

Master 2 Professionnel, Droit et Pouvoirs Publics  
Droit des Nouvelles Technologies et Société de l'Information



## Mémoire

*« Quels enjeux juridiques pour le transfert d'une base  
de données vers un autre pays ? »*

Anne-Gaëlle LEFEBVRE

Année Universitaire 2008 - 2009

# Sommaire :

<b>Introduction :</b> .....	<b>5</b>
<b>TITRE I : Le transfert de données entrant dans le champ d'application de la Directive.....</b>	<b>10</b>
<b>CHAPITRE I : Etendue de la protection des données conférée par la Directive de 1995.....</b>	<b>10</b>
<b>Section I : Les grands principes applicables aux transferts. ....</b>	<b>11</b>
<i>A : L'origine des données.....</i>	<i>11</i>
<i>B :La déclaration préalable du traitement.....</i>	<i>12</i>
<i>1 : La déclaration du traitement auprès de la CNIL.....</i>	<i>13</i>
<i>2 : Légitimation de la mise en place d'un système de traitement de données....</i>	<i>14</i>
<i>3 : La nomination d'un CIL au sein de l'organisation.....</i>	<i>15</i>
<b>Section II : Le transfert vers les pays de l'Union Européenne et de l'EEE. ..</b>	<b>17</b>
<i>A : Transposition de la directive en droit interne.....</i>	<i>17</i>
<i>B : Le contrôle effectif de la protection des données.....</i>	<i>19</i>
<i>1 : Création de commissaires nationaux pour la protection des données. ....</i>	<i>19</i>
<i>2 : Le groupe dit « article 29 ».....</i>	<i>20</i>
<b>CHAPITRE II :Le transfert vers des pays tiers à l'Union Européenne. ....</b>	<b>22</b>
<b>Section I :Les pays bénéficiant d'une protection adéquate.....</b>	<b>22</b>
<i>1 : Les pays ayant reçu l'aval de la commission.....</i>	<i>23</i>
<i>2 : Activité Internationales de ces pays.....</i>	<i>24</i>
<i>B : Le cas spécifique du Canada.....</i>	<i>25</i>

<b>Section II : Les autres pays tiers à l'Union Européenne .....</b>	<b>27</b>
1 : La procédure devant la CNIL .....	27
2 : Le contrat de flux transfrontalier de données.....	28
3 : Les règles internes d'entreprises. ....	30
<b>B : Le cas des Etats-Unis.....</b>	<b>31</b>
1 : La reconnaissance par la commission des « safe harbor principles ».....	31
2 : Une protection efficace ?.....	33
<b>C : Les dérogations autorisant le transfert vers un pays tiers n'assurant pas un niveau adéquat de protection.....</b>	<b>34</b>
1 : Utilisation des dérogations.....	34
2 : Interprétation stricte des dérogations.....	35
3 : L'autorisation de la personne pour le transfert .....	35

**TITRE II : Les données exclues du champ d'application de la Directive.....37**

**CHAPITRE I : Les données contenues dans les grands fichiers de police..... 37**

**Section I : Les grands fichiers de police européens.....37**

<b>A : Présentation.....</b>	<b>38</b>
1 : Système d'Information Schengen (SIS).....	38
2 : EURODAC .....	39
3 : VIS .....	40
4 : EUROPOL .....	40
<b>B : Modalités de Transferts.....</b>	<b>41</b>

**Section II : Les fichiers de police nationaux .....**

<b>A : Présentation des spécificités des fichiers de police nationaux.....</b>	<b>42</b>
--	-----------

<i>B : La procédure applicable aux données qu'ils contiennent. ....</i>	<i>43</i>
<b>CHAPITRE II : Les données « PNR ».....</b>	<b>44</b>
<b>Section I : Présentation des données « PNR ».....</b>	<b>44</b>
<i>A : Définition et catégories de données.....</i>	<i>44</i>
<i>B : Appartenance au troisième pilier.....</i>	<i>45</i>
<b>Section II : Les différents accords pour leur transfert.....</b>	<b>48</b>
<i>A : La décision de la Commission Européenne en date du 14 et 29 mai 2004. ....</i>	<i>48</i>
<i>B : L'accord actuel : Décision de la Commission en date du 26 juillet 2007.....</i>	<i>50</i>
<b>Bibliographie :.....</b>	<b>52</b>
<b>Webographie :.....</b>	<b>54</b>
<b>Annexe A : Extrait de la loi Informatique et Libertés du 6 janvier 1978. .....</b>	<b>55</b>
<b>Annexe B : Extrait de la Directive européenne du 24 Octobre 1995. ....</b>	<b>62</b>
<b>Annexe C : Les « safe Harbor principles ».....</b>	<b>65</b>

## **Introduction :**

Aujourd'hui, dès que nous « surfons » sur internet nous sommes appelés à répondre à toutes sortes de questions nous concernant. Ces questions vont du simple pseudo, à notre adresse complète. Ces renseignements peuvent même permettre de faire le profil complet d'une personne s'ils sont divulgués. C'est tout le problème de la protection des données.

Leur collecte peut s'avérer indispensable : comment envoyer un colis à une personne si on n'a pas le droit de collecter son adresse, comment contrôler la sécurité d'une entreprise si on ne peut pas mettre dans une base de données les informations la concernant afin de ne laisser entrer à l'intérieur que les personnes autorisées ? Mais d'un autre côté, ces données peuvent permettre l'identification d'une personne directement ou indirectement, elles peuvent aussi apporter des informations précieuses sur ces personnes qui peuvent ainsi conduire à des discriminations ou avoir une forte incidence sur leur vie privée.

Il faut donc réussir à conjuguer, la volonté de sécurité qui est de plus en plus présente aujourd'hui dans notre société et en même temps le droit au respect de la vie privée auquel tout être humain peut prétendre. Ce droit au respect de sa vie privée est aujourd'hui affirmé par l'ensemble des conventions internationales concernant les droits de l'homme. Il est notamment présent dans la Convention Européenne de Sauvegarde des Droits de l'Homme et des libertés fondamentales (CESDH) en son article 8<sup>1</sup>.

---

<sup>1</sup> Article 8 de la CESDH : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

L'affirmation de ce droit dans la CESDH a bien sûr des conséquences en Europe sur la protection qui va être apportée aux données personnelles. La collecte de ces données n'est pas interdite, elle est simplement réglementée. A cette réglementation, plusieurs garde-fous sont apportés : c'est le cas de la CNIL<sup>2</sup> en France, ou encore du Contrôleur européen à la protection des données personnelles.

Le premier texte à s'être intéressé au sort des données personnelles est la Convention 108 prise dans le cadre du Conseil de l'Europe en date du 28 janvier 1981. Elle met en place certaines règles très légères en matière de protection des données personnelles. Ce sont en fait des grands principes visant à garantir le respect des droits fondamentaux et notamment le droit à la vie privée lors du traitement des données personnelles.

Aujourd'hui, les deux grands textes législatifs, sur lesquels est fondée la protection des données personnelles en France, sont d'une part la Directive européenne du 24 octobre 1995<sup>3</sup> du Parlement Européen et d'autre part la loi « Informatique et Libertés » du 6 janvier 1978<sup>4</sup> telles que modifiées par la loi de transposition de la directive de 1995 en date du 6 août 2004<sup>5</sup>. Ces deux grands textes visent à protéger l'utilisateur de l'outil informatique et instaure une protection des libertés fondamentales sur Internet.

C'est d'ailleurs bien avant les recommandations de l'Union Européenne et la directive de 1995, que la CNIL fût créée. Si une réelle protection des données personnelles n'est effective que depuis 1995 en Europe et 2004 en France, la CNIL a été créée par la loi du 6 janvier 1978. C'est une autorité administrative indépendante. Elle fait l'objet du Chapitre III de cette même loi. Elle possède différentes missions qui sont définies à l'Article 11<sup>6</sup> de cette même loi. Voici l'une de ses missions : « Elle donne un avis sur la conformité aux dispositions de la présente loi des projets de règles professionnelles et des produits et

---

<sup>2</sup>CNIL : Commission Nationale de l'Informatique et des Libertés

<sup>3</sup> Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données :

<sup>4</sup> Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés :

<sup>5</sup> Loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés :

<sup>6</sup> Voir Annexe A

procédures tendant à la protection des personnes à l'égard du traitement de données à caractère personnel, ou à l'anonymisation de ces données, qui lui sont soumis ».

Tout d'abord, il convient de déterminer ce qu'est une donnée personnelle. La directive de 1995 en donne une définition dans son article 2 (a). Cette définition a ensuite été reprise par la loi du 6 août 2004 qui modifie la loi Informatique et Libertés et qui dans son article 2 alinéa 2 donne la définition suivante d'une donnée personnelle : « Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. »

A l'intérieur même de cette catégorie de données appelées données personnelles, il y a une autre catégorie de données qui bénéficie d'un niveau encore plus élevé de protection : ce sont les données considérées comme sensibles : « Une donnée sensible est une donnée qui fait apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle d'une personne.<sup>7</sup> » Ici les données collectées ne permettent plus simplement d'identifier une personne, mais d'en donner des caractéristiques qui peuvent aujourd'hui amener à des discriminations. C'est le cas, par exemple, des données biométriques lesquelles peuvent permettre de déterminer la couleur de peau d'une personne par le visage, donner l'activité de la personne par la reconnaissance veineuse et même déterminer son état de santé grâce à la rétine. La collecte de ces données est aujourd'hui interdite par l'article 8<sup>8</sup> de la loi Informatique et Libertés sauf exceptions qui sont prévues dans ce même article.

Cependant même si, comme on vient de le voir, tout est mis en œuvre au sein de l'Union Européenne pour concilier protection de la vie privée et intérêt sécuritaire, des dérives existent toujours, notamment avec les fichiers de police. D'un autre côté, quand on se place dans le domaine des organisations privées qui constituent une base de données, au vue du nombre de bases de données personnelles non déclarées, on peut se demander si la CNIL en France et son équivalent dans les autres pays européens sont efficaces. Et même quand un

---

<sup>7</sup> Définition [www.juripole.fr](http://www.juripole.fr)

<sup>8</sup> Voir Annexe A

fichier est déclaré, les contrôles de la CNIL sont aujourd'hui très rares et ne peuvent donc assurer un contrôle efficace des garanties qui ont été données par le responsable de traitement lors de la mise en place de la base et de sa déclaration.

De plus, il faut définir ce qu'est un traitement de données plus communément appelés base de données. Il est défini par la loi « Informatique et Libertés » de 1978 comme « toute opération et tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion ainsi que le verrouillage, l'effacement ou la destruction ».

La question de la protection des données, si elle est aujourd'hui plutôt satisfaisante en Europe, il n'en est pas de même dans l'ensemble des pays du monde, très peu de pays se sont intéressés à cette question. Si le nombre de pays possédant une protection équivalente à l'Union Européenne est très faible, le chiffre augmente jusqu'à 25 si on prend en compte les pays ayant mis en place une législation concernant la protection des données personnelles. Cependant cette législation reste très restreinte et dans la plupart des cas ne concerne que certaines activités ou encore certaines catégories de données personnelles très limitées. Certains pays, comme Monaco ou la Nouvelle-Zélande, ont mis en place une commission chargée des contrôles des traitements de données personnelles.

Il en est de même au niveau du droit international où la question de la protection des données personnelles reste quasiment ignorée des grandes organisations et des grandes conventions. Si, comme on l'a vu plus haut, indépendamment de l'Union Européenne, il existe la Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel de 1981, les deux seules autres conventions ne sont que des lignes directrices émises par l'ONU<sup>9</sup> et l'OCDE<sup>10</sup>. Elles contiennent des grands principes comme ceux contenues dans la Convention 108 du Conseil de l'Europe. Le prochain texte sera sans doute la nouvelle directive adoptée par l'Union Européenne dans ce domaine qui fera partie du paquet télécom prochainement.

---

<sup>9</sup> Lignes directrices pour la réglementation des fichiers informatisés de données à caractère personnel de 1989

<sup>10</sup> Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel en date du 23 septembre 1980

Au regard de ce constat sur la législation mondiale, il convient d'inscrire la constitution d'une base de données dans un contexte international. Dans ce contexte de flux continu de données, le transfert d'une base de données ou tout simplement d'une partie d'une base de données personnelle constituée en France devient problématique. En effet, s'il n'était pas envisagé par le droit positif, il suffirait d'envoyer la base de données, collectée en France, à l'étranger pour la soustraire aux formalités et protections européennes. Or ce n'est pas le cas, la directive de 1995 reprise par la loi de transposition de 2004 a prévu le cas des transferts de données personnelles vers l'étranger. Quelles sont alors les procédures et règles à respecter pour exporter une base de données depuis la France ?

