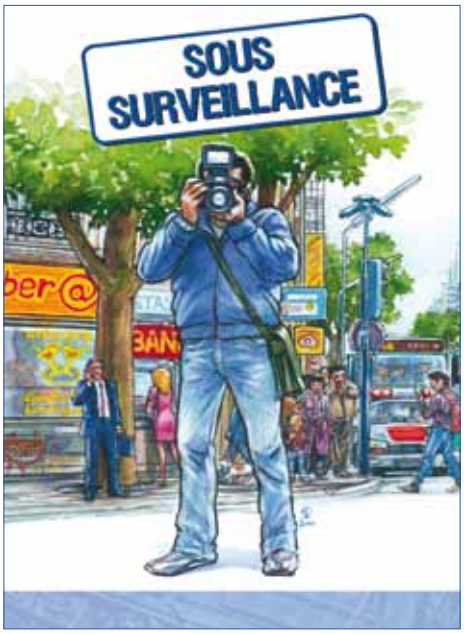
PROTECTION DES DONNEES PERSONNELLES

ANALYSE COMPAREE DES LEGISLATIONS ET DES PRATIQUES DANS NEUF PAYS EUROPEENS

DANS LE CONTEXTE DU CADRE JURIDIQUE EUROPEEN

- **Mobilité et transports**
- **Identité biologique**
- **Communications interpersonnelles**
- **Réseaux sociaux**



Coordination :
LDH, Ligue des droits de l'Homme

Partenaires :
AEDH, Association européenne pour la défense des droits de l'Homme
EDRi, European Digital Rights
Pangea, Coordinadora Comunicació per a la Cooperació
luRe, Iuridicum Remedium

JUIN 2010

PROTECTION
DES DONNEES PERSONNELLES

ANALYSE COMPAREE
DES LEGISLATIONS ET DES PRATIQUES
DANS NEUF PAYS EUROPEENS

DANS LE CONTEXTE DU CADRE JURIDIQUE EUROPEEN

- Mobilité et transports
- Identité biologique
- Communications interpersonnelles
- Réseaux sociaux

SOMMAIRE

1.INTRODUCTION - CONTEXTE

Dans le cadre de l'appel à propositions 2007 de la DG JLS « Droits fondamentaux et citoyenneté » la Ligue française pour la défense des droits de l'Homme et du citoyen a mis en place un programme visant à lancer une campagne de sensibilisation des jeunes adultes sur la protection de la vie privée et des données personnelles dans un contexte où les nouvelles technologies sont de plus en plus souvent utilisées dans la vie courante. En effet, cette utilisation généralisée des nouvelles technologies peut constituer une menace pour les libertés à l'insu de l'utilisateur s'il y a une insuffisance du cadre juridique et institutionnel et la méconnaissance de la façon dont les données personnelles peuvent être utilisées abusivement.
Deux réseaux européens, l'AEDH et EDRi et deux ONG nationales, IuRe et Pangea ont contribué à ce projet de façon à obtenir une étude comparative transnationale des législations et des pratiques et puis lancer une campagne de sensibilisation au niveau européen. Toutes ces structures sont impliquées dans la défense des droits de l'Homme et la protection des données personnelles.

Le résultat de notre travail comprend donc :

- Une vue d'ensemble comparative des législations de protection des données et des politiques dans les Etats membres de l'UE dans le cadre européen avec des recommandations visant à sensibiliser en priorité les autorités nationales et européennes (pour de meilleurs cadres juridiques, politiques et pratiques). Cette analyse comparative est basée sur :
  - neuf études nationales, pour recueillir des données éparses et les présenter dans une langue compréhensible par tous,
  - une présentation du cadre juridique européen et les tendances en matière de protection des données personnelles : texte unique disponible pour obtenir une description de toutes les initiatives pertinentes, évolutions et débats de ces dernières années.

  Ces études (450 pages environ) sont disponibles en anglais sur les sites de chaque partenaire.

- Une bande dessinée, pour la campagne de sensibilisation (cible principale : les jeunes adultes), traduite et publiée en 4 langues (CZ, EN, FR, SP) qui donne une approche très pédagogique, montrant que les TIC sont omniprésentes dans notre vie quotidienne et que la surveillance et le contrôle sont ainsi possibles partout, mais pas inéluctables. La bande dessinée papier est distribuée (80 000 copies) lors d'événements ciblant les jeunes adultes, organisés par ou avec l'appui des partenaires. Elle est mise à disposition dans les bibliothèques publiques, ainsi que dans les points d'information jeunesse. Elle est également disponible sur les sites de chacun des partenaires.

