettre, évidemment *mutatis mutandis*, par les Etats membres, en principe, chaque traitement relevant de son champ d'application spatial devrait alors être soumis au droit d'un seul Etat membre (e.g. le droit de l'Etat sur le territoire duquel est établi l'établissement du responsable de traitement dans le cadre des activités duquel (établissement) est réalisé le traitement de données à caractère personnel). Il serait logique, en raison de l'harmonisation opérée par la directive 95/46, que les Etats membres reconnaissent mutuellement leurs réglementations en la matière. Il faut toutefois noter que cette harmonisation n'empêche pas les divergences entre législations nationales, eu égard à la marge de manœuvre laissée aux Etats membres par la directive 95/46. Cela est bien entendu d'autant plus vrai en ce qui concerne les Etats parties à la Convention n°108.

161 Groupe 29, WP 168, L'avenir de la protection de la vie privée, Contribution conjointe à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel, adoptée 1er décembre 2009, pp. 10-11.

162 LRDP Kantor Ltd, en association avec Centre for Public Reform, « Etude comparative sur les différentes approches des nouveaux défis en matière de protection de la vie privée, en particulier à la lumière des évolutions technologiques, Rapport final », disponible sur http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_fr.pdf, janvier 2010, p. 29, n°37.

163 Par exemple, dans le cadre du *cloud computing*, la localisation des moyens de traitement (en particulier les ressources de mémoire et de calcul) peut être dictée, en temps réel, par la recherche d'une efficacité optimale du service et de la meilleure allocation des ressources informatiques du prestataire de service.

164 LRDP Kantor Ltd, en association avec Centre for Public Reform, *op. cit.*, p. 30, n°39.

Il est intéressant de relever que la protection des données ne suit pas ici les mêmes règles de détermination du droit applicable que la vie privée elle-même – notamment consacrée par l'article 8 CEDH[165]. Le droit applicable aux obligations non contractuelles découlant d'une atteinte au droit fondamental à la vie privée n'est d'ailleurs pas non plus déterminé par le règlement « Rome II », déterminant la loi applicable aux obligations non contractuelles[166]. Autrement dit, c'est le droit national des Etats membres qui répond à cette question. Par exemple en Belgique, dans la lignée de la logique unilatéraliste adoptée dans la directive, la loi vie privée détermine unilatéralement son champ d'application territorial, tandis que le Code belge de droit international privé, au moyen d'une règle multilatérale – désignant, en toutes hypothèses le droit applicable (étranger ou belge) –, définit quel droit régit une obligation résultant d'une atteinte à la vie privée[167]. Autrement dit théoriquement, l'identification d'une atteinte à la vie privée se fondant sur l'effet horizontal (en tous cas indirect) de l'article 8 CEDH et sa réparation pourraient être régies par le droit d'un Etat membre de l'Union européenne, tandis que les aspects relatifs à la protection des données seraient quant à eux soumis à l'application du droit d'un Etat tiers à l'UE. De même, la relation contractuelle entre un consommateur – personne concernée – et un prestataire de service – responsable de traitement – pourrait être régie par le droit de l'Etat de résidence habituelle du consommateur[168] tandis que les aspects relatifs à la protection des données pourraient l'être par le droit d'un Etat tiers à l'Union européenne.

Finalement, au sein même d'un espace où les droits sont *a priori* harmonisés et où les Etats se doivent reconnaissance mutuelle de leurs législations, la question du droit applicable en matière de protection des données demeure complexe et ne garantit pas nécessairement la sécurité juridique, au préjudice des personnes concernées et des responsables de traitement. Cela est d'autant plus vrai au sujet des relations entre Etats parties à la Convention n°108, mais encore entre Etats parties à la CEDH. Il est d'ailleurs désormais utile de souligner le rôle potentiel que pourrait jouer l'article 8 CEDH quant aux règles déterminant le droit applicable en matière de protection des données et de vie privée.