La CNIL, quant à elle stipule qu'il faut entendre par transfert de données « toute communication, copie ou déplacement de données par l'intermédiaire d'un réseau, ou toute communication, copie ou déplacement de ces données d'un support à un autre, quel que soit le type de ce support, dans la mesure où ces données ont vocation à faire l'objet d'un traitement dans le pays destinataire ».

Contexte international d'une part, d'un point de vue du secteur privé, où la plupart des multinationales sont amenées à transférer les données qu'elles collectent en France vers d'autres succursales à l'étranger, voir même vers leur maison-mère (Titre I). D'autre part, on retrouve tous les fichiers de police qui, on le sait aujourd'hui, sont de plus en plus importants depuis les attentats du 11 septembre 2001 dans un objectif de sécurité accrue à l'intérieur des pays mais aussi à l'extérieur : contrôle aux frontières, régulation de l'immigration. Toutes ces problématiques sont à l'origine de transferts par les états vers l'étranger de données personnelles et parfois hautement sensibles (Titre II).

# **TITRE I : Le transfert de données entrant dans le champ d'application de la Directive.**

C'est l'article 3 de la Directive européenne qui donne le champ d'application sans surprise de la protection des données personnelles tel que mis en place par la directive. Il était évident, en raison de l'organisation en pilier de l'Union Européenne, que la directive ne s'appliquerait qu'aux données contenues dans un traitement qui aurait pour objet « la sécurité publique, la défense, la sûreté de l'état et les activités de l'Etat relatives à des domaines de droit pénal ». Il en est de même pour « les traitements effectués pour l'exercice d'activités exclusivement personnelles ou domestiques. »

Entrent donc dans le champ d'application de la Directive tous les traitements de données qui s'apparentent à la libre circulation rentrant ainsi dans le champ d'application du droit communautaire. Il convient alors de voir, d'un point de vue général : l'étendue de la protection apportée par la Directive de 1995 (Chapitre I) et ensuite le cas spécifique des transferts de données vers des pays tiers à l'Union Européenne (Chapitre II).

## **CHAPITRE I : Etendue de la protection des données conférée par la Directive de 1995.**

La Directive de 1995 pose quelques principes qui sont un préalable obligatoire à tout transfert de données (Section I) et un cadre législatif qui a été transposé dans l'ensemble des pays européens rendant la procédure de transfert quasi-inexistante quand le transfert s'opère de façon interne à l'Union Européenne (Section II).

## **Section I : Les grands principes applicables aux transferts.**

Il existe aujourd'hui deux grands principes qui sont posés par la Directive de 1995 et la loi Informatique et Libertés. Le premier concerne l'origine des données transférées (A) et quel que soit le pays destinataire des données il doit y avoir une déclaration préalable à la mise en place d'un traitement, c'est le deuxième (B).

### **A : L'origine des données.**

L'article 6 de la Directive de 1995 repris à l'article 6 de la loi Informatique et Libertés du 6 janvier 1978, prévoit les conditions auxquelles les données conservées doivent satisfaire. Ces conditions sont notamment relatives à leur collecte qui doit être loyale et licite, mais aussi à leur finalité qui doit être définie et légitime.

Tous les caractères des données présentées dans cet article doivent être respectés sans quoi la collecte de ces données pourrait ne pas être autorisée.

Cet article de la loi demande par exemple au responsable du traitement de données de définir une finalité relative à la collecte des données. Cette finalité l'engage alors dans un champ restreint pour l'utilisation de ces données, puisqu'il ne pourra pas les traiter ultérieurement pour une finalité différente dans demander à nouveau l'autorisation de la personne. Il existe cependant des exceptions qui sont limitativement énoncées par la loi, comme l'utilisation ultérieure à des fins de statistiques, ou de recherche scientifique par exemple.

On retrouve dans cet article un principe bien connu du droit communautaire qui est le principe de proportionnalité : les catégories de données collectées doivent rester en adéquation avec la finalité annoncée par le responsable. Pour prendre un exemple extrême on ne pourrait pas demander l’empreinte digitale de quelqu’un pour vérifier si on peut lui envoyer un simple colis commandé sur internet. C’est la CNIL qui vérifiera ce principe de proportionnalité lors de son contrôle au moment de la déclaration et de l’autorisation<sup>11</sup> de mise en place du traitement.

On retrouve au dernier alinéa de cet article un principe défendu par toutes les organisations de défense des droits de l’homme : le Droit à l’oubli. En effet aucune donnée même si la finalité du traitement est légitime ne doit être conservée de manière illimitée.

### **B :La déclaration préalable du traitement.**

Il existe aujourd’hui des grands principes et surtout une procédure de déclaration à la CNIL d’un traitement qui doit être un préalable obligatoire à sa mise en place (1). Dans le cas des données sensibles, comme peuvent l’être les données biométriques, cette déclaration se transforme en autorisation<sup>12</sup>. D’un autre côté on ne peut pas mettre en place un traitement de données personnelles comme on le veut, il lui faut une raison légitime (2). Pour simplifier les déclarations préalables aux traitements, une entreprise peut faire le choix de désigner un correspondant informatique et liberté (3).

---

<sup>11</sup> Une autorisation préalable à la mise en place du traitement est nécessaire pour certaines catégories de données : c’est le cas par exemple des données biométriques.

<sup>12</sup> Article 25 de la loi Informatique et Liberté de 1978 : relève d’un régime d’autorisation « 2° Les traitements automatisés portant sur des données génétiques, à l’exception de ceux d’entre eux qui sont mis en œuvre par des médecins ou des biologistes et qui sont nécessaires aux fins de la médecine préventive, des diagnostics médicaux ou de l’administration de soins ou de traitements ; »

## 1 : La déclaration du traitement auprès de la CNIL.

Il existe trois types de déclaration à faire à la CNIL : La déclaration de conformité, la déclaration normale et l'autorisation.

La déclaration de conformité se décline en deux versions. La première est la déclaration de conformité à une autorisation unique. La CNIL autorise dans des décisions cadres des fichiers ou traitement de données personnelles sensibles ou à risques visant une même finalité, des catégories de données et de destinataires identiques. Lorsqu'un traitement ou fichiers envisagés par une personne correspond en tout point à la finalité, les catégories de données et de destinataires de ceux autorisés dans les décisions cadre alors la procédure se voit simplifier. En effet seule une déclaration de conformité suffit. Il en est de même pour les fichiers ou traitements du secteur public où il faut alors effectuer une déclaration de conformité à un acte réglementaire unique.

La déclaration normale est la procédure la plus courante ; le formulaire mis à disposition par la CNIL est le même qu'il s'agisse d'une autorisation ou d'une déclaration normale permettant au responsable de traitement d'éviter les erreurs. La CNIL définit elle-même au vue des éléments du dossier si c'est une autorisation ou simplement une déclaration qui est nécessaire. La CNIL demande elle-même en cas d'autorisation au responsable du traitement les documents pour compléter le dossier.

Tout a été mis en œuvre par la CNIL pour simplifier la procédure de déclaration, celle-ci peut être faite aujourd'hui directement en ligne permettant de simplifier les démarches et d'accélérer le traitement du dossier. Par contre, pour la procédure d'autorisation, si les délais sont de plus en plus courts pour le traitement du dossier par la CNIL se rapprochant du délai légal, c'est toujours long. Cette longueur a pour conséquence le nombre important de traitement de données ou de fichiers qui soient aujourd'hui mis en place sans qu'aucune formalité ne soit accomplie.

On peut aussi faire incomber ce constat à la méconnaissance des formalités à accomplir en pratique de la part des responsables de traitements lorsqu'ils mettent en place une petite base de données.

## 2 : Légitimation de la mise en place d'un système de traitement de données.

Un système de traitement automatisé de données doit être légitime dans sa mise en place. Les cas restrictifs sont prévus à l'article 7 de la Directive de 1995 repris dans l'article 7 de la loi Informatique et Libertés du 6 janvier 1978.

« Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes :

1° Le respect d'une obligation légale incombant au responsable du traitement ;

2° La sauvegarde de la vie de la personne concernée ;

3° L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;

4° L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;

5° La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée. »

○ L'autorisation de la personne concernée :

L'une des conditions les plus simples à remplir est d'avoir l'autorisation de la personne dont on veut collecter les données personnelles. Pour que l'autorisation de la personne soit valable il faut que celle-ci respecte les conditions de n'importe quel contrat. En effet, la personne doit donner son autorisation en toute connaissance de cause et son acceptation doit être explicite et non présumée. L'absence de refus de la non collecte ne peut pas être suffisant. Les grandes caractéristiques qui conditionnent la validité de l'autorisation sont expliquées plus bas pour l'autorisation donnée par la personne concernée au transfert de ces données vers un pays tiers ne bénéficiant pas d'une protection adéquate.

- Information à transmettre aux personnes concernées :

Il existe des obligations en termes d'information des personnes concernées qui reposent sur le responsable du traitement. Celles-ci sont prévues à l'article 10 de la directive de 1995 et reprises à l'article 32<sup>13</sup> de la loi Informatique et Libertés de 1978.

L'information principale qui doit être transmise à la personne concernée est l'identité du responsable du traitement pour que celle-ci puisse le contacter afin d'exercer par exemple son droit d'accès, de rectification et de suppression.

La personne doit également être informée en cas de transferts envisagés vers un état non membre de la communauté européenne.

### 3 : La nomination d'un CIL<sup>14</sup> au sein de l'organisation.

Le correspondant Informatique et Libertés a été créé par la loi du 6 août 2004 qui a refondu la loi Informatique et Libertés de 1978. Il est nommé par l'ensemble des responsables de traitement, que ce soient des personnes morales de droit privé ou public, des associations ou des entreprises,...

Son rôle global est de veiller au respect de la protection des données personnelles au sein de l'entité dans laquelle il exerce ses fonctions et devenir ainsi un interlocuteur privilégié entre les responsables de traitement et la CNIL.

---

<sup>13</sup>[http://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=1D6E0CE93E0C29272CF350904C7F5A2F.tpdjo15v\\_3?idArticle=LEGIARTI000006528127&cidTexte=LEGITEXT000006068624&dateTexte=20090421](http://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=1D6E0CE93E0C29272CF350904C7F5A2F.tpdjo15v_3?idArticle=LEGIARTI000006528127&cidTexte=LEGITEXT000006068624&dateTexte=20090421)

<sup>14</sup> CIL : Correspondant Informatique et Libertés

Son rôle ne se limite pas aux démarches de déclaration/autorisation auprès de la CNIL. Il doit aussi « assurer le respect des droits des personnes (droit d'accès, droit de rectification et de radiation, droit d'opposition..) en leur fournissant une information suffisante sur les traitements mis en œuvre ». Il doit encore « veiller à la proportionnalité des traitements mis en œuvre qui ne doivent porter qu'une atteinte limitée à la vie privée des personnes ». Enfin, il doit « assurer la sécurité et la confidentialité des données traitées, et les informations traitées ne doivent pas être communiquées à des personnes n'ayant aucune raison de les connaître. »

La désignation du CIL se fait directement auprès de la CNIL, soit par son site internet soit par une procédure papier.

## **Section II : Le transfert vers les pays de l'Union Européenne et de l'EEE<sup>15</sup> :**

Le transfert d'une base de données vers les pays de l'Union Européenne ne pose aujourd'hui aucun problème. En effet, celui-ci peut se faire automatiquement sans aucune formalité supplémentaire à celles qui sont aujourd'hui un préalable à la mise en place du traitement. Cette absence de procédure a été rendue possible grâce à la transposition de la Directive de 1995 dans l'ensemble des pays européens (A) et était indispensable à la bonne réalisation de l'objectif communautaire de libre circulation.

Comme le voulait la Directive, tous des pays de l'UE<sup>16</sup> et de l'EEE ont mis en place l'équivalent de la CNIL. Cette autorité<sup>17</sup> de protection des données est chargée de contrôler le respect par les différents acteurs de l'ensemble du dispositif de protection des données (B).

### **A : Transposition de la directive en droit interne.**

La transposition de la directive de 1995, dans l'ensemble des pays de l'UE est aujourd'hui terminée. La plupart des pays de l'Union Européenne ont adopté des lois de transposition entre 1996 et 2000 venant ainsi modifier leur législation antérieure qui était conforme aux principes énoncés par la convention 108 du Conseil de l'Europe ou alors tout simplement adopté une législation sur la protection des données pour les derniers entrants dans l'Union Européenne.

---

<sup>15</sup> EEE : Espace Economique Européen : a été créé en 1992 par accord entre l'Union Européenne et l'AELE (« Association Européenne de Libre Echange » ; en anglais, « *European Free Trade Association* », ou « EFTA »). Cet accord ne concerne que trois sur quatre des pays de l'AELE, à savoir l'Islande, la Norvège et le Liechtenstein, à l'exception de la Suisse, qui a rejeté l'EEE par référendum en 1992. Les pays de l'EEE se sont engagés à transposer dans leurs législations nationales environ 1 400 textes communautaires.