Ce document présente en six chapitres l'analyse comparée et les principales recommandations, en commençant par les rapports nationaux et la législation européenne :

- La méthodologie,
- Le cadre juridique européen (principales caractéristiques),
- Les cadres juridiques nationaux : principales caractéristiques et synthèse,
- Les autorités nationales de protection des données personnelles,
- Les thèmes étudiés (mobilité et transports, identité biologique, communications interpersonnelles, réseaux sociaux) et pour chacun des thèmes les risques principaux, les utilisations, les bonnes pratiques en matière de protection des données personnelles et les différences entre pays,
- Les recommandations.

Toutes les données rassemblées ici sont à jour à la date du 31/12/2009.

2. METHODOLOGIE - THEMES ETUDIES

Les pays que nous avons choisis pour l'étude sont les pays des trois partenaires nationaux : la France (FR), l'Espagne (ES) et la République tchèque (CZ) pour des études approfondies ainsi que l'Allemagne (D), le Royaume-Uni (UK), la Roumanie (RO), la Finlande (FI), les Pays-Bas (NL) et la Grèce (EL) pour des études plus courtes menées par les réseaux européens partenaires, l'AEDH et EDRi.

Par conséquent, nous avons pour l'analyse comparative un panel très représentatif des situations dans l'Union européenne qui prend en compte la diversité géographique, historique et culturelle.

À partir de la connaissance et de l'expertise de chaque structure, nous avons choisi collectivement (lors d'un premier séminaire à Paris en février 2009) les principaux thèmes que nous estimions pertinents par rapport à notre objectif final : la sensibilisation des jeunes adultes à la protection de leurs données personnelles lors de l'utilisation des nouvelles technologies dans la vie quotidienne.

Ces principaux thèmes sont : la mobilité et les transports, l'identité biologique, les communications interpersonnelles et les réseaux sociaux. Chaque partenaire était libre de choisir au sein de ces chapitres les principaux sujets pertinents en fonction de l'utilisation dans un pays donné, les dangers potentiels pour les libertés et les tendances.

Toutefois, un cadre commun pour l'analyse était indispensable pour permettre une analyse comparative par la suite. Ce cadre a été collectivement établi et adopté par tous les partenaires pour le travail national. La grille comprend : la technologie, les fichiers (ou bases de données) générés et les risques, les cadres juridiques d'utilisation, les utilisateurs et leur degré de prise de conscience, les conclusions et recommandations.

Chaque partenaire a produit des rapports nationaux avec des travaux basés sur :

- la mobilisation des compétences internes,
- des discussions internes afin de sélectionner les sujets pour chaque thème,
- les informations recueillies (recherche documentaire - Internet, rapports, etc.),
- les entretiens avec des experts sélectionnés,
- des questionnaires qui ont parfois été mis en place et soumis à certaines institutions ciblées (IuRe, Pangea).

Pendant ce temps, les deux réseaux européens (AEDH, EDRi) ont aussi travaillé sur une présentation du cadre juridique européen et ses évolutions sur les thèmes choisis.

Grâce à ces informations, l'analyse comparative a été réalisée par l'équipe de coordination et discutée lors d'une réunion transnationale (lors du 2e séminaire qui a eu lieu en septembre 2009 à Prague). Des recommandations ont été adoptées lors du 3e séminaire à Barcelone (février 2010).

Un expert externe de la protection des données personnelles a assuré un suivi de l'ensemble du projet et une évaluation approfondie de toutes ses étapes.

Les thèmes étudiés dans plusieurs pays :

- PNR (Passenger Name Record, dossier des données passagers) : CZ, FR, UK
- Cartes de transport : CZ, ES, FI, FR, NL
- Passeports biométriques : D, ES, FI, FR, RO, UK
- Bases de données ADN (pour les enquêtes de police) : CZ, EL, RO, UK
- Reconnaissance biométrique (utilisation dans le privé) : CZ, FR, NL
- Conservation des données : CZ, D, FI, FR, NL, RO, UK
- Réseaux sociaux nationaux : CZ, EL, ES, FI, FR, NL / soumis à la législation nationale
- Réseaux sociaux internationaux : CZ, D, ES, FR, RO, UK / prétendants être soumis principalement à la législation américaine