13.4. L'INCIDENCE DE L'ARTICLE 8 CEDH SUR LA DETERMINATION DU DROIT APPLICABLE EN MATIERE DE VIE PRIVEE ET DE PROTECTION DES DONNEES

Avant tout, il convient de rappeler les liens juridiques évoqués *supra* (cf. le point 1.1.1. de ce rapport) existant entre protection des données et vie privé. La Cour européenne des droits de l'homme a reconnu, à plusieurs reprises, l'application de l'article 8 CEDH au traitement de données à caractère personnel[169], se référant d'ailleurs à la Convention n°108. Ce qui présente un double

---

165 Il peut être relevé que, dans une certaine mesure – car la protection des données ne se limite pas à sauvegarder la vie privée –, la réglementation protégeant les personnes contre le traitement de données à caractère personnel procède à l'horizontalisation de l'article 8 CEDH. Voy. infra quant à l'éventuelle incidence de l'article 8 CEDH sur les règles de droit international privé.

166 Voy. article 1er, § 2, g), du règlement "Rome II".

167 Voy. article 99 de la loi du 16 juillet 2004, portant le Code de droit international privé, *Monit.B.* du 27 juillet 2004, et l'article 3 bis de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *Monit.B.* du 18 mars 1993.

168 Voy. article 6 du Règlement (CE) n o 593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles (Rome I), *JO* L 177 du 4.7.2008 ; J.-P. Moiny et B. De Groote, « 'Cyberconsommation' et droit international privé », *Revue du Droit des Technologies de l'Information*, 2009, n°37, pp. 5-37.

169 V. not. Cour eur. D.H., 16 février 2000, *Amann c. Suisse*, no 27798/95, 16 février 2000 ; Cour eur. D.H., 4 mai 2000, *Rotaru c. Roumanie*, no 28341/95 ; Cour eur. D.H., 31 mai 2005, *Antunes Rocha c. Portugal*, n°64330/01 ; Cour eur. D.H., 10 octobre 2006, *LL c. France*, n°7508/02 ; Cour eur. D.H., 4 décembre 2008, *Marper v. Royaume-Uni*, n°30562/04 et 30566/04 ; Cour eur. D.H., 2 septembre 2010, *Uzun c. Allemagne*, n°35623/05.

intérêt. D'une part principalement, cela implique que la Cour EDH peut être amenée à sanctionner le comportement d'un Etat partie à la CEDH pour des raisons liées à la réglementation du traitement des données à caractère personnel. Alors que l'application de la Convention n°108 et de son protocole ne relève pas de la compétence de la Cour. Il faut également noter que le Traité de Lisbonne prévoit que l'Union européenne doit adhérer à la CEDH[170], ce qui renforce le rôle de la Cour EDH vis-à-vis de l'Union européenne[171] dont les actes pourraient dès lors être contestés devant ladite Cour. D'autre part, cela implique que les Etats n'ayant pas encore signé et/ou ratifié ces instruments demeurent néanmoins tenus, sur la base de l'article 8 CEDH, à des règles en matière de traitement de données à caractère personnel.

Ainsi, la Cour EDH, en application de l'article 8 CEDH, pourrait être amenée à contrôler[172] – et le cas échéant sanctionner – un Etat en raison de l'application par une de ses juridictions, dans un cas particulier, d'un droit étranger, à l'occasion de laquelle l'article 8 CEDH aurait été méconnu au préjudice de l'individu litigant concerné[173] – individu « relevant de la juridiction » de l'Etat au sens de l'article 1er CEDH[174]. « Dès que l'Etat exerce ses compétences, […], il doit agir en conformité avec la Convention »[175]. Dans ce type d'hypothèse, le droit étranger pourrait être écarté via le jeu d'un mécanisme du type exception d'ordre public. Logiquement, si ce « droit étranger » est le droit d'un autre Etat du Conseil de l'Europe, le jeu de cette exception devrait être limité (*a fortiori* si ledit Etat est également partie à la Convention n°108, et encore à plus forte raison si les Etats sont membres de l'Union européenne). C'est principalement lorsque serait en cause un Etat tiers à la Convention n°108 ne garantissant pas une protection adéquate que le jeu d'une telle exception serait requis. Dans ces hypothèses on imagine que le « noyau dur » de la Convention n°108 du Conseil de l'Europe devrait être appliqué au litige en question, sous peine, le cas échéant, d'encourir la sanction de la Cour européenne des droits de l'homme, susceptible de juger que le noyau dur de la Convention n°108 est garanti sur la base de l'article 8 CEDH. Il en irait alors de même pour toutes les règles de protection des données dégagées par la Cour sur la base de l'article 8.