<sup>16</sup> UE : Union Européenne

<sup>17</sup> National data Commissioner

Le dernier pays à avoir transposé dans son droit interne les dispositions de la Directive est la France. C'est en effet par une loi en date du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel que la France a transposé la Directive de 1995 dans son droit interne.

La France comme d'autres pays de l'Union (Allemagne<sup>18</sup>, Autriche<sup>19</sup>, Danemark<sup>20</sup>, Luxembourg<sup>21</sup>...) possédait déjà une législation en matière de protection des données personnelles. Cependant, d'une manière générale, ces législations ne posaient que des grands principes qui s'avéraient conformes à ceux de la Convention 108 mais qui n'étaient pas efficaces. La CNIL comme son homologue européen montrait dans ses rapports que beaucoup de traitements de données ne respectaient pas la législation. Il en était de même en ce qui concerne la collecte de données personnelles notamment sur internet.

En France, cependant malgré le fait que la loi de 2004 soit une loi de transposition, son adoption par le Parlement Français ne fût pas sans heurts. En effet, un recours devant le Conseil Constitutionnel fût présenté par le fait que, selon les députés et sénateurs auteurs de la saisine, cette loi portait atteinte aux libertés individuelles et aux droits des personnes. Le Conseil Constitutionnel l'a, cependant, validée dans sa quasi intégralité mises à part certaines dispositions autorisant la constitution de fichiers d'infractions par tous les professionnels s'estimant particulièrement exposés à la fraude.

Cette loi donne à la CNIL des pouvoirs de contrôle à posteriori des fichiers, beaucoup plus étendus, ainsi que des pouvoirs de sanctions des fichiers non conformes à la déclaration qui en a été faite, beaucoup plus forts. En outre, elle dispense, de toute formalité déclarative, les organismes qui auront choisi de désigner un "correspondant à la protection des données" sur lequel pourra s'appuyer la CNIL.

---

<sup>18</sup> Loi fédérale du 21 janvier 1977 portant protection contre l'emploi abusif de données d'identification personnelles dans le cadre du traitement de données

<sup>19</sup> Loi fédérale sur la protection des données du 18 octobre 1978

<sup>20</sup> Lois du 8 juin 1978 sur les registres privés et sur les registres des pouvoirs publics

<sup>21</sup> Loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques

## **B : Le contrôle effectif de la protection des données.**

Pour que la protection des données dans l'Union Européenne soit la plus effective possible, il a semblé opportun d'imposer aux états-membres la création de commissaires nationaux pour la protection des données (1). D'un autre coté, à l'échelle européenne, la Directive a créé un groupe chargé de s'occuper de la surveillance de l'effectivité de la protection dans l'Union-Européenne qui est appelé « groupe article 29 » (2).

### 1 : Création de commissaires nationaux pour la protection des données.

C'est l'article 28<sup>22</sup> de la Directive européenne de 1995 qui demande aux états de prévoir « qu'une ou plusieurs autorités publiques soi(en)t chargée(s) de surveiller l'application, sur son territoire, des dispositions adoptées par les Etats membres en application » de la Directive. La Directive donne ensuite des indications sur les pouvoirs dont doivent disposer ces autorités et leurs missions. Elles doivent par exemple rendre des avis. La Directive demande aussi à ce que les « autorités exercent en toute indépendance les missions dont elles sont investies. » Elles doivent donc être indépendantes de l'Etat qui les met en place afin d'exercer leurs contrôle et missions dans de bonnes conditions sans aucune pression.

C'est ainsi qu'en France la voie toute naturelle fût de confier cette mission à la CNIL. En effet cette autorité administrative indépendante existait bien avant la Directive de 1995. Elle fût créée par la loi « Informatique et Libertés » qui disait en son article 6 que la CNIL « est chargée de veiller au respect des dispositions de la présente loi, notamment en informant les personnes concernées de leurs droits et obligations, en se concertant avec elles et en contrôlant les applications de l'informatique au traitement des informations nominatives. »

Si à l'origine on ne parlait pas de données personnelles, la CNIL devait déjà contrôler le traitement des informations nominatives. Son statut d'autorité administrative indépendante lui donnait déjà l'indépendance voulue par la Directive pour exercer sa mission et elle disposait déjà du pouvoir réglementaire et de sanctions demandées aussi par la Directive. Il ne

---

<sup>22</sup> Voir Annexe B

fallait donc que compléter ses attributions et la développer puisque ses activités restaient restreintes.

Le choix du commissaire national à la protection des données opéré en France fût le même pour d'autres grands pays européens qui disposaient déjà d'une commission ayant quasiment les mêmes attributions. C'est le cas par exemple en Belgique avec la commission pour la protection de la vie privée.

D'autres pays, comme ceux entrés récemment dans l'UE qui ont dû intégrer l'acquis communautaire dans leur législation, ont dû aussi créer une institution indépendante qui joue ce rôle.

Aujourd'hui, une commission nationale pour la protection des données est présente dans l'ensemble des pays. Si le fonctionnement diffère en fonction des pays, leurs missions sont les mêmes puisque celles-ci sont d'abord définies par la Directive qui a été transposée dans l'ensemble des pays.

## 2 : Le groupe dit « article 29 ».

L'article 29 de la Directive de 1995 met en place un groupe de protection des personnes à l'égard du traitement des données à caractère personnel. Le seul nom que la Directive lui donne est « groupe ». C'est la pratique qui lui donne le nom de groupe « article 29 ». Il est composé « d'un représentant de l'autorité ou des autorités de contrôle désignées par chaque Etat membre, d'un représentant de l'autorité ou des autorités créées pour les institutions et organismes communautaires et d'un représentant de la Commission. » Le président de ce groupe « article 29 » est Alex Türk (actuel président de la CNIL en France.)

C'est l'article 30 de la Directive de 1995 qui définit les missions de ce groupe. Si la mission générale est la surveillance au sein des Etats membres de l'Union Européenne de l'état de la protection des données personnelles, le détail de ses missions va de l'information de la commission dans ce domaine, à l'édiction de recommandations. Le groupe « article 29 » participe avec la commission en la conseillant sur les modifications utiles de la Directive.

C'est le groupe « article 29 », en partenariat avec les chambres de commerce et d'industries des différents Etats, qui est à l'origine de la nouvelle rédaction en date du 27 décembre 2004 des clauses contractuelles types émises par la commission en 2001.

Il exerce aussi un rôle important de veille sur les différentes pratiques des Etats-membres. En effet de part sa composition, c'est lui qui est au plus prêt de ce qui se passe en terme de protection des données comme les nouveaux traitements qui sont envisagés par les acteurs privés au sein des Etats-membres. C'est d'ailleurs pour cela qu'il est le plus à même de conseiller la commission sur d'éventuelles modifications à apporter à la Directive Européenne de 1995.

Il est, en quelque sorte, le coordinateur de l'ensemble des doctrines des différentes commissions nationales de protection des données. En effet c'est par exemple lui qui, par un avis en date 11 octobre 2002, confirme la position prise par les commissaires sur la nécessité d'une limite à la durée de conservation systématique des données de connexion à la suite de la directive « Vie privée » de 2002.

## **CHAPITRE II :Le transfert vers des pays tiers à l'Union Européenne.**

Si comme on vient de le voir, le transfert vers des pays de l'UE ne pose aucun problème et ne nécessite aucune formalité, il n'en est pas de même à partir du moment où le transfert s'effectue vers des pays tiers à l'UE.

Cependant il faut encore distinguer entre deux catégories de pays. Ceux, d'une part, qui ont une législation en matière de protection des données jugée adéquate par la commission européenne (Section I) et ceux, d'autre part, qui ont une législation soit insuffisante soit inexistante et qui n'ont donc pas de protection adéquate (Section II).

### **Section I :Les pays bénéficiant d'une protection adéquate.**

L'Argentine, le Canada, Guernesey, l'île de Man, Jersey et la Suisse sont aujourd'hui les six pays que la Commission a reconnus comme ayant une protection adéquate. En effet la volonté de l'Union Européenne et des différents états-membres étant de garantir à leurs ressortissants la même protection sur leurs données sensibles lors du transfert à des pays tiers, c'est seulement une décision de la Commission qui peut harmoniser un constat pour l'ensemble de l'Union (A). Il reste cependant une réserve relative au champ d'application de la loi canadienne pour le cas spécial du Canada (B).

#### **A : L'intervention de la commission européenne.**

La Commission a reçu, de la part du Conseil de l'Union Européenne et du Parlement Européen, le pouvoir de décider sur la base de l'article 25 (6°) si un pays tiers offre un niveau de protection adéquat en raison de sa législation. Il faut donc que la Commission rende une décision dite d'adéquation (1). Cette décision permet de réduire au maximum les formalités préalables au transfert (2).

## 1 : Les pays ayant reçu l'aval de la commission.

Les pays qui ont reçu l'aval de la Commission sont aujourd'hui au nombre de six. Le premier pays à avoir fait l'objet d'une décision d'adéquation par la Commission Européenne est la Suisse. C'est en effet par une décision en date du 26 juillet 2000<sup>23</sup> que la Commission dispose que la loi fédérale sur la protection des données de 1992 confère un niveau de protection adéquat pour le transfert des données.

Dans ce groupe des six, il y a aussi les deux îles Anglo-Normandes Jersey et Guernesey et l'île de Man. Jersey est la dernière pour qui la commission a constaté le caractère adéquat de sa législation par une décision en date du 8 mai 2008<sup>24</sup>. Pour Guernesey c'est par une décision en date du 21 novembre 2003<sup>25</sup> que la commission constate le niveau de protection adéquat des données de sa législation. L'île de Man fit l'objet d'une décision d'adéquation le 28 avril 2004<sup>26</sup>, lequel a constaté le niveau de protection adéquat des données.

L'Argentine, pays beaucoup plus éloigné de l'Europe, a bénéficié d'une décision en date du 30 juin 2003<sup>27</sup> constatant le niveau de protection adéquat des données.

Comme on peut le remarquer, ces pays sont très proches des conceptions européennes. Pour les trois îles et pour la Suisse, le rapprochement est autant géographique qu'économique. Ces pays fonctionnent avec l'Union Européenne de manière étroite, même s'ils n'en font pas

---

<sup>23</sup> Décision 2000/518/CE du 26 juillet 2000 relative à la constatation, conformément à la Directive 95/46/CE du parlement Européen et du conseil, du caractère adéquat de la protection des données à caractère personnel en Suisse

<sup>24</sup> Décision 2008/393/CE du 8 mai 2008 constatant le niveau de protection adéquat des données à caractère personnel de la Loi du 21 janvier 2005 sur la protection des données (Jersey)

<sup>25</sup> Décision n° 2003/821/CE du 21 novembre 2003 constatant le niveau de protection adéquat des données à caractère personnel de la loi sur la protection des données de 1986 complété par une loi de 2001 (Guernesey)

<sup>26</sup> Décision n°2004/411/CE du 28 avril 2004 constatant le niveau de protection adéquat des données à caractères personnel de la loi sur la protection des données (data protection act) de 2002 et entrée en vigueur le 1<sup>er</sup> avril 2003 (île de Man).

<sup>27</sup> Décision n°2003/1731/CE constatant conformément à la directive 95/46/CE du parlement européen et du conseil, le niveau de protection adéquat des données à caractère personnel assuré par la loi argentine sur la protection des données à caractère personnel de la loi sur la protection des données personnelles du 2 novembre 2000

partie. De plus, leur législation et leur conception idéologique s'en rapprochent. Il en est de même pour l'Argentine.

Il convient cependant de préciser que des procédures ont été engagées avec la Nouvelle-Zélande et l'Australie, mais les lois de protection des données de ce dernier État n'assurent pas, en l'état, la protection des étrangers.

Lorsque la Commission Européenne reconnaît le niveau de protection adéquat des données à caractère personnel, la procédure est alors simplifiée à l'extrême. Si une déclaration préalable au transfert est toujours nécessaire, ce n'est qu'une simple déclaration. En effet l'autorisation est supprimée. Il suffit que le responsable de traitement envoie le formulaire de déclaration normale à la CNIL en précisant que le transfert s'effectue vers des pays reconnus par la Commission Européenne comme ayant un niveau de protection adéquat des données.

## 2 : Activité Internationales de ces pays.

Les pays<sup>28</sup> qui ont mis en place une commission ou simplement un commissaire pour la protection des données se réunissent en une conférence internationale des commissaires nationaux à la protection des données et de la vie privée. Cela un peu à l'instar du groupe de l'article 29 qui existe au sein de l'Union Européenne. A cette conférence est associé le contrôleur européen à la protection des données<sup>29</sup>.