Les thèmes étudiés dans un seul pays :

Nous avons également eu quelques sujets pour lesquels un partenaire a souhaité apporter une contribution en fonction du contexte local :

- Communications interpersonnelles : courrier électronique, la téléphonie mobile, la messagerie instantanée : ES,
- Bases de données des jeunes (fichiers scolaires ou étudiants) : CZ,
- Vidéosurveillance (même si nous avons décidé de ne pas traiter ce sujet) : EL,
- La reconnaissance de plaques d'immatriculation : D,
- Géo localisation : FR,
- Les registres nationaux de la santé / dépôts centraux d'ordonnances électroniques : CZ,
- Les détecteurs de mensonge : EL.

Il est à noter que certains de ces thèmes sont néanmoins transversaux à certains pays (voire tous les pays), mais n'avaient pas été considérés comme étant au cœur de notre projet. Exemples : la vidéosurveillance ou les bases de données des jeunes qui ont été et sont l'objet de campagnes d'ONG dans les pays autres que CZ ou EL.

Les études se sont basées sur des recherches approfondies avec collecte des données et vérification des informations auprès d'experts juridiques et techniques et des partenaires.

3. LA LEGISLATION EUROPEENNE (LES GRANDES LIGNES)

Le cadre initial de la protection des données personnelles dans l'Union européenne et ses développements ultérieurs.

Dans le contexte de la construction européenne, une politique ambitieuse s'est développée depuis 1990 pour consacrer le droit à la protection des données personnelles qui s'est peu à peu dégradée pour partie en l'absence de moyens pour sa mise en œuvre effective, et aussi sous la pression « sécuritaire » dont la responsabilité incombe essentiellement au Conseil, à cause d'une profusion d'initiatives législatives, réglementaires et institutionnelles. L'entrée en vigueur du traité de Lisbonne sera-t-elle une opportunité pour changer cette tendance ?

La mise en place du cadre général du droit à la protection des données personnelles dans l'Union européenne dans les années 90 (ouverture des frontières, libre circulation des personnes, des biens et services), les évolutions de ces initiatives et leur impact sur la scène internationale.

■ La liberté de circulation des personnes

A l'approche de l'ouverture des frontières à la libre circulation des personnes, les gouvernements des Etats membres, en vue d'assurer la sécurité dans le territoire de l'Union, devaient en 1985 passer un accord, connu sous le nom d'accord de Schengen, visant à créer un fichier commun des personnes recherchées (ainsi que des objets, œuvres d'art et véhicules volés).

Les commissaires des Etats membres en charge de la protection des données à caractère personnel, préoccupés par l'absence de règles communes de nature à protéger les personnes concernées par ce fichier, obtiendront de telles garanties dans la convention intergouvernementale passée en 1990, établissant le système d'information (SIS I) et l'institutionnalisation d'une autorité de contrôle commune composée de leurs représentants. Cette convention sera par la suite intégrée au traité.

Suite à cette première légitime préoccupation gouvernementale, un déluge d'initiatives sécuritaires se focalise sur le suivi et le contrôle des mouvements de population grâce à l'identité biométrique. La politique suivie est inique, commençant par les populations les plus fragiles : les demandeurs d'asile dès 1990, puis les demandeurs de visa de court séjour à partir du 8 juin 2004, puis de long séjour, pour finir avec les citoyens des Etats membres avec le nouveau passeport européen (décision du Conseil du 13 décembre 2004) muni d'une puce lisible à distance, comprenant les empreintes digitales. Cette approche a été développée en collaboration avec les industriels du secteur pour qui elle avait valeur d'expérience sur le plan mondial (Il convient de souligner que par la suite, avec le soutien de l'Union européenne et de certains Etats membres, leurs produits et systèmes ont été déployés sur une grande échelle dans les pays du Sud – ex. : Congo, Côte d'Ivoire, Bénin - au moment des recensements effectués en vue d'élections « fiables » ou de l'introduction de l'OACI passeport électronique). Il n'existe toutefois aucune enquête indépendante sur les conditions de validité de la reconnaissance en cause, qui est particulièrement attentatoire à la personne humaine et à la souveraineté en cas d'invasion. La société civile mondiale a appelé à un moratoire sur l'utilisation de la biométrie (déclaration de Madrid du 3 novembre 2009).