13.5. CONCLUSION : UNE REGLE DETERMINANT LE DROIT APPLICABLE DANS LA CONVENTION 108 ?

L'objectif de la Convention n°108 est « de garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement

---

170 « L'Union adhère à la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales. Cette adhésion ne modifie pas les compétences de l'Union telles qu'elles sont définies dans les traités » (article 6, § 2, du Traité sur l'Union européenne). Les pourparlers d'adhésion ont commencé le 7 juillet 2010, voy. http://www.coe.int/t/dc/files/themes/eu_and_coe/default_FR.asp?.

171 Voy. Assemblée parlementaire, Commission des questions juridiques et des droits de l'Homme, M.-L. Bemelmans-Videc (rapporteuse), « Adhésion de l'Union européenne/Communauté européenne à la Convention européenne des Droits de l'Homme », 18 mars 2008, disponible sur http://assembly.coe.int/Documents/WorkingDocs/Doc08/FDOC11533.pdf, p. 8, n°12.

172 Au sujet de ce contrôle, v. not. P. MAYER, "La Convention européenne des droits de l'homme et l'application des normes étrangères", *Rev. crit. dr. internat. privé*, 1991, p. 664.

173 En ce qui concerne l'influence de la CEDH sur les règles de conflits de loi, voy. not. L. GANNAGÉ, "A propos de l' "absolutisme" des droits fondamentaux", in *Vers de nouveaux équilibres entre ordres juridiques – Liber amicorum Hélène Gaudemet-Tallon*, Paris, Dalloz, 2008, pp. 265-284.

174 A ce sujet, voy. les développements de S. KARAGIANNIS, « Le territoire d'application de la convention européenne des droits de l'homme, *Vaetera et nova* », *Rev. trim. dr. h.*, n°61, 2005, pp. 33-120. Voy. not. Cour eur. D.H., 23 mars 1995, *Loizidou c.Turquie* [GC], n°15318/89 ; Cour eur. D.H., 12 décembre 2001, *Bankovic et al. c. Belgique et al.* [décision GC], n°52207/99 ; plus récemment, Cour eur. D.H., 29 mars 2010, *Medvedyev et al. c. France* [GC], n°3394/03.

175 G. COHEN-JONATHAN et J.-F. FLAUSS, « Cour européenne des droits de l'homme et droit international général », *Annuaire français de droit international*, n°47, 2001, p. 438.

automatisé des données à caractère personnel la concernant » (article 1er de la Convention). C'est ce qu'elle fait en garantissant un cadre commun minimal de droit matériel de la protection des données qui, le cas échéant selon ce qui a été exposé précédemment, peut connaître certaines lacunes. Sans aucun doute, les développements précédents ont démontré la complexité des questions de droit international privé se posant en la matière, en particulier quant aux questions de droit applicable.

Bien entendu, des règles communes de droit international privé contribueraient à l'objectif précité. D'une part, elles augmenteraient la sécurité juridique et, par là, contribueraient certainement à une meilleure effectivité, en pratique, des règles matérielles[176]. Clairement, un manque de clarté quant aux règles de droit applicables est susceptible de préjudicier à l'application effective des règles matérielles de droit, en compliquant substantiellement – peut-être excessivement – la vie des entreprises. Ainsi, au sein de l'Union européenne, dont la réglementation poursuit l'établissement d'un marché unique, une règle commune est d'autant plus nécessaire.

D'autre part, devant une juridiction nationale, une lacune pourrait apparaître dans la protection des individus si le juge était amené à appliquer un droit étranger moins protecteur (protection non adéquate). Dans un telle hypothèse, un mécanisme du type de l'exception d'ordre public permettrait d'éviter, *in casu* devant les juridictions nationales, que l'application d'une règle étrangère ne prive un individu de tout ou partie du « noyau dur » de la Convention n°108, ou des droits garantis sur la base de l'article 8 CEDH.