Lors de la 31<sup>ème</sup> conférence internationale des commissaires nationaux à la protection des données et de la vie privée, le groupe des commissaires propose la mise en place de normes internationales pour la protection de la vie privée et la protection des données. Ce groupe rappelle « qu'avec l'expansion de la société de l'information, le droit à la protection des données et à la vie privée est une condition indispensable dans une société démocratique pour garantir le respect des droits des personnes, la libre circulation des informations et une économie de marché ouverte ». L'ensemble des commissaires souhaite agir pour que les

---

<sup>28</sup> C'est le cas pour l'ensemble des pays de l'UE, de l'EEE, des pays ayant un niveau de protection adéquat, mais aussi par exemple de l'Australie, de la Nouvelle-Zélande, du Japon...

<sup>29</sup> Autorité indépendante qui a pour but de contrôler la protection des données à caractère personnel et de la vie privée au sein des organes et institutions de l'Union Européenne. Il est en charge par exemple de contrôler la mise en place et le fonctionnement des grands fichiers Européens.

conventions et recommandations de l'APEC et de l'OCDE, notamment, ne soient qu'un début et non une fin à l'élaboration d'« un instrument juridique universel contraignant consacrant, recensant et complétant les principes communs de protection des données et de respect de la vie privée énoncés dans différents instruments existants et renforçant la coopération internationale entre les autorités de protection des données ».

L'ensemble des Etats est donc conscient qu'une protection des données efficace ne passe que par l'adoption, par un très grand nombre de pays, d'une législation aussi protectrice que celle qui existe en Europe et dans les pays ayant mis en place une protection équivalente.

On peut cependant remarquer que pour l'ensemble des pays tiers à l'Union Européenne, la mise en place d'une législation sur les données personnelles, qu'elle soit ou non équivalente à la législation européenne, date des années 2000. Cela laisse donc à penser que l'influence de l'Europe en la matière est très importante, peut être aussi par l'adoption de règles contraignantes pour le commerce international...

### **B : Le cas spécifique du Canada.**

Dans une décision en date du 20 décembre 2001, la commission constate le caractère adéquat de la loi fédérale sur la protection des données de 1982 complétée par la loi fédérale sur la protection des renseignements personnels et les documents électroniques de 2000.

Cependant, le cas du Canada nécessite quelques petites précisions. Le champ d'application de la loi canadienne est restreint : il se limite à toutes les données recueillies, utilisées ou communiquées par une organisation<sup>30</sup> dans le cadre d'une activité commerciale. La loi canadienne ne s'applique pas aux organisations sans but lucratif ou caritatives. En ce qui concerne les autres dispositions, la loi canadienne est sensiblement identique à la directive de 1995 et, dans tous les cas, celle-ci offre un niveau de protection similaire à celui mis en place au sein de l'Union Européenne.

---

<sup>30</sup> Le terme organisation est entendu au sens large et désigne aussi bien une entreprise, qu'une association ou encore un syndicat.

La Commission Européenne a mis en place une FAQ<sup>31</sup> pour expliquer les cas de mise en œuvre de la loi canadienne et donc les cas où le transfert de données personnelles vers le Canada ne nécessite aucune formalité particulière. Dans tous les cas où le transfert n'entre pas dans le champ d'application de la loi canadienne, les modalités requises pour le transfert vers un pays tiers n'ayant pas un niveau de protection adéquat, relèvent donc d'un régime d'autorisation CNIL.

---

<sup>31</sup> [http://ec.europa.eu/justice\\_home/fsj/privacy/thridcountries/adequacy-faq\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/adequacy-faq_en.htm)

## **Section II : Les autres pays tiers à l'Union Européenne.**

Si comme on vient de le voir la procédure est simplifiée voir quasi inexistante pour les pays ayant une protection adéquate, il n'en est pas de même pour les autres pays. En effet la volonté de l'Union Européenne et de ses Etats-membres étant de conférer aux données transférées la même protection dans le pays destinataire que dans leur pays d'origine, la procédure est contraignante (A). Cependant il existe une exception toute particulière pour les Etats-Unis en raison du nombre important d'échanges commerciaux, ceci permet d'échapper à une procédure contraignante et de retomber dans le cas de pays ayant un niveau de protection des données adéquat (B).

### **A : Une procédure contraignante généralisée pour l'ensemble des pays tiers.**

Depuis la Directive de 1995, le transfert de données personnelles depuis la France vers un pays n'ayant pas un niveau de protection des données adéquat doit faire l'objet d'une autorisation de la CNIL (1). Pour bénéficier de cette autorisation, il faut, notamment, que les données bénéficient de la même protection, une fois le transfert effectué, que si elles étaient restées en France. Cette protection peut s'acquérir grâce à un contrat de flux transfrontalier de données (2) ou encore à des règles internes aux entreprises concernées (3).

#### **1 : La procédure devant la CNIL.**

Selon l'article 69 alinéa 8, tout transfert de données ou de fichiers de données à caractère personnel vers un pays tiers n'ayant pas un niveau suffisant de protection des données, doit faire l'objet d'une autorisation préalable, au début du transfert, de la part de la CNIL.

Cette autorisation contrairement à la déclaration normale ne peut se faire directement sur le site internet de la CNIL. En effet, toute autorisation demande une instruction du dossier par la CNIL. L'autorisation du transfert se fera au cas par cas en fonction de la protection qui sera apportée aux données dans le pays destinataire des données, en fonction du pays et si le transfert répond aux exigences de la doctrine de la CNIL.

La demande d'autorisation auprès de la CNIL se fait grâce à deux formulaires dont l'un est commun avec la déclaration préalable à la mise en place d'un traitement. L'envoi de ces deux formulaires devra s'accompagner de l'ensemble des documents qui peuvent être utiles à la CNIL, précisant par exemple le niveau de protection apportée aux données dans le pays destinataire, afin de l'aider à prendre sa décision.

## 2 : Le contrat de flux transfrontalier de données.

La réalisation d'un contrat de flux-transfrontières de données est un préalable obligatoire pour le transfert. Celui-ci a pour but de palier le manque de législation dans le pays destinataire. Il devra être transmis à la CNIL pour l'autorisation de transfert.

Le niveau de protection apportée aux données par le contrat de flux transfrontalier de données, s'il ne peut être identique à celui apporté en France, doit s'en rapprocher le plus possible. En effet il ne pourra pas y avoir de contrôle sur les données par l'autorité du pays, cependant la CNIL devra pouvoir exercer un contrôle à posteriori sur la protection effective ou non dans le pays destinataire. En l'absence d'accord entre les pays, cela ne pourra être possible que grâce à un lien contractuel entre le destinataire des données et l'exportateur.

En tout état de cause, le respect de la vie privée des personnes concernées<sup>32</sup> ne doit jamais être remis en cause ainsi que leurs droits sur les données. Leurs droits d'accès de rectification ou de modification des données doit être protégé par le contrat de flux transfrontalier de données.

---

<sup>32</sup> Personne concernée : personne à qui appartiennent les données collectées et transférées le cas échéant.

Vu le nombre de pays qui n'a pas un niveau de protection suffisant, la Commission a mis en place des clauses contractuelles types qui sont conformes avec les exigences de la législation européenne. Elles sont disponibles dans toutes les langues européennes<sup>33</sup>. Elles se trouvent en annexe de la décision dans laquelle la Commission a mis place ces clauses. Elles sont disponibles en deux versions, l'une datant de 2001<sup>34</sup> et l'autre de 2004<sup>35</sup>.

La commission, suite aux sollicitations du groupe « article 29 » et de la plupart des chambres de commerce et d'industrie, a dû réfléchir à de nouvelles clauses. En effet celles de 2001 étaient jugées inadaptées aux réalités des transferts de données dans un cadre commerciale. Les nouvelles clauses adoptées par la Commission en 2004 sont en partie issues de celles rédigées par le groupe « article 29 » et les chambres de commerce et d'industrie.

Ces clauses (dans leurs deux versions) sont aujourd'hui reconnues par la CNIL et telles quelles permettent d'obtenir l'autorisation de la CNIL. Certaines clauses complémentaires peuvent être ajoutées. Cependant elles ne doivent pas dénaturer le reste et amoindrir le niveau de protection conféré aux données sinon le transfert sera refusé par la CNIL.

Certaines clauses complémentaires peuvent être ajoutées comme par exemple la désignation d'un tribunal compétent et de la loi applicable, en cas de litiges. On peut aussi inclure une clause pour le recours à l'arbitrage international.

Certaines clauses peuvent aussi prévoir le montant d'indemnisation des parties en cas de non respect du contrat. Elles peuvent aussi limiter le champ d'utilisation de la base.

Si l'utilisation des clauses contractuelles types est recommandée, elle n'est pas obligatoire, les parties peuvent décider de rédiger leur propre contrat ou de modifier les clauses contractuelles types. Le contrat devra toujours respecter et procurer une protection équivalente à celle que les données auraient si elles restaient en Europe.

---

<sup>33</sup> [http://ec.europa.eu/justice\\_home/fsj/privacy/modelcontracts/index\\_fr.htm](http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_fr.htm)

<sup>34</sup> Version anglaise des clauses de 2001 en version PDF : <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:006:0052:0062:EN:PDF>

<sup>35</sup> Version anglaise des clauses de 2004 en version PDF : <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:EN:PDF>

Il est recommandé, pour favoriser l'autorisation de la CNIL, de fournir un tableau de concordance entre les clauses contractuelles types de la Commission et le contrat soumis à la CNIL si celui-ci est différent des clauses contractuelles types.

### 3 : Les règles internes d'entreprises.

L'article 69 alinéas 8<sup>36</sup> de la loi « informatique et liberté » prévoit qu'il est possible de recourir à des règles internes d'entreprises pour encadrer les transferts internationaux de données au sein d'une même entreprise. Les règles internes d'entreprises s'entendent comme « un ensemble de règles relatives à la protection des données personnelles élaborées par l'organisme du responsable de traitement, le plus souvent une société multinationale, dont le respect est obligatoire pour chacune des entités membres du groupe. »<sup>37</sup>

La loi « informatique et liberté » a autorisé et favorisé la pratique des règles internes d'entreprise pour permettre de faciliter le transfert de données personnelles au sein des entreprises multinationales qui peuvent être très important, répété et d'une grande variété de catégories de données. Ces règles internes d'entreprise doivent procurer les mêmes garanties que celles que pourraient offrir un contrat de flux transfrontalier de données.

Pour faciliter leur élaboration, le « groupe de l'article 29 » a diffusé un document de travail<sup>38</sup> qui détermine les conditions générales dans lesquelles de telles règles doivent être élaborées, mais aussi les grandes lignes de ces règles.

La CNIL quant à elle émet une liste dans son guide que doivent respecter les règles internes pour faire l'objet d'une autorisation de transfert : Le caractère contraignant des règles doit être établi, des mesures doivent être prises assurant l'application des règles internes, les personnes doivent avoir la possibilité de se prévaloir de l'existence de ces règles, la description précises des transferts couverts par les règles afin d'offrir une sorte de « mode d'emploi » de la protection des données personnelles au sein de l'entreprise pour les

---

<sup>36</sup> Voir annexe A

<sup>37</sup> Définition donnée par la CNIL dans son guide sur « le transfert de données à caractère personnel vers des pays non membres de l'Union Européenne » de Juin 2008

<sup>38</sup> Document de travail WP 74 complété par un autre document de travail du « groupe de l'article 29 » dit « model checklist » (document WP 108).

personnes appelées à en traiter, et finalement des garanties doivent avoir été prises pour que les principes de la protection des données personnelles soient appliqués en pratique dans le groupe (information des personnes, sécurité des données, droit d'accès, respect du principe de finalité...).

C'est aux responsables de traitement qui demande l'autorisation de transfert de prouver à la CNIL que le caractère contraignant des clauses est effectif dans l'ensemble du groupe d'entreprise. Pour se faire les entreprises peuvent se référer aux documents de travail mis en place par le groupe « article 29 » qui donnent des exemples des éléments de nature à assurer une nature contraignante aux règles.

## **B : Le cas des Etats-Unis.**

Il existe, pour les transferts vers les Etats-Unis, un moyen d'échapper à la procédure contraignante décrite ci-dessus : il suffit que le destinataire des données adhère aux « safe harbor principes » négociés par le département du commerce américain avec la Commission Européenne dans les années qui ont suivies l'adoption de la Directive de 1995 (1). Cependant au vu de la procédure qui est aujourd'hui applicable pour l'adhésion à ces principes on peut se demander si cette solution est efficace (2).

### 1 : La reconnaissance par la commission des « safe harbor principes ».

Le cas des Etats-Unis est particulier. Pour diverses raisons un accord a été conclu entre eux et la Commission Européenne sur la mise en place d'une « sphère de sécurité » visant à favoriser le transfert de données personnelles de l'Europe vers les Etats-Unis pour des raisons avant tout commerciales. En effet, beaucoup d'entreprises américaines collectent des données personnelles en France et sont ainsi amenées à les transférer aux Etats-Unis. Il fallait donc trouver une solution pour leur simplifier les démarches.