La libre circulation des biens et services

Les commissaires en charge de la protection des données ont décidé, lors de leur conférence annuelle à Berlin en 1989, d'intervenir auprès de la Commission européenne pour qu'elle prenne une initiative visant à instaurer un régime de protection dans tous les Etats membres (alors inexistante dans six d'entre eux).

La Commission a alors proposé, en 1990, une politique cohérente et ambitieuse basée, dans son domaine de compétences, sur quatre propositions complémentaires visant à :

1. L'harmonisation des législations nationales applicables aux activités « relevant du droit communautaire », soit toutes les activités sauf celles des secteurs de la sécurité et de la défense.

La proposition de 1990 prévoyait des principes généraux développés à partir de ceux de la Convention 108 du Conseil de l'Europe, principe de finalité légitime, critère de licéité : le consentement, obligation légale, principe de proportionnalité/minimisation/nécessité/, protection renforcée des données sensibles en terme de discrimination (origines raciales ou ethniques, convictions religieuses, opinions politiques, santé etc.), principe de sécurité, droit des personnes à l'information, à accéder à leur données, à les corriger si nécessaire, droit de s'opposer à un traitement pour des motifs légitimes et de ne pas être soumis à des décisions automatiques, dérogations à ces principes limitées à ce qui est « nécessaire dans une société démocratique » pour la défense et l'ordre public et en accord avec la jurisprudence de la Cour européenne des droits de l'Homme de Strasbourg.

Ces principes étaient assortis de dispositions nouvelles sur le plan du droit international relatives à la mise en œuvre des législations (principe d'une autorité indépendante de protection des données personnelles) et aux garanties requises pour les transferts de données vers des pays tiers. Elle a également proposé une innovation en droit communautaire en prévoyant une double comitologie basée sur l'institutionnalisation à titre consultatif du groupe des autorités nationales, mais doté du pouvoir d'initiative pour les recommandations, et d'un comité des Etats membres compétent uniquement sur l'adéquation de la protection des données transmises à des pays tiers.

Cette proposition devait conduire à l'adoption le 24 octobre 1995 de la directive au Parlement et 95/46/CE du Conseil, relative à la protection des personnes au regard du traitement des données à caractère personnel et la libre circulation de ces données, texte fondateur, consistant et digne. Ce texte vise à assurer un « haut niveau » de protection des données personnelles sur tout le territoire de l'UE, afin que les Etats membres lèvent les barrières à la libre circulation des données.

L'adoption de ce texte aura quatre conséquences positives et immédiates, parfois imprévues, au niveau européen et mondial :

- La transposition de la directive dans tous les Etats membres (15 à l'époque), en particulier dans ceux qui n'avaient pas de législation dans ce domaine, puis dans tous ceux du Nord et de l'Est qui ont adhéré à l'Union (27) tout comme ceux des Etats de l'Espace économique européen (3).
- Le Conseil de l'Europe adoptera en 2003 un protocole additionnel à la Convention 108, ouvert à la signature des pays tiers, sur les innovations en matière d'autorité de contrôle et de transferts de données vers des pays tiers.
- Certains grands pays devaient trouver ici un argument supplémentaire à l'extension au secteur privé du régime de protection assuré jusque là uniquement dans le secteur public (l'Australie, le Québec suivi par le Canada au niveau fédéral).
- Cette directive constitue, encore aujourd'hui, le texte de référence pour tout pays, en particulier du Sud et de l'Est, s'interrogeant sur le cadre de protection des données à instaurer pour des motifs nationaux et pour une meilleure insertion dans le marché mondial, en répondant ainsi au critère de la « protection suffisante » fixée par la directive en matière de transferts de données vers des pays tiers.

Il convient d'ajouter que, en vertu des accords de l'OMC négociés au moment où la directive était élaborée (entre 1990 et 1994), l'année de l'adoption de l'Accord général sur les tarifs douaniers et le commerce (GATT), la Commission prendra, de manière très opportune, une initiative visant à permettre le refus d'accès à son territoire des acteurs économiques non conformes à ses règles sur la protection des données à caractère personnel.