Toutefois deux difficultés majeures se posent quant à l'éventuelle définition de règles déterminant le droit applicable dans le contexte de la Convention n°108. D'une part, est-il *politiquement* envisageable que les Etats du Conseil de l'Europe s'accordent sur l'adoption d'une telle règle ? Relevons d'abord qu'à l'occasion de l'adoption de la Déclaration de Madrid, il n'y a pas eu d'accord sur les questions de droit international privé et que, en toutes hypothèses, l'adoption d'une telle règle nécessite une coordination avec l'Union européenne. Les divergences entre les législations matérielles des Etats parties à la Convention sont en tous cas susceptibles de causer des difficultés à cet égard.

D'autre part, la multiplicité des situations, des acteurs et des matières juridiques en cause à l'occasion d'un litige en matière de protection des données compliquent la tâche quant à l'établissement de règles régissant les questions de droit international privé. Probablement, en matière de droit applicable, une règle prévoyant des rattachements subsidiaires pourrait être utile. Cette règle devrait, notamment, prendre en compte la diversité des ordres juridiques en cause (européen, Conseil de l'Europe – CEDH –, Conseil de l'Europe – Convention n°108 et protocole additionnel –, international « au sens large » – relation avec les Etats tiers). Un instrument tel que la Convention n°108 se doit d'être suffisamment souple pour permettre aux Etats (et à leurs organes) d'appréhender le triple éclatement identifié à titre introductif, et d'y opérer judicieusement l'arbitrage entre droits, libertés et intérêts des individus seuls, tout en considérant l'intérêt de la société au sens large. Dans tous les cas, le juge national doit disposer des outils nécessaires à l'appréhension de situations pouvant être très différentes, et c'est en principe à lui qu'incombera, *in casu,* le travail interprétatif des règles, quelle que soit leur origine (le cas échéant, sous le contrôle d'un juge international – CJUE ou Cour EDH quant à l'application de l'article 8 CEDH). Ce sont donc ici, plus fondamentalement, les faisabilités *théorique et pratique* de l'établissement d'une règle commune de désignation du droit applicable en matière de protection des données qui sont en cause.

---

176 Au niveau de l'Union européenne, au sujet de l'article 4 de la directive 95/46, l'on a récemment relevé que, pour les entreprises et organisations actives au niveau international, « il est de plus en plus difficile pour elles de se conformer aux règles et principes relatifs à la protection des données[, c]es problèmes [étant] décuplés dans le nouvel environnement sociotechnique internationalisé, et surtout (mais pas seulement) pour ce qui concerne l'Internet », LRDP Kantor Ltd, en association avec Centre for Public Reform, *op. cit.*, p. 30, n°42.

Eu égard à l'ensemble des considérations précédentes, **on peut s'interroger sur le fait que l'absence de règles définissant le droit applicable en matière de protection des données constitue une lacune de la Convention n°108** ; le droit international privé des Etats membres est appelé à régir cette question. Plus les législations des Etats se rapprochent, moins les conséquences liées au jeu de ces règles sont importantes. A ce sujet, il peut être rappelé une fois de plus que des Etats non membres du Conseil de l'Europe peuvent adhérer à la Convention n°108 (article 23) et, ensuite, au protocole additionnel (article 3, § 2). Dans tous les cas, un droit sera toujours, *in fine,* déclaré applicable en cas de litige, par le juge. Mais un débat quant aux règles déterminant le droit applicable en matière de protection des données n'en est pour autant pas moins utile et même indispensable : aux fins d'une part, d'assurer aux individus une meilleure effectivité de leur protection et, d'autre part, de renforcer la sécurité juridique du point de vue des responsables de traitement. A cet égard, une **recommandation du Comité des Ministres** du Conseil de l'Europe pourrait à tout le moins opportunément enrichir le débat et être utile dans une recherche d'harmonisation des dispositions portant sur le droit applicable.

Au terme de ces développements, il est important d'apporter un élément de réflexion non directement lié à la question du droit applicable mais qui pourrait avoir incontestablement un impact sur cette question. Il s'agit de considérer la **possibilité de préciser au sein même de la Convention 108 que celle-ci ou à tout le moins certaines de ses dispositions (clairement indiquées) ont un effet direct leur permettant d'être directement invoquées devant les juridictions nationales**.[177] Il conviendrait dans ce cas de tenir compte des conditions habituellement admises pour reconnaître un effet direct à des dispositions contenues dans un instrument international.