Très vite le département du commerce américain et plus particulièrement la « National Information Agency » a entamé des négociations avec la Commission Européenne et ce dès 1998. Interrompues puis reprises, elles ont finalement donné lieu à la publication par le « US department of commerce » des « safe harbor privacy principles ». Ils constituent une sorte de sphère de sécurité et fonctionnent comme une sorte de label.

Ces principes sont directement issus de la Directive de 1995, et contiennent des principes essentiels, comme par exemple l'information des personnes, la possibilité accordée à la personne concernée de s'opposer à un transfert à des tiers ou à une utilisation des données pour des finalités différentes, le consentement explicite pour les données sensibles, le droit d'accès ou encore la sécurité du transfert en lui-même.

Ces principes permettent ainsi de donner le niveau de protection adéquat requis par la Commission Européenne à toute entreprise qui s'y inscrit. C'est une décision de la Commission Européenne en date du 26 juillet 2000<sup>39</sup> qui donne l'équivalent du niveau de protection adéquat aux entreprises adhérant à la sphère de sécurité. Cette sphère de sécurité inclut les « safe harbor privacy principles » mais aussi les FAQ<sup>40</sup>. Celles-ci sont au nombre de 15. Elles se présentent sous forme d'interprétation de certains termes et ce n'est qu'à la condition que les entreprises respectent ces interprétations, que le niveau adéquat de protection est effectif.

Pour les entreprises qui veulent s'y inscrire, la démarche est simple, puisqu'il leur suffit d'écrire une lettre informant le département du commerce que l'entreprise rejoint la sphère de sécurité. Elle doit déclarer publiquement son adhésion à la « safe harbor ». Elle doit en plus se trouver sous la compétence de la « federal trade commission ». Cette dernière, en vertu du « federal trade commission act », est compétente pour toutes les manœuvres et les pratiques déloyales ou frauduleuses dans le domaine du commerce ou de tout autre organisme remplissant une mission analogue. Elle s'est d'ailleurs déclarée compétente pour étudier les plaintes venant d'une personne non résidente aux Etats-Unis.

---

<sup>39</sup> Décision n° 2000/520/CE du 26 Juillet 2000, conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la «sphère de sécurité» et par les questions souvent posées y afférentes, publiées par le ministère du commerce des États-Unis d'Amérique.

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:FR:PDF>

<sup>40</sup> FAQ : « Frequently Asked Questions »

Cependant la CNIL précise que lors des formalités préalables, les responsables de traitement devront « mentionner l'existence d'un transfert de données vers une société adhérente aux « Safe Harbor » et devront fournir à la Commission les extraits pertinents de la « Safe Harbor List », disponibles sur ce site<sup>41</sup>. Cette liste permet d'avoir accès aux détails de l'autocertification de la société adhérente. »

## 2 : Une protection efficace ?

A la suite de la parution de ces principes et de la mise en place de cette sphère de sécurité, les premières critiques ont fusées. En effet, si sur le papier ces principes semblent être une bonne alternative à l'attente d'une législation adéquate, l'effectivité du respect de ces normes s'avère plus douteux.

En effet, contrairement à la France où la mise en place d'une base de données relève d'une déclaration et même d'une autorisation auprès de la CNIL, l'adhésion à ces principes ne nécessite aux Etats-Unis qu'une simple déclaration de respect, par l'entreprise, des « safe harbor privacy principles ». Il n'y a aucun contrôle qui est fait sur l'effectivité réelle de cette mise en place. Les seules suites ne se font que si un titulaire de données porte plainte auprès de la « federal trade commission »...

Aujourd'hui les Etats-Unis ont adopté plusieurs dispositions visant à protéger les données tant au niveau fédéral que fédéré (notamment l'état de Californie), mais très peu de ces dispositions offre un réel niveau de protection.

---

<sup>41</sup><http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list?OpenDocument&Start=1>

## **C : Les dérogations autorisant le transfert vers un pays tiers n'assurant pas un niveau adéquat de protection.**

Il existe des dérogations prévues dans la Directive de 1995<sup>42</sup> et reprises à l'article 69<sup>43</sup> de la loi de 1978 qui autorisent le transfert vers un pays n'assurant pas un niveau de protection adéquat.

### **1 : Utilisation des dérogations**

La volonté de la CNIL, du groupe « article 29 » et de la Commission, est de conférer aux personnes titulaires des données une protection identique quel que soit le pays vers lequel elles sont transférées. Or l'utilisation des différentes dérogations implique une absence totale de protection si le pays dans lequel elles sont transférées n'a pas adopté de législation dans ce domaine.

C'est pourquoi la CNIL, conformément aux recommandations<sup>44</sup> du groupe « article 29<sup>45</sup> », recommande que « le champ d'application des dispositions soit *a priori* limité à des cas exceptionnels dans lesquels il serait réellement inapproprié, voire impossible, que le transfert ait lieu sur la base des dispositions de l'article 69 alinéa.8 (contrat, règles internes) ».

La CNIL, comme le groupe « article 29 », recommande surtout « que des transferts répétitifs, massifs ou structurels de données personnelles, dont l'importance ou la régularité justifie qu'ils soient encadrés de manière précise, fassent l'objet d'un encadrement juridique spécifique et ne reposent donc pas sur ces dérogations. »

---

<sup>42</sup> L'article 26-1 de la directive de 1995

<sup>43</sup> Voir Annexe A

<sup>44</sup> « *Ces dérogations*, formulées de manière restrictive, ne doivent concerner que des cas dans lesquels les risques pour la personne concernée sont relativement faibles, ou des cas dans lesquels d'autres intérêts (qu'ils soient publics ou propres à la personne concernée elle-même) priment le droit de la personne concernée au respect de sa vie privée »

<sup>45</sup> Il a émis ses recommandations dans un document de travail WP 114 ( [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2005/wp114\\_fr.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_fr.pdf) ) où il affine les recommandations présentées dans le document de travail WP 12

En résumé, l'utilisation de ces dérogations ne doit être que subsidiaire, le responsable du traitement devant privilégier la mise en place de règles ou contrat mettant en place un niveau de protection suffisant.

## 2 : Interprétation stricte des dérogations.

L'ensemble des dérogations présentées ci-dessus sont d'interprétations strictes conformément aux principes généraux du droit français et du droit communautaire. La CNIL interprète, strictement et au vue de ces observations sur chaque dérogation, toute utilisation de celle-ci. En effet, l'utilisation de ces dérogations entraîne une absence totale ou quasi-totale de protection pour la personne dont les données seront transférées. La nécessité d'une interprétation stricte est conforme aux recommandations adoptées par le groupe « article 29 » dans son document de travail WP 12<sup>46</sup>.

## 3 : L'autorisation de la personne pour le transfert.

Le consentement de la personne concernant le transfert doit être libre, spécifique et non vicié.

Ce consentement doit tout d'abord être une manifestation positive de la volonté de la personne. Le consentement ne saurait donc être déduit d'une absence de refus par exemple ou encore d'un accord implicite. Cette condition exclut donc tous les transferts où la personne ne pourrait s'opposer qu'à postériori. L'utilisation de cases pré-cochées est à exclure pour la manifestation du consentement de la personne pour le transfert alors que la possibilité de cases à cocher est possible.

La liberté du consentement implique que le consentement donné par une personne qui aurait été mise devant le fait accompli n'est pas valable. Il en est de même pour le consentement donné quand il existe un lien de subordination entre la personne et le responsable du traitement, ce peut être le cas dans le cadre d'une relation de travail. Le consentement d'un salarié pour le transfert de ses données personnelles par son entreprise

---

<sup>46</sup> [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/1998/wp12\\_fr.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_fr.pdf)

n'est à priori pas libre. Il faut que le salarié puisse refuser de donner son consentement sans craindre de préjudices ou être libre de le retirer ultérieurement dans les mêmes conditions. La liberté du consentement d'un salarié n'est que très rarement admise et dans des cas très précis.

Le consentement de la personne, concernant le transfert, doit être spécifique, empêchant ainsi un consentement à priori par anticipation d'un transfert futur, dont la survenance ou les circonstances précises ne sont pas acquises au jour où le consentement des personnes est requis<sup>47</sup>. Si la personne est appelée à consentir à plusieurs points, chacun d'eux doit faire l'objet d'une manifestation de volonté distincte.

Enfin la dernière caractéristique du consentement est l'information de la personne. En effet, quand celle-ci donne son consentement, elle doit avoir été préalablement informée des circonstances spécifiques du transfert (finalité du transfert, identité et coordonnées du ou des destinataires, etc.). L'information qu'elle aura reçue a aussi pour but de l'informer sur le fait que les pays vers lesquels les données seront transférées n'ont pas forcément un niveau de protection adéquat.

L'exception due au consentement de la personne ne sera admise par la CNIL que si toutes les caractéristiques énoncées ci-dessus sont réunies et que le consentement ne fait aucun doute.

---

<sup>47</sup> Exemple donné par la CNIL : « une société ne pourra pas, au moment où elle collectera les données de ses clients pour une finalité précise, demander à ceux-ci de consentir par anticipation au transfert de leurs données vers des pays tiers, dans l'éventualité où cette société se ferait hypothétiquement racheter par une société tierce. »

## **TITRE II : Les données exclues du champ d'application de la Directive.**

Comme on l'a vu dans l'introduction du Titre I, la Directive ne s'applique qu'aux données qui entrent dans le champ d'application du droit communautaire, soit le premier pilier. Les données exclues du champ d'application de la Directive Européenne de 1995 sont celles du deuxième et du troisième pilier, c'est le cas par exemple du transfert des données contenues dans les fichiers de police européens (Chapitre I) ou des données PNR qui ont fait l'objet d'un long cheminement jurisprudentiel (Chapitre II).

### **CHAPITRE I : Les données contenues dans les grands fichiers de police.**

Dans les fichiers de police qui relèvent du troisième pilier on doit distinguer le transfert qui concerne les données contenues dans les grands fichiers de police européens (Section I) de celles contenues dans les fichiers nationaux (Section II).

#### **Section I : Les grands fichiers de police européens.**

Il faut tout d'abord présenter les grands fichiers de police européens qui sont nombreux (A) et voir leurs spécificités avant d'aborder les règles qui sont applicables aux transferts des données qu'ils contiennent (B).

## **A : Présentation.**

### 1 : Système d'Information Schengen (SIS).

Le fichier Système d'Information Schengen a été créé par la convention d'application de la Convention de Schengen. L'accord de Schengen en date du 14 juin 1985 prévoit la libre circulation des personnes avec la levée des contrôles aux frontières intérieures. Il est renvoyé à une convention d'application pour le choix des mesures visant à compenser la libre circulation des personnes.

Cette convention d'application a été mise en place en juin 1990. La clé de voûte de cette convention est le SIS. Au début, la Commission Européenne était très réticente sur la mise en place de ce fichier et progressivement les états s'y sont intéressés. Cependant contrairement à tous les Etats qui vont rejoindre la Convention de Schengen, le Royaume-Uni et l'Irlande ne rejoignent pas cette convention en raison de l'absence de frontière terrestre avec les autres Etats de l'UE.

L'acquis de Schengen doit cependant être ventilé entre le premier et le troisième pilier. En effet la libre circulation des personnes à l'intérieur de l'Europe relève du premier pilier et du droit communautaire. Cependant le SIS, en tant que fichier relevant de la coopération policière et des contrôles aux frontières, reste dans le troisième pilier. A l'origine, le SIS est destiné à lutter contre l'immigration clandestine et à contrôler les flux migratoires.

Le SIS est un système fonctionnant de manière classique : système d'information central (CSIS), il se trouve à Strasbourg et chaque état dispose d'un système d'information national. Il est créé par l'Article 92 de la Convention d'application Schengen. Les états envoient, depuis leurs fichiers nationaux, le signalement au fichier central et quand un état a besoin d'informations sur un signalement, il le demande au CSIS. Il y a d'autre part les signalements en matière de terrorisme ou de trafic de stupéfiants.

Finalement avec les nouveaux états membres, le SIS est devenu inadapté au nombre d'états surtout que le Royaume-Uni et l'Irlande commencent à être intéressés par ce fichier de police. Il a été prévu de remplacer le SIS par le SIS II afin de répondre aux nouvelles exigences : augmenter le nombre d'états pouvant y accéder et y inclure des données

biométriques (empreintes digitales, empreinte faciale et empreinte génétique à terme). Le SIS II devait entrer en fonction en 2009.