La révision en cours de la directive de 1995 : cette directive, dont l'application n'a pas été significativement suivie par la Commission, a fait l'objet d'une consultation en 2009 en vue d'une éventuelle révision, en lien avec les évolutions technologiques et la mondialisation. L'AEDH et EDRi ont répondu à cette consultation voir : **http://ec.europa.eu.justice_home/news/consulting_public/news_consulting_0003_en.htm**

Il convient de mettre en exergue qu'au vu de la politique courageuse menée par l'Union européenne à l'origine, celle-ci détient une responsabilité mondiale dans ce domaine.

2. **L'application complémentaire des principes définis dans la directive générale en ce qui concerne les services particuliers offerts par les réseaux de télécommunications ouverts au public en cours de « dérégulation » (ouverture à la concurrence).**

La proposition de la Commission de 1990 adoptée en 1997 développe et rend contraignante une recommandation élaborée dans ce domaine au sein du Conseil de l'Europe. Les dispositions prévoient notamment le secret des correspondances, l'affichage ou non du numéro de l'appelant selon son souhait, appel par appel, la prospection électronique (par fax, composeur automatique etc.) sur la base du consentement, la protection des numéros appelés sur la facture détaillée à la demande de l'abonné, etc.

Cette directive dite « e-privacy » fut adaptée au contexte des communications électroniques en 2002 (prospection électronique soumise au consentement préalable du destinataire - e-mail, sms -, interdiction des logiciels espions et autres logiciels malicieux - internet, CD ROM, clef USB -) et fît l'objet d'une nouvelle adaptation (en 2009) pour prévenir de nouveaux risques (perte ou vol de fichiers). Dans le cadre de la négociation, la société civile se bat contre l'approche de la « réponse graduée » automatique visant le téléchargement illégal d'œuvres protégées par droit d'auteur et vise à garantir au moins que l'auteur du téléchargement ait droit à un procès équitable.

3. **L'établissement d'un cadre juridique et institutionnel d'application aux institutions et organes européens**

Le traité d'Amsterdam adopté en 1997 a été l'occasion de constitutionaliser le Contrôleur européen de la protection des données personnelles. Le règlement proposé en 1990 adopté le 18 décembre 2000 par le Parlement et le Conseil reprend l'intégralité des principes de la directive et prévoit, pour sa mise en œuvre, un Contrôleur européen de la protection des données (CEPD) et un adjoint, désignés par le Conseil et le Parlement sur proposition de la Commission, après un appel à candidatures et examen par un jury indépendant. Le contrôleur est appuyé par des délégués à la protection des données dans chaque institution et organisme communautaires. Ses pouvoirs de contrôle a priori dans les matières à risques et d'enquêtes a posteriori, s'étendent à la consultation comme pour le G29, dont il est membre, sur toute initiative européenne ayant des implications sur la protection des données. Il peut également être entendu en tant que de besoin, par la Cour de justice de Luxembourg.

4. **L'établissement d'une politique de sécurité des systèmes d'information**

Les quatre initiatives d'origine constituaient une politique ambitieuse qui trouvera un autre achèvement dans la Charte européenne des droits de l'Homme qui consacrera dans son article 8 le droit à la protection des données personnelles et le principe d'une autorité indépendante pour sa supervision.

Une telle consécration est à saluer tant il apparaît aujourd'hui que le droit à la protection des données sous-tend l'exercice des autres libertés et droits fondamentaux.

Principaux problèmes liés aux activités de sécurité

L'Union européenne se définit comme un espace démocratique où les libertés fondamentales sont reconnues, mais pour des raisons sécuritaires, les politiques européennes ne cessent d'être en contradiction avec ces valeurs démocratiques.

Ainsi la directive du Parlement et du Conseil du 15 mars 2006 sur la conservation des données générales générées et traitées dans le cadre de l'accès aux services de communication sur les réseaux de communication ouverts au public qui impose aux fournisseurs de tels services, de garder de 6 à 24 mois (selon le choix des Etats) toutes les données de connexion de leurs clients, est une atteinte très grave à toutes les libertés

de communication et d'information. Sa transposition n'est pas sans poser des problèmes dans les Etats membres où des discussions ont encore lieu. Elle doit être abandonnée !

Le **traité de Prüm** signé en 2005 pour lutter « contre le terrorisme, la criminalité transfrontalière et la migration illégale », résume par son titre une orientation qui met sur le même plan, immigration irrégulière, terrorisme et criminalité. Une politique européenne, à la fois sectorielle, sélective et utilitariste des migrations va être imposée par les Etats, à partir de juillet 2001, justifiée et amplifiée par les événements du 11 septembre. Contrôles et surveillance vont accompagner des politiques dites de « sécurité » au dépend du respect de la vie privée et des libertés.