13.6. ELEMENTS ADDITIONNELS SUR LES FLUX TRANSFRONTIERES DE DONNEES

Au-delà de ce qui a été dit sur les flux transfrontières aux paragraphes précédents, il s'indique d'ajouter les éléments suivants :

Dans le nouvel environnement technologique, **il est indispensable de clarifier ce que l'on entend par FTD**. Il importe notamment de spécifier si la notion de « transfert » qui est utilisée à l'article 2 du Protocole additionnel[178] couvre la mise à disposition d'une donnée, sa diffusion, sa publication. Cette précision est cruciale pour ce qui concerne la mise à disposition de données sur un site Internet[179].

---

[177] Il est à noter que la principauté d'Andorre reconnait déjà aujourd'hui un effet direct à la Convention 108. Cela a notamment permis de combler certaines lacunes de la législation de cet Etat en matière de protection des données à caractère personnel. C'est en prenant en compte cet effet direct que le Groupe de l'article 29 a reconnu qu'Andorre offrait un niveau de protection des données adéquat. Cf. Groupe de l'article 29, Avis 7/2009 sur le niveau de protection des données à caractère personnel dans la Principauté d'Andorre, WP 166, 1er décembre 2009, disponible à l'adresse http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp166_fr.pdf

[178] « Chaque Partie prévoit que le transfert de données à caractère personnel vers un destinataire soumis à la juridiction d'un Etat ou d'une organisation qui n'est pas Partie à la Convention ne peut être effectué que si cet Etat ou cette organisation assure un niveau de protection adéquat pour le transfert considéré. »

[179] V. l'affaire Lindqvist tranchée par la C.J.C.E qui a été l'occasion de discussion sur la notion de transfert dans le contexte d'Internet et qui a conduit à une réponse maladroite de la Cour de Justice sur ce point : C.J.C.E., 6 novembre 2003, (Lindqvist), C-101-01, *Rec*. p. I-12971. Pour une critique de cet arrêt, v. C. de TERWANGNE, « Arrêt Lindqvist ou quand la Cour de Justice des Communautés européennes prend position en matière de protection des données personnelles », note sous C.J.C.E., 6 novembre 2003, *R.D.T.I*., 2004, n° 19, pp. 67 et s.

L'article 2 du Protocole additionnel[180] adopte le concept de « protection adéquate » comme critère pour l'acceptation d'un flux transfrontières. Sans doute serait-il utile d'ajouter que **la détermination du caractère adéquat suppose une interprétation évolutive** dans la mesure où l'adéquation se constate non pas une fois pour toutes mais en fonction des interprétations données à la Convention par la jurisprudence de la Cour de Strasbourg et des réglementations nouvelles prises (recommandations, protocoles additionnels).

Le Rapport explicatif du Protocole additionnel apporte cette précision concernant l'évaluation du caractère adéquat : « 27. Le niveau de la protection devrait être évalué au cas par cas et pour chaque transfert ou catégorie de transfert effectué. […] 28. Une appréciation du caractère adéquat peut toutefois être faite pour l'ensemble d'un Etat ou d'une organisation permettant ainsi tous les transferts de données vers cette destination. Dans ce cas, le niveau adéquat de protection est déterminé par les autorités compétentes de chaque Partie. » Il conviendrait **d'être complet sur le niveau où a lieu l'évaluation du caractère adéquat** de la protection d'un Etat tiers. C'est au niveau des « autorités compétentes » pour les évaluations globales mais rien n'est dit pour ce qui concerne les évaluations au cas par cas.

14. Autorités de contrôle

Un bilan mitigé a pu être récemment dressé sur les autorités de protection des données mises en place:

« Les DPA ont une excellente connaissance de la législation, et elles donnent des conseils très utiles à ce sujet, mais elles ne sont pas très efficaces en termes d'exécution: le «contrôle» de la conformité aux lois sur la protection des données par les DPA est généralement déficient et inefficace. »[181]
« Ce rapport comparatif met en évidence les principales failles du système actuel de protection des données à caractère personnel dans les 27 États membres de l'UE. Des lacunes ont été observées en termes de manque d'indépendance, de ressources adéquates et de pouvoir de certaines des autorités chargées de la protection des données. »[182]

Il conviendrait sans doute de **tirer des leçons de tels constats et d'envisager si des réponses sur le plan législatif pourraient corriger la situation**, **notamment en énonçant les critères garantissant l'indépendance des autorités**. Il s'indiquerait aussi peut-être de **compléter** les compétences de telles autorités, en leur attribuant par exemple une **compétence d'avis, obligatoire ou non, lors de l'élaboration de toute norme ayant une incidence sur la vie privée**.