Il y est prévu un droit d'accès et un droit de rectification. Mais en France, le droit d'accès est indirect, il faut d'abord passer par la CNIL et c'est cette dernière qui va tout vérifier en envoyant deux magistrats : est-ce que la personne est fichée et quelles sont les données figurent au fichier ? En principe, la personne a un droit de rectification et aussi un droit au juge : article 111. Le conseil d'état s'est reconnu compétent puisque c'est un fichier de police et il a même reconnu qu'il était compétent pour accéder à un signalement d'un autre état que la France pour vérifier si ce signalement peut figurer dans le SIS.

## 2 : Système EURODAC.

Le système EURODAC est une base de données qui été créée par un règlement du Conseil de l'UE en date du 11 décembre 2000. C'est le contrôleur européen à la protection des données qui s'est imposé comme étant l'autorité compétente pour la protection des données. C'est un fichier destiné à prendre en compte toutes les empreintes digitales des demandeurs d'asile dans un état membre et de prendre les empreintes de tous les étrangers en situation irrégulière.

Cette base de données Européenne est opérationnelle depuis le 15 janvier 2003. La base de données EURODAC rentre dans le système Dublin qui vise à déterminer quel état est compétent pour traiter d'une demande d'asile.

La base de données EURODAC comprend une base de données centrale informatisée, dans laquelle sont traitées les empreintes digitales et des données administratives en vue de la comparaison des données personnelles des étrangers de plus de 14 ans ayant passé la frontière européenne étant en situation irrégulière et n'ayant pas été refoulés par les autorités douanières, mais aussi les étrangers se trouvant sur le territoire d'un état membre en situation irrégulière sans qu'il ait fait une demande d'asile dans un autre état membre. Le système EURODAC comprend aussi une unité centrale, équipée d'un système informatisé de reconnaissance des empreintes digitales, gérant la base de données et des moyens de transmission des données entre les états membres et la base de données centrale.

Les états appartenant au système EURODAC sont plus nombreux que ceux appartenant au système Schengen puisque la Suisse, l'Islande, le Liechtenstein et la Norvège ainsi que l'ensemble des pays de l'Union Européenne appartiennent au système EURODAC.

(i) 3 : Système VIS.

Le système d'information sur les Visas ou VIS a été créé par une Décision 2004/512/CE du Conseil européen en date du 8 juin 2004, portant création du système d'information sur les visas (VIS).

Le système d'information sur les visas (VIS) repose sur une architecture centralisée. Il comprend un système d'information central, «le système central d'information sur les visas» (CS-VIS), une interface dans chaque état membre : «les interfaces nationales», (NI-VIS), lesquelles assurent la connexion avec les autorités centrales nationales des états membres respectifs et une infrastructure de communication entre le système central d'information sur les visas et les interfaces nationales.

Il devrait entrer en fonction cette année et devenir ainsi le plus grand fichier mondial contenant des données biométriques. Toute personne qui demandera un visa devra donner une photo et ses empreintes digitales qui seront alors enregistrées dans les interfaces nationales. Ce système est considéré comme étant lié au Système d'Information Schengen.

4 : EUROPOL<sup>48</sup>.

EUROPOL a été créé en 1995 par l'office européen de police. Le siège d'EUROPOL se trouve à la Haye. EUROPOL est une organisation intergouvernementale créée dans le cadre du troisième pilier et qui est destinée à faciliter la coopération judiciaire européenne en matière de poursuite d'infractions pénales. C'est un office qui travaille par échanges d'informations et qui fonctionne par analyses. Il a pour but de faciliter l'échange de

---

<sup>48</sup> EUROPOL : European Police Office

renseignements entre polices nationales en matière de stupéfiants, de terrorisme, de criminalité internationale et de pédophilie au sein de l'Union Européenne.

Cette convention EUROPOL prévoit de conclure des accords de coopération stratégique avec des états tiers : dans le cadre des accords de coopération opérationnelle, EUROPOL échange ses données et ses fichiers d'analyse. EUROPOL travaille avec un ensemble d'états tiers parmi lesquels se trouvent les Etats-Unis.

C'est le directeur d'EUROPOL qui signe les accords sans demander l'autorisation aux autorités de l'EU. Cependant, d'après une décision du Conseil Justice et Affaires Intérieures du 6 avril et à compter du 1<sup>er</sup> janvier 2010, EUROPOL sera une agence communautaire, augmentant alors les pouvoirs de l'office central mais aussi ceux du Parlement Européen.

## **B : Modalités de Transferts.**

Il n'existe pas aujourd'hui de texte réglementant précisément le transfert entre états-membres de données contenues dans des fichiers de police comme peut le faire la Directive de 1995 pour les données entrant dans le champ du droit communautaire.

La particularité des fichiers de police est qu'ils relèvent du troisième pilier de l'Union Européenne et donc de la coopération intergouvernementale entre les autorités de l'ensemble des états membres. Plusieurs décisions cadres de l'Union Européenne visent à encadrer la coopération entre les états et à la renforcer.

C'est le cas de la décision du 27 novembre 2008 sur la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale qui a été prise par l'Union Européenne et qui relève du troisième pilier Justice et Affaires Intérieures (JAI).

## **Section II : Les fichiers de police nationaux.**

Les fichiers de police nationaux sont encore plus spécifiques que les fichiers de police européens car leur constitution est de la souveraineté des Etats. En général, les Etats les mettent en place pour la sécurité nationale (A). Les règles applicables au transfert des données qu'ils contiennent sont aussi spécifiques au vu des données particulières qu'ils peuvent contenir (B).

### **A : Présentation des spécificités des fichiers de police nationaux.**

La tendance actuelle en matière de fichiers de police est d'augmenter le nombre et la variété des données qu'ils contiennent en y intégrant notamment un plus grand nombre de données biométriques. C'est le cas, en France, avec les données ADN qu'on enregistre aujourd'hui dans le FNAEG<sup>49</sup>. Ce fichier créé en 1998 recense l'ensemble des traces ADN trouvées lors d'investigations policières. Progressivement, la prise des empreintes ADN des individus condamnés d'abord pour infractions sexuelles s'est étendue à d'autres infractions.

Cette demande de sécurité de plus en plus croissante a été à l'origine d'un important débat concernant la création du Fichier EDWIGE. Celui-ci devait comporter des données considérées comme sensibles, exemple : l'appartenance à un syndicat ou encore la religion des personnes concernées par ce traitement de données.

Aujourd'hui abandonné, ce projet, s'il avait fait l'objet d'une utilisation entre divers états, voire même avec des états non membres comme pour les autres fichiers de police, aurait pu être à l'origine de nombreuses dérives. Cependant il est possible qu'un tel projet finisse par être adopté dans les années à venir.

---

<sup>49</sup> FNAEG : Fichier National Automatisé des Empreintes Génétiques

## **B : La procédure applicable aux données qu'ils contiennent.**

Le transfert de données contenues dans les fichiers de Police nationaux relève de la coopération intergouvernementale. En Europe c'est par exemple le troisième pilier de l'Union Européenne qui est concernée. Cependant aucune norme précise n'a été défini à part les grands principes de respect des libertés fondamentales telles que protégées par la CESDH, ou encore la Déclaration Universelle des Droits de l'Homme et du Citoyen. Certains traités peuvent cependant signés entre les Etats pour garantir et fixé certaines modalités pour le transfert de données policières. C'est le cas par exemple du Traité de Prüm.

Le Traité de Prüm du 27 mai 2005 (aussi appelé Schengen III) est destiné à faciliter et à accélérer l'échange d'informations entre les autorités judiciaires pour permettre de comparer les empreintes ADN et permettre de coordonner les bases de données à des fins de prévention du terrorisme et de maintien de l'ordre et de la sécurité. Ce traité à été introduit dans le cadre de l'UE par une décision de 2008 qui permet l'échange de données entre états membres selon le principe de disponibilité.

Partiellement intégré aux acquis de l'UE, il prévoit l'échange de données génétiques, d'empreintes digitales et de données à caractère personnel, la constitution de patrouilles policières communes ainsi que d'autres formes d'intervention (gardes armés à bord des aéronefs, assistance lors d'événements de grande envergure, autorisation pour les forces de l'ordre de traverser les frontières en cas de danger imminent, etc.).

## **CHAPITRE II : Les données « PNR<sup>50</sup> ».**

Les données dites PNR ont provoqué de nombreux débats, notamment en raison de leurs particularités : elles sont collectées par des entreprises commerciales pour des raisons commerciales mais avaient vocation à être transmises à des autorités étatiques. Il fallait donc déterminer à quel pilier de l'UE, elles devaient être rattachées (Section I). Leur transfert n'a pas été plus simple à mettre en place et a fait l'objet d'un long processus de négociations (Section II).

### **Section I : Présentation des données « PNR ».**

Pour saisir les enjeux qui ont entouré les données dites PNR, il faut regarder les spécificités de ces données, par qui elles sont collectées et dans quel but (A) et ainsi comprendre le processus qui a permis de ne pas soumettre ces données aux champs restrictifs de la protection des données tels que mis en place par la Directive européenne de 1995 (B).

#### **A : Définition et catégories de données.**

Après les attentats du 11 septembre 2001, une psychose s'est installée aux Etats-Unis ayant pour conséquence la mise en place par le gouvernement américain d'une politique sécuritaire. Toute intrusion dans la vie privée des personnes, même exagérée, pouvait être justifiée par le besoin de sécurité et de poursuite des terroristes. Cette psychose concernant la sécurité a connu son apogée dans les aéroports où les contrôles aux frontières sont plus que jamais vigilants et même intrusifs.

C'est dans ce cadre que la loi américaine du 19 novembre 2001 sur la sûreté de l'aviation et des transports (Aviation and Transportation Security Act) créa l'obligation de transmission, par les compagnies aériennes assurant le transport de passagers au départ, à destination ou via les Etats-Unis ; de l'ensemble des données PNR de leurs passagers.

---

<sup>50</sup> PNR : « Passenger Name Records »

Ces données PNR peuvent se définir comme étant l'ensemble des données qu'une compagnie aérienne peut détenir lorsqu'un client effectue sa réservation auprès de cette compagnie. Cela peut être, par exemple, les renseignements sur l'agence de voyage auprès de laquelle la réservation est effectuée, ou encore les services demandés à bord de l'avion, tels que le numéro de place affecté à l'avance, les repas (végétarien, asiatique, cascher, etc.) et les services liés à la santé (diabétique, aveugle, sourd, assistance médicale etc.).

Ces données sont habituellement collectées par les compagnies aériennes non pour des raisons de sécurité, mais pour des raisons de fonctionnement interne. En effet les données fournies par un passager sur son régime alimentaire sont nécessaires pour la distribution des repas pendant le vol. Il en est de même pour les données liées à la santé qui sont obligatoires pour la gestion d'un vol.

### **B : Appartenance au troisième pilier.**

Le fait que les données PNR soient collectées par une entreprise commerciale dans un but commercial a incité la Commission Européenne à inclure les accords sur les données PNR dans le champ d'application de la Directive. Cette conception semblait aller dans le courant jurisprudentiel de la CJCE qui avait déjà considéré plutôt largement le champ d'application de la Directive de 1995 dans deux affaires antérieures.

Cependant dans son arrêt en date 30 mai 2006, la Commission Européenne dispose que le transfert de données PNR « constitue un traitement ayant pour objet la sécurité publique et les activités de l'Etat relatives à des domaines du droit pénal ». Elle exclut donc du champ d'application de la Directive de 1995 le transfert de données PNR vers les autorités américaines.

Elle exerce alors une interprétation au cas par cas, car les données issues de la collecte des compagnies aériennes, telles qu'elles, entrent bien dans le champ d'application de la Directive. Ce n'est que leur transfert vers les autorités américaines en vue d'assurer la sécurité de leur territoire qui est exclu du champ d'application de la Directive et rentre dans celui de la Décision-cadre proposée le 6 novembre 2007 par le Conseil de l'Union.

Mais cette application semble contraire à sa jurisprudence issue de l'arrêt *Österreichischer Rundfunk*<sup>51</sup> où elle avait jugé qu'il ne serait pas approprié d'interpréter l'expression : « activités qui ne relèvent pas du champ d'application du droit communautaire » comme ayant une portée telle qu'il serait alors nécessaire de vérifier, au cas par cas, si l'activité spécifique en cause affectait directement la libre circulation entre états-membres.

Elle justifie cette décision par le fait que « le traitement qui est pris en compte dans la décision d'adéquation possède une nature toute autre : cette décision (...) ne vise pas un traitement de données nécessaire à la réalisation d'une prestation de services, mais considéré comme nécessaire à la sauvegarde de la sécurité publique et à des fins répressives ». En effet, selon la CJCE « il ne ferait pas de doute que le traitement des données PNR après le transfert à l'autorité américaine visé par la décision d'adéquation est effectué, et le sera, pour l'exercice d'activités propres aux Etats au sens du point 43 de l'arrêt du 6 novembre 2003, *Lindqvist* ».