Ainsi, en 2005, le programme de La Haye affirme : « Il serait inadmissible que le maintien effectif de l'ordre public et les enquêtes relatives à la criminalité transfrontière dans un espace de libre circulation soient entravés par des procédures contraignantes d'échange d'informations ». Passer outre ces procédures contraignantes signifie échanger des fichiers de données personnelles disponibles au niveau des Etats en les rendant interopérables, c.à.d. rendre les fichiers plus performants et pouvoir en créer de nouveaux, c'est aussi développer les échanges internationaux de bases de données, y compris celles détenues par des opérateurs privés quitte à les détourner de leur finalité.

L'orientation sécuritaire prend le parti que la sécurité des personnes passe par une limitation de la protection du droit de la vie privée au prétexte que seuls ceux qui auraient quelque chose à cacher sont visés par ces mesures. C'est une question de protection des personnes et de leur liberté, par exemple, de « trouver des solutions équilibrées, respectant intégralement les droits fondamentaux relatifs à la protection de la vie privée et à la protection des données, ainsi que le principe de disponibilité des informations ». On aboutit de fait à privilégier la disponibilité des informations par rapport à la protection de la vie privée et des libertés individuelles.

Ainsi, la décision-cadre du Conseil du 27 novembre 2008 (2008/977/JAI) sur la protection des données personnelles traitées dans le cadre la coopération policière et judiciaire prévoit un régime de protection des personnes à la baisse et ne concernant que les données « disponibles » qui seraient échangées et non toutes celles qui dans le même cadre seraient traitées sur le plan national !

Par ailleurs, il s'agit aussi de répondre à la fois à un besoin économique et à un besoin sécuritaire. D'un point de vue économique, économie du tourisme, activité des entreprises, etc., il faut fluidifier la circulation des voyageurs aux frontières et à l'intérieur de l'Union. Du point de vue sécuritaire, il faut fermer les frontières pour empêcher l'immigration irrégulière, dissuader les personnes jugées indésirables de venir en Europe, identifier les terroristes et les criminels potentiels.

Il en résulte un empilement législatif et de bases de données pour surveiller les entrées, les séjours et les sorties de l'Union européenne dont le contrôle est assuré par autant d'autorités communes composées de représentants des autorités de protection des données nationales ou du Contrôleur européen en coopération avec elles.

Premiers éléments de ce dispositif, les **Systèmes d'Information Schengen, SIS et SIS 2** intègrent des éléments biométriques d'identification des personnes concernées et des éléments d'identification d'objets. Si un tel système parait légitime pour identifier les personnes condamnées ou recherchées, la question se pose du bien-fondé du fichage de nombreuses personnes par exemple de celles simplement « soupçonnées ». Les recours montrent les abus qui peuvent être commis.

Le Système d'Information sur les Visas, VIS évoluant vers VIS 2 permet de comparer des données biométriques contenues dans une puce électronique, en particulier les empreintes digitales. Dans son principe, le visa biométrique vise à faciliter l'entrée dans l'espace européen Schengen. Il permet aussi de repérer ceux qui pourraient oublier d'en sortir à l'expiration de leur visa.

Le fichier « **EURODAC** » assure le contrôle des demandeurs d'asile et des réfugiés, il permet la comparaison de dix empreintes digitales pour rendre « efficace » le règlement qui définit les conditions communes de l'asile (le règlement de Dublin assignant le demandeur d'asile dans le pays de l'Union où il est entré en Europe).

Les citoyens de l'Union européenne qui voyagent ne sont pas exempts de contrôles pour entrer et sortir de l'Union. Leurs **passeports** doivent dorénavant comporter des éléments biométriques, et les enfants doivent avoir un passeport individuel. Le passeport comporte dans une puce électronique, une photo faciale et des empreintes digitales numérisées. En passant son doigt sur un capteur électronique cela devrait permettre au final d'éviter tout contrôle à l'entrée et à la sortie de l'espace Schengen. Le passage de la frontière sera libre en apparence, en réalité sous surveillance. Innocent : rien à craindre ! Oui mais fiché, et déplacements surveillés et sans être à l'abri d'une erreur.