La Déclaration de Madrid pour sa part réaffirme la nécessité « d'autorités indépendantes de protection des données, rendant des décisions, dans le contexte d'un cadre juridique, de manière transparente et sans aucun avantage commercial ou influence politique ». La Résolution de Madrid est plus précise sur les caractéristiques que devraient présenter de telles autorités (Article 23, § 2).

Le Contrôleur européen à la protection des données tire lui aussi des conclusions quant à la situation actuelle : « Les défis nouveaux en matière de protection des données nécessitent un contrôle renforcé, plus uniforme et efficace. En conséquence, il conviendrait que le nouveau cadre garantisse l'uniformité des normes en ce qui concerne l'indépendance, les pouvoirs réels, le rôle consultatif de ces autorités dans le processus législatif et leur capacité à définir leur propre programme de travail,

[180] « Chaque Partie prévoit que le transfert de données à caractère personnel vers un destinataire soumis à la juridiction d'un Etat ou d'une organisation qui n'est pas Partie à la Convention ne peut être effectué que si cet Etat ou cette organisation assure un niveau de protection adéquat pour le transfert considéré. »

[181] LRDP Kantor Ltd, en association avec Centre for Public Reform, *op. cit.*, p. 52, § 104.

[182] Comparative Legal Study on assessment of data protection measures and relevant institutions, rapport commandé par l'Agence des droits fondamentaux (FRA) de l'Union européenne, Synthèse, 2009, para. 8.

notamment par la définition de priorités en matière de traitement des plaintes. Il conviendrait que la coopération internationale entre les autorités chargées de la protection des données soit pareillement renforcée. »[183]

La réflexion pourrait aussi porter sur **l'opportunité d'introduire la catégorie des « officiers de protection de données »**, à côté des autorités de contrôle. Ces officiers serviraient de relais de ces autorités au sein même des organisations, institutions, entreprises, etc. De la sorte ils pourraient peut-être être les garants d'un meilleur respect des principes et règles de protection des données au sein de leur organisme.

Enfin, de toutes part on réclame que **soit prévu un renforcement du dialogue et de la coopération internationale, entre les autorités de contrôle notamment**.

Dans sa Recommandation de l'OCDE relative à la coopération transfrontière dans l'application des législations protégeant la vie privée du 12 juin 2007, l'OCDE recommande que « Les pays Membres coopèrent au-delà des frontières pour faire appliquer les lois protégeant la vie privée, en prenant des mesures appropriées pour :

- Améliorer leurs cadres nationaux pour l'application des lois sur la vie privée afin que leurs autorités puissent mieux coopérer avec les autorités étrangères.
- Elaborer des mécanismes internationaux efficaces destinés à faciliter la coopération transfrontière pour l'application des lois sur la vie privée.
- Se prêter mutuellement assistance dans la mise en application des lois protégeant la vie privée, notamment par des actions telles que la notification, la transmission des plaintes, l'entraide pour les enquêtes et l'échange d'information, assorties de garanties appropriées.
- Associer les parties prenantes intéressées aux discussions et activités visant à développer la coopération dans l'application des lois protégeant la vie privée. »

Dans le même sens, la Résolution de Madrid consacre un article très complet à l'établissement et l'amélioration de la coopération et de la coordination entre les autorités de contrôle dans le but de réaliser une protection plus uniforme (Article 24).

[183] P. Hustinx (CEDP), «30 ans après: l'impact des Lignes directrices de l'OCDE sur la protection de la vie privée», Table ronde conjointe PIIC-GTSIVP, Paris, le 10 mars 2010, Session 3: Les Lignes directrices sur la protection de la vie privée dans le monde actuel, disponible à l'adresse http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2010/10-03-10_Privacy_guidelines_FR.pdf