Si on peut penser que cette solution est conforme aux solutions retenues par la directive en date du 15 mars 2006<sup>52</sup> sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou

---

<sup>51</sup> Arrêt *Österreichischer Rundfunk* de la CJCE en date du 20 mai 2003

<sup>52</sup> Directive 2006/24/CE du parlement européen et du conseil sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications et modifiant la Directive 2002/58/CE

Article 1er: « La présente directive a pour objectif d'harmoniser les dispositions des États membres relatives aux obligations des fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications en matière de conservation de certaines données qui sont générées ou traitées par ces fournisseurs, en vue de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne.

de réseaux publics de communications, on peut se demander si cette solution ne révèle pas une volonté d'annuler l'accord d'adéquation de la Commission Européenne au vu du peu de garantie apporté par les Etats-Unis quant au sort des données une fois arrivées sur le territoire américain (conservation illimitée, transmissions à d'autres services que ceux mentionnés à l'origine...).

Décision d'espèce ou non, la cour annule l'accord d'adéquation de la commission en date du 29 mai 2004 portant sur le transfert vers les Etats-Unis des données PNR.

## **Section II : Les différents accords pour leur transfert.**

Si leur définition a suscité beaucoup de débats, leur transfert vers les Etats-Unis encore plus. En effet un premier accord entre la Commission Européenne et les Etats-Unis publié dans une décision de la Commission en date du 29 mai 2004 (A) fût annulé par la CJCE. Aujourd'hui ces données sont transférées aux autorités américaines en vertu d'un accord publié dans une décision de la Commission Européenne en date du 26 juillet 2007 (B).

### **A : La décision de la Commission Européenne en date du 14 et 29 mai 2004.**

Dans deux décisions en date du 14<sup>53</sup> et du 29 mai 2004, la Commission Européenne a rendu une décision concernant le niveau adéquat de protection de ses données qui comprenait les recommandations suivantes :

- un nombre plus réduit de données collectées et conservées par les autorités américaines (34 catégories de données sont transférées),
- les données sensibles permettant de révéler des indications sur la religion ou la santé ne seront plus transmises ou si elles le sont, seront filtrées et supprimées ultérieurement,
- les données ne pourront être utilisées que dans le cadre de la lutte contre le terrorisme et la grande criminalité,
- les données sont effacées après un délai maximal de trois ans et six mois, sauf pour les données consultées dans le cadre d'investigations spécifiques ou bien manuellement,
- les autorités américaines informent notamment les passagers sur la finalité du transfert et des traitements et sur l'identité du responsable des traitements,
- les personnes concernées disposent d'un droit d'accès et de rectification,

---

<sup>53</sup> 2004/535/CE : Décision de la Commission du 14 mai 2004 relative au niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférés au Bureau des douanes et de la protection des frontières des États-Unis d'Amérique

- les autorités chargées de la protection des données dans l'Union Européenne ont compétence pour assister les personnes dans le cadre d'une plainte auprès des autorités américaines,
- le tri des données ne pourra être effectué par les autorités américaines qu'au cas par cas et pour des objectifs convenus,
- le transfert des données vers d'autres autorités gouvernementales américaines ou étrangères se feront au cas par cas et après notification à une autorité désignée de l'Union Européenne,
- la Commission et des représentants des autorités de protection des données effectueront chaque année un bilan sur le respect de leurs engagements par les États-Unis.

Cet accord a été annulé par la CJCE dans une décision en date du 30 mai 2006, au vu des conditions inefficaces de protection qui étaient apportées aux données une fois qu'elles étaient arrivées sur le territoire américain et du fait que les dispositions de l'accord n'étaient pas satisfaisantes. Cependant l'annulation devant se fonder sur du droit et ne voulant pas désavouer la commission, la CJCE ne s'est basée que sur le champ d'application de la Directive de 1995.

## **B : L'accord actuel : Décision de la Commission en date du 26 juillet 2007.**

A la suite de l'annulation par la CJCE du premier accord, la commission a dû négocier un second accord plus restrictif en l'attente de l'adoption d'une décision cadre dont le projet a été présenté et est en cours de transposition dans l'ensemble des pays membres de l'Union Européenne.

Le nouvel accord conclu par l'Union Européenne comprenait l'envoi des données suivantes aux autorités américaines :

1. Code repère du dossier API/PNR
2. Date de la réservation
3. Date(s) prévue(s) du voyage
4. Nom du passager
5. Autres noms figurant dans les données API/PNR
6. Itinéraire complet
7. Identification des billets gratuits
8. Billet aller simple
9. Informations sur l'établissement des billets
10. Données ATFK (automatic ticket quote)
11. Numéro du billet
12. Date d'émission du billet
13. Passager répertorié comme défaillant
14. Nombre de bagages
15. Numéro de l'étiquette des bagages
16. Passager de dernière minute sans réservation
17. Nombre de bagages pour chaque segment
18. Sur-classement demandé/non demandé

19. Historique des changements apportés aux données API/PNR pour ce qui est des éléments précités

Toutes les données citées ci-dessus sont transmises au Department of Homeland Security des États-Unis (ministère de la sécurité intérieure), qui les recevra, puis éliminera les informations sensibles figurant dans les données PNR et n'en fera pas usage, sauf dans les cas exceptionnels où des vies sont en danger.

Concernant l'accès à ces données par d'autres services : il n'y aura pas d'accès direct inconditionnel à la base de données du Department of Homeland Security. L'accès sera strictement limité à ces fins et sera proportionné à la nature de l'affaire pour laquelle les données sont demandées. Les informations transmises par les passagers sur leurs habitudes alimentaires et utiles aux compagnies pour la distribution des plateaux repas pendant le vol seront transmises en même temps que les autres données mais seront considérées par le Department of Homeland Security comme des données sensibles.

Les données PNR seront conservées dans une base de données active pendant une durée de sept ans et par la suite sur une base de données inactive pendant une période de huit ans.

## **Bibliographie :**

« Biométrie et maîtrise des flux : vers une « géo-technopolis du vivant-en-mobilité » ? » P. Bonditti « Cultures & conflits » n°58 (2005) p 131-154

« Bases de données personnelles et politiques de sécurité : une protection illusoire ? » S. Preuss-Laussinotte « Cultures & conflits » n°64 (2006) p 77-95

« Enjeux d'identification et de surveillance à l'heure de la Biométrie » A.Ceyhan « Culture & conflits » n°64 (2006) p 33-47

« Données personnelles : des données personnelles à l'identité numérique » P. De la Faye, I.Daviaud, G.Le Grand, G.Haas et F.Jaspart « Lamy droit de l'immatériel » n°47 Mars 2009 p 85-90

« La protection des données à caractère personnel dans le contexte de la construction en pilier de l'Union Européenne » F ; Dumortier « Lamy droit de l'immatériel » juillet 2007

« Les autorités européennes prennent position sur le conflit du droit entre les règles de e-discovery et la protection des données à caractère personnel » O.Proust « Lamy droit de l'immatériel » 03/2009

« Les transferts internationaux de données dans la loi de 2004 » M.Vivant « Lamy droit de l'immatériel » 10/2005

« Flux transfrontières de données, vie privée et groupes d'entreprises » Y.Poullet « Lamy droit de l'immatériel » 09/2005

« La nouvelles loi Informatique et Libertés : les pouvoirs de contrôle à posteriori de la CNIL renforcés » F.Naftalski « Lamy droit de l'immatériel » 11/2004

« La CNIL, un obstacle aux transferts de données hors Union Européenne ? » M.Grigner « Lamy droit de l'immatériel » 04/2008

« Le conflit de droits entre les règles américaines de *e-discovery* et le droit européen de la protection des données à caractère personnel... Entre le marteau et l'enclume » O.Proust et C.Burton « Lamy droit de l'immatériel » Février 2009 p 79-84

« Aterritorialité des atteintes face aux logiques territoriales de protection juridiques et problème de l'absence d'homogénéité des législations protectrices (quid des safe harbor principes) » C. Chassigneux « Lex Electronica », vol 9 n°2 Numéro spécial hiver 2004

« Protection des données dans l'union européenne » publié par l'Office des publications officielles des communautés européennes.

« Droit et Internet » Marie Céline Halpern aux éditions de Vecchi

« Internet et protection des données personnelles » M-P Fenoll-Trousseau et G Hass  
Collection Droit@Litec, édition Litec

« Libertés et droits fondamentaux à l'épreuve de l'internet » A Lepage collection Juris  
classeur Droit@Litec aux éditions Litec

## **Webographie :**

<http://biosecure.it-sudparis.eu>

<http://www.cnil.fr/>

<http://fr.wikipedia.org/wiki/Accueil>

<http://ec.europa.eu>

<http://www.export.gov/safeharbor>

<http://www.vie-publique.fr>

<http://www.privacyconference2009.org>

<http://www.senat.fr/ue/pac/E3568.html>

<http://www.droit-technologie.org>

<http://www.ladocumentationfrancaise.fr>

<http://www.edps.europa.eu/EDPSWEB/edps/lang/fr/pid/1>

<http://www.laquadrature.net>

<http://www.cnpd.lu>

<http://www.journaldunet.com/>

<http://www.legalbiznext.com>

<http://www.zdnet.fr>

<http://www.europe-international.developpement-durable.gouv.fr>

<http://www.droit-technologie.org/>

<http://www.feral-avocats.com>

# **Annexe A : Extrait de la loi Informatique et Libertés** **du 6 janvier 1978.**

## **Chapitre Ier : Principes et définitions.**

**Article 2 :** « La présente loi s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l'exception des traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles, lorsque leur responsable remplit les conditions prévues à l'article 5.

Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.

Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.

La personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement. »

## **Chapitre II : Conditions de licéité des traitements de données à caractère personnel.**

### **Section 1 : Dispositions générales.**

**Article 6 :** « Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes :

1° Les données sont collectées et traitées de manière loyale et licite ;

2° Elles sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. Toutefois, un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et des procédures prévus au présent chapitre, au chapitre IV et à la section 1 du chapitre V ainsi qu'aux chapitres IX et X et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ;

3° Elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ;

4° Elles sont exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées ;

5° Elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées. »

## **Section 2 : Dispositions propres à certaines catégories de données.**

**Article 8 :** « I.-Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci.

II.-Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne sont pas soumis à l'interdiction prévue au I :

1° Les traitements pour lesquels la personne concernée a donné son consentement exprès, sauf dans le cas où la loi prévoit que l'interdiction visée au I ne peut être levée par le consentement de la personne concernée.

2° Les traitements nécessaires à la sauvegarde de la vie humaine, mais auxquels la personne concernée ne peut donner son consentement par suite d'une incapacité juridique ou d'une impossibilité matérielle.

3° Les traitements mis en œuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical :

-pour les seules données mentionnées au I correspondant à l'objet de la dite association ou du dit organisme,

-sous réserve qu'ils ne concernent que les membres de cette association ou de cet organisme et, le cas échéant, les personnes qui entretiennent avec celui-ci des contacts réguliers dans le cadre de son activité,

-et qu'ils ne portent que sur des données non communiquées à des tiers, à moins que les personnes concernées n'y consentent expressément.

4° Les traitements portant sur des données à caractère personnel rendues publiques par la personne concernée.

5° Les traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice.

6° Les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du code pénal.

7° Les traitements statistiques réalisés par l'Institut National de la Statistique et des Etudes Economiques ou l'un des services statistiques ministériels dans le respect de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques, après avis du Conseil National de l'Information Statistique et dans les conditions prévues à l'article 25 de la présente loi.

8° Les traitements nécessaires à la recherche dans le domaine de la santé selon les modalités prévues au chapitre IX.

III.-Si les données à caractère personnel visées au I sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la Commission Nationale de l'Informatique et des Libertés, celle-ci peut autoriser, compte tenu de leur finalité, certaines catégories de traitements selon les modalités prévues à l'article 25. Les dispositions des chapitres IX et X ne sont pas applicables.

IV.-De même, ne sont pas soumis à l'interdiction prévue au I, les traitements, automatisés ou non, justifiés par l'intérêt public et autorisés dans les conditions prévues au I de l'article 25 ou au II de l'article 26.

### **Chapitre III : La Commission Nationale de l'Informatique et des Libertés.**

**Article 11 :** « La Commission Nationale de l'Informatique et des Libertés est une autorité administrative indépendante. Elle exerce les missions suivantes :

1° Elle informe toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations.

2° Elle veille à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente loi.