Pour les résidants de long séjour des pays tiers, le titre de séjour a été uniformisé et incorpore aussi des éléments de reconnaissance biométrique. La voie est ainsi ouverte à la mise en place d'un fichier européen ad hoc. Ceci permettra d'accompagner les politiques d'immigration sélectives comme celle des travailleurs hautement qualifiés. Les hommes et les femmes qui viennent et travaillent dans nos pays sont-ils de simples produits dont on doit assurer la traçabilité ?

Pour les délinquants, ou soupçonnés de l'être, des **fichiers ADN** sont mis en place dans chaque pays et rendus accessibles aux autorités policières des autres pays européens. Un méga fichier européen ADN se constitue donc afin de « … créer un système d'informations policières moderne afin de pouvoir lutter efficacement, à échelle européenne, contre des malfaiteurs ». C'est l'identité de millions de personnes qui est ainsi répertoriée et conservée en Europe, souvent pour des délits mineurs, pour beaucoup parce que l'on a « oublié » d'effacer ceux entendus comme simples témoins ou ceux soupçonnés et innocentés. La Cour de Luxembourg a condamné les Etats responsables de tels oublis, sans aucun effet sur la croissance des fichiers ADN.

A tout ceci s'ajoutent des fichiers plus anciens ou nouveaux de coopération policière et judiciaire en Europe : **EUROPOL** concerne les auteurs (ou présumés tels) d'infraction, avec le projet de permettre l'accès aux fichiers Eurodac ; **EUROJUST** permet la consultation des fichiers disponibles dans le cadre des actions judiciaires pénales ; **ECRIS** est relatif à la consultation des casiers judiciaires, dans un contexte où la définition des crimes et des délits, l'inscription des condamnations dans les casiers et leur accès n'est pas la même dans tous les pays de l'Union.

L'Union européenne se propose de consolider tout ceci par la mise en place **d'EUROSUR**, un « super » système de surveillance des frontières, qui « devrait fournir le cadre technique commun permettant de rationaliser la coopération et la communication quotidienne », et d'utiliser des nouveaux outils de surveillance : capteurs, satellites et drones qui se couplent avec les fichiers de données personnelles existants ou à créer.

De plus, la législation européenne oblige les opérateurs de télécommunications et d'Internet à conserver les données d'identification des personnes ayant téléphoné, échangé des courriels et consulté des sites Internet. L'objet est de disposer d'un instrument « pour la prévention, la recherche, la détection et la poursuite d'infractions pénales, notamment en matière de crime organisé ».

Enfin des accords internationaux permettent la transmission de données personnelles à des pays tiers. Il faut citer l'accord PNR avec les Etats-Unis (Passenger Name Record : dossier standardisé lié à chaque réservation aérienne) qui permet la transmission, aux autorités américaines, de 19 rubriques de données personnelles concernant les voyageurs aériens qui survolent le territoire des Etats-Unis ou qui s'y rendent. Les garanties données par les autorités américaines, sur leur traitement, leur conservation, leur transmission, leur utilisation sont totalement insatisfaisantes. Cependant, l'Union européenne persiste dans sa volonté de prolonger cet accord et pense généraliser les PNR à l'ensemble du transport aérien européen.

■ Conclusions

Une Europe sous haute surveillance pourquoi ? Pour quelle efficacité ? Vouloir aller encore toujours plus loin alors qu'il est d'abord nécessaire de faire une évaluation sérieuse de la pertinence d'un tel système de fichiers.

S'il peut être justifié d'accéder à des informations est-il pour autant acceptable que ce soient les Etats eux-mêmes qui soient les garants de l'utilisation des données fournies par un autre pays. Une autorité indépendante européenne doit garantir le contenu des fichiers, leur finalité, leur proportionnalité, leur accessibilité, leur durée de conservation, leur effacement.

La finalité des fichiers doit être respectée. La durée de conservation des données est généralement trop longue par rapport à cette finalité et devrait dans la plupart des cas être considérablement réduite. L'usage de la biométrie doit être strictement limité.

L'Union européenne doit se mettre elle-même en conformité avec sa propre législation de protection des données personnelles, avec la Charte des droits fondamentaux, avec la Convention européenne des droits de l'Homme. D'autant que la multiplication des fichiers de données personnelles, leur juxtaposition, les risques d'interopérabilité, constituent une atteinte à l'intégrité mêmes des personnes concernées.