A ce titre :

a) Elle autorise les traitements mentionnés à l'article 25, donne un avis sur les traitements mentionnés aux articles 26 et 27 et reçoit les déclarations relatives aux autres traitements.

b) Elle établit et publie les normes mentionnées au I de l'article 24 et édicte, le cas échéant, des règlements types en vue d'assurer la sécurité des systèmes.

c) Elle reçoit les réclamations, pétitions et plaintes relatives à la mise en œuvre des traitements de données à caractère personnel et informe leurs auteurs des suites données à celles-ci.

d) Elle répond aux demandes d'avis des pouvoirs publics et, le cas échéant, des juridictions, et conseille les personnes et organismes qui mettent en œuvre ou envisagent de mettre en œuvre des traitements automatisés de données à caractère personnel.

e) Elle informe sans délai le procureur de la République, conformément à l'article 40 du Code de Procédure Pénale, des infractions dont elle a connaissance, et peut présenter des observations dans les procédures pénales, dans les conditions prévues à l'article 52.

f) Elle peut, par décision particulière, charger un ou plusieurs de ses membres ou des agents de ses services, dans les conditions prévues à l'article 44, de procéder à des vérifications portant sur tous traitements et, le cas échéant, d'obtenir des copies de tous documents ou supports d'information utiles à ses missions.

g) Elle peut, dans les conditions définies au chapitre VII, prononcer, à l'égard d'un responsable de traitement, l'une des mesures prévues à l'article 45.

h) Elle répond aux demandes d'accès concernant les traitements mentionnés aux articles 41 et 42.

3° A la demande d'organisations professionnelles ou d'institutions regroupant principalement des responsables de traitements :

a) Elle donne un avis sur la conformité aux dispositions de la présente loi des projets de règles professionnelles et des produits et procédures tendant à la protection des personnes à l'égard du traitement de données à caractère personnel, ou à l'anonymisation de ces données, qui lui sont soumis.

b) Elle porte une appréciation sur les garanties offertes par des règles professionnelles qu'elle a précédemment reconnues conformes aux dispositions de la présente loi, au regard du respect des droits fondamentaux des personnes.

c) Elle délivre un label à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel, après qu'elle les ait reconnus conformes aux dispositions de la présente loi.

4° Elle se tient informée de l'évolution des technologies de l'information et rend publique le cas échéant son appréciation des conséquences qui en résultent pour l'exercice des droits et libertés mentionnés à l'article 1<sup>er</sup>.

A ce titre :

a) Elle est consultée sur tout projet de loi ou de décret relatif à la protection des personnes à l'égard des traitements automatisés.

b) Elle propose au Gouvernement les mesures législatives ou réglementaires d'adaptation de la protection des libertés à l'évolution des procédés et techniques informatiques.

c) A la demande d'autres autorités administratives indépendantes, elle peut apporter son concours en matière de protection des données.

d) Elle peut être associée, à la demande du Premier ministre, à la préparation et à la définition de la position française dans les négociations internationales dans le domaine de la protection des données à caractère personnel. Elle peut participer, à la demande du Premier ministre, à la représentation française dans les organisations internationales et communautaires compétentes en ce domaine.

Pour l'accomplissement de ses missions, la commission peut procéder par voie de recommandation et prendre des décisions individuelles ou réglementaires dans les cas prévus par la présente loi.

La commission présente chaque année au Président de la République, au Premier ministre et au Parlement un rapport public rendant compte de l'exécution de sa mission. »

## **Chapitre XII : Transferts de données à caractère personnel vers des Etats n'appartenant pas à la Communauté Européenne.**

**Article 68** : « Le responsable d'un traitement ne peut transférer des données à caractère personnel vers un Etat n'appartenant pas à la Communauté européenne que si cet Etat assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet.

Le caractère suffisant du niveau de protection assuré par un Etat s'apprécie en fonction notamment des dispositions en vigueur dans cet Etat, des mesures de sécurité qui y sont appliquées, des caractéristiques propres du traitement, telles que ses fins et sa durée, ainsi que de la nature, de l'origine et de la destination des données traitées.

**Article 69 :** « Toutefois, le responsable d'un traitement peut transférer des données à caractère personnel vers un Etat ne répondant pas aux conditions prévues à l'article 68 si la personne à laquelle se rapportent les données a consenti expressément à leur transfert ou si le transfert est nécessaire à l'une des conditions suivantes :

1° A la sauvegarde de la vie de cette personne ;

2° A la sauvegarde de l'intérêt public ;

3° Au respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice ;

4° A la consultation, dans des conditions régulières, d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime ;

5° A l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures précontractuelles prises à la demande de celui-ci ;

6° A la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers.

Il peut également être fait exception à l'interdiction prévue à l'article 68, par décision de la Commission nationale de l'informatique et des libertés ou, s'il s'agit d'un traitement mentionné au I ou au II de l'article 26, par décret en Conseil d'Etat pris après avis motivé et publié de la commission, lorsque le traitement garantit un niveau de protection suffisant de la vie privée ainsi que des libertés et droits fondamentaux des personnes, notamment en raison des clauses contractuelles ou règles internes dont il fait l'objet.

La Commission nationale de l'informatique et des libertés porte à la connaissance de la Commission des Communautés européennes et des autorités de contrôle des autres Etats membres de la Communauté européenne les décisions d'autorisation de transfert de données à caractère personnel qu'elle prend au titre de l'alinéa précédent.

**Article 70 :** « Si la Commission des Communautés européennes a constaté qu'un Etat n'appartenant pas à la Communauté européenne n'assure pas un niveau de protection suffisant à l'égard d'un transfert ou d'une catégorie de transferts de données à caractère personnel, la Commission nationale de l'informatique et des libertés, saisie d'une déclaration déposée en application des articles 23 ou 24 et faisant apparaître que des données à caractère personnel seront transférées vers cet Etat, délivre le récépissé avec mention de l'interdiction de procéder au transfert des données.

Lorsqu'elle estime qu'un Etat n'appartenant pas à la Communauté européenne n'assure pas un niveau de protection suffisant à l'égard d'un transfert ou d'une catégorie de transferts de données, la Commission nationale de l'informatique et des libertés en informe sans délai la Commission des

Communautés européennes. Lorsqu'elle est saisie d'une déclaration déposée en application des articles 23 ou 24 et faisant apparaître que des données à caractère personnel seront transférées vers cet Etat, la Commission nationale de l'informatique et des libertés délivre le récépissé et peut enjoindre au responsable du traitement de suspendre le transfert des données. Si la Commission des Communautés européennes constate que l'Etat vers lequel le transfert est envisagé assure un niveau de protection suffisant, la Commission nationale de l'informatique et des libertés notifie au responsable du traitement la cessation de la suspension du transfert. Si la Commission des Communautés européennes constate que l'Etat vers lequel le transfert est envisagé n'assure pas un niveau de protection suffisant, la Commission nationale de l'informatique et des libertés notifie au responsable du traitement l'interdiction de procéder au transfert de données à caractère personnel à destination de cet Etat.

# **Annexe B : Extrait de la Directive européenne du 24**

**Octobre 1995.**

## **CHAPITRE VI AUTORITÉ DE CONTRÔLE ET GROUPE DE PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL.**

### **Article 28 :**

Autorité de contrôle

1. Chaque État membre prévoit qu'une ou plusieurs autorités publiques sont chargées de surveiller l'application, sur son territoire, des dispositions adoptées par les États membres en application de la présente directive.

Ces autorités exercent en toute indépendance les missions dont elles sont investies.

2. Chaque État membre prévoit que les autorités de contrôle sont consultées lors de l'élaboration des mesures réglementaires ou administratives relatives à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel.

3. Chaque autorité de contrôle dispose notamment :

- de pouvoirs d'investigation, tels que le pouvoir d'accéder aux données faisant l'objet d'un traitement et de recueillir toutes les informations nécessaires à l'accomplissement de sa mission de contrôle,

- de pouvoirs effectifs d'intervention, tels que, par exemple, celui de rendre des avis préalablement à la mise en œuvre des traitements, conformément à l'article 20, et d'assurer une publication appropriée de ces avis ou celui d'ordonner le verrouillage, l'effacement ou la destruction de données, ou d'interdire temporairement ou définitivement un traitement, ou celui d'adresser un avertissement ou une admonestation au responsable du traitement ou celui de saisir les parlements nationaux ou d'autres institutions politiques,

- du pouvoir d'ester en justice en cas de violation des dispositions nationales prises en application de la présente directive ou du pouvoir de porter ces violations à la connaissance de l'autorité judiciaire.

Les décisions de l'autorité de contrôle faisant grief peuvent faire l'objet d'un recours juridictionnel.

4. Chaque autorité de contrôle peut être saisie par toute personne, ou par une association la représentant, d'une demande relative à la protection de ses droits et libertés à l'égard du traitement de données à caractère personnel. La personne concernée est informée des suites données à sa demande.

Chaque autorité de contrôle peut, en particulier, être saisie par toute personne d'une demande de vérification de la licéité d'un traitement lorsque les dispositions nationales prises en vertu de l'article 13 de la présente directive sont d'application. La personne est à tout le moins informée de ce qu'une vérification a eu lieu.

5. Chaque autorité de contrôle établit à intervalles réguliers un rapport sur son activité. Ce rapport est publié.

6. Indépendamment du droit national applicable au traitement en cause, chaque autorité de contrôle a compétence pour exercer, sur le territoire de l'État membre dont elle relève, les pouvoirs dont elle est investie conformément au paragraphe 3. Chaque autorité peut être appelée à exercer ses pouvoirs sur demande d'une autorité d'un autre État membre.

Les autorités de contrôle coopèrent entre elles dans la mesure nécessaire à l'accomplissement de leurs missions, notamment en échangeant toute information utile.

7. Les États membres prévoient que les membres et agents des autorités de contrôle sont soumis, y compris après cessation de leurs activités, à l'obligation du secret professionnel à l'égard des informations confidentielles auxquelles ils ont accès.

## **Article 29**

Groupe de protection des personnes à l'égard du traitement des données à caractère personnel

1. Il est institué un groupe de protection des personnes à l'égard du traitement des données à caractère personnel, ci-après dénommé «groupe».

Le groupe a un caractère consultatif et indépendant.

2. Le groupe se compose d'un représentant de l'autorité ou des autorités de contrôle désignées par chaque État membre, d'un représentant de l'autorité ou des autorités créées pour les institutions et organismes communautaires et d'un représentant de la Commission.

Chaque membre du groupe est désigné par l'institution, l'autorité ou les autorités qu'il représente. Lorsqu'un État membre a désigné plusieurs autorités de contrôle, celles-ci procèdent à la nomination d'un représentant commun. Il en va de même pour les autorités créées pour les institutions et organismes communautaires.

3. Le groupe prend ses décisions à la majorité simple des représentants des autorités de contrôle.

4. Le groupe élit son président. La durée du mandat du président est de deux ans. Le mandat est renouvelable.

5. Le secrétariat du groupe est assuré par la Commission.

6. Le groupe établit son règlement intérieur.

7. Le groupe examine les questions mises à l'ordre du jour par son président, soit à l'initiative de celui-ci, soit à la demande d'un représentant des autorités de contrôle ou de la Commission.

### **Article 30**

1. Le groupe a pour mission :

a) d'examiner toute question portant sur la mise en œuvre des dispositions nationales prises en application de la présente directive, en vue de contribuer à leur mise en œuvre homogène,

b) de donner à la Commission un avis sur le niveau de protection dans la Communauté et dans les pays tiers,

c) de conseiller la Commission sur tout projet de modification de la présente directive, sur tout projet de mesures additionnelles ou spécifiques à prendre pour sauvegarder les droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel, ainsi que sur tout autre projet de mesures communautaires ayant une incidence sur ces droits et libertés;

d) de donner un avis sur les codes de conduite élaborés au niveau communautaire.

2. Si le groupe constate que des divergences, susceptibles de porter atteinte à l'équivalence de la protection des personnes à l'égard du traitement des données à caractère personnel dans la Communauté, s'établissent entre les législations et pratiques des États membres, il en informe la Commission.

3. Le groupe peut émettre de sa propre initiative des recommandations sur toute question concernant la protection des personnes à l'égard du traitement de données à caractère personnel dans la Communauté.

4. Les avis et recommandations du groupe sont transmis à la Commission et au comité visé à l'article 31.

5. La Commission informe le groupe des suites qu'elle a données à ses avis et recommandations. Elle rédige à cet effet un rapport qui est transmis également au Parlement européen et au Conseil. Ce rapport est publié.

6. Le groupe établit un rapport annuel sur l'état de la protection des personnes physiques à l'égard du traitement des données à caractère personnel dans la Communauté et dans les pays tiers, qu'il communique à la Commission, au Parlement européen et au Conseil. Ce rapport est publié.

## **Annexe C : Les « safe Harbor principles »<sup>54</sup>**

**NOTICE:** An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party(1).

**CHOICE:** An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party(1) or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

For sensitive information (i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party treats and identifies it as sensitive.

**ONWARD TRANSFER:** To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party

---

<sup>54</sup> <http://www.export.gov/safeharbor>

would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing.

**SECURITY:** Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

**DATA INTEGRITY:** Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

**ACCESS:** Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

**ENFORCEMENT:** Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.