4. LES CADRES JURIDIQUES NATIONAUX CONCERNANT LA VIE PRIVEE ET LA PROTECTION DES DONNEES PERSONNELLES

Les différents cadres constitutionnels, institutionnels et juridiques sont naturellement liés à l'histoire de chaque pays. De ce fait la protection des données personnelles a des racines et parfois des significations très différentes. La mise en œuvre des directives européennes tend à combler les écarts entre les législations nationales, sans toutefois effacer complètement leurs caractéristiques, du fait de la marge d'appréciation laissée par ces directives, d'une mise en œuvre peu adéquate, et de l'interprétation nationale des principes - d'autant plus que, dans chaque cas la pression de l'opinion publique peut conduire à des changements au niveau réglementaire ou législatif et influencer les pratiques. L'examen de la transposition des directives montre qu'il existe une marge de manœuvre au niveau national soit pour renforcer les contrôles et les options sécuritaires et/ou pour permettre une gestion des données très libérale, soit pour donner la priorité à la protection des données personnelles.

En outre, une législation qui semble satisfaire aux exigences de la protection des données peut être rendue inefficace par ses procédures d'application, sa non application, un manque de ressources allouées, ou des limitations imposées par d'autres entités juridiques qui restreignent son champ d'application.

Il convient également de souligner que l'Union européenne peut permettre une progression dans certains pays sur la question de la protection des données alors que dans d'autres pays elle sape au nom de la sécurité et des mesures antiterroristes, etc., les principes établis.

Une typologie des pays peut ainsi être esquissée :

- **Les pays dans lesquels la situation correspond à une longue tradition de principes établis sur la protection des droits et libertés individuelles. La protection des données personnelles fait partie de cette tradition, alors que des changements législatifs actuellement en cours donnent progressivement la priorité aux questions de sécurité et de contrôle plutôt qu'à la protection des données personnelles et des libertés individuelles.**
- **Les pays dans lesquels l'histoire a induit de fortes craintes concernant les données enregistrées sur le fichier et dans lesquels, en réaction, une grande attention est accordée à la protection des données personnelles. La législation reste très attentive et est étroitement liée à l'opinion publique, même en cette période sécuritaire.**
- **Les pays dans lesquels la question de la protection des données personnelles est émergente et dans lesquels un cadre législatif est encore en cours d'élaboration, en lien avec leur entrée dans l'Union européenne. L'application des textes n'est souvent pas encore une réalité dans tous les domaines.**

La Grèce

■ La constitution et la protection des données personnelles

L'article 9 de la Constitution protège le droit à la vie privée : « Le domicile de chaque personne est un sanctuaire. La vie privée et familiale de l'individu est inviolable. Aucune recherche ne doit être faite au domicile, sauf dans les cas spécifiés par la loi, et toujours en présence de représentants des pouvoirs judiciaires. Les contrevenants à la disposition précédente sont punis pour violation de domicile et abus de pouvoir, et seront responsables de tout dommage à la victime, comme spécifié par la loi ». L'article 9 bis ajouté en 2001 établit le droit à la protection des données et constitutionnalise l'Autorité de protection des données. «Tout individu a le droit d'être protégé contre la collecte, le traitement et l'utilisation, en particulier par des moyens électroniques, de ses données personnelles, telles que spécifiées par la loi. Le droit à la protection des données est garanti par une autorité indépendante dont la composition et le fonctionnement sont fixés par la loi ».
L'article 19 de la Constitution protège la confidentialité des communications : « Le secret des courriers et

de toutes les formes de la libre correspondance ou communication est absolument inviolable. Les garanties en vertu desquelles l'autorité judiciaire ne doit pas être liée par ce secret pour des raisons de sécurité nationale ou pour enquêter sur des crimes particulièrement graves doit être spécifié par la loi ». La modification de 2001 ajoute deux nouvelles dispositions à cet article. Elle établit une autorité indépendante chargée de superviser les questions relatives aux télécommunications. L'article 19 (2) indique maintenant : « Les questions relatives à l'établissement, au fonctionnement et aux pouvoirs de l'autorité indépendante garantissant le secret défini au paragraphe 1 sont fixées par la loi. » L'article 19 (3) stipule que : « l'utilisation d'éléments de preuve obtenus en violation du présent article et des articles 9 et 9A est interdite en vertu de l'article 9bis de la Constitution grecque ».

■ Transposition des directives européennes

La loi grecque de protection des données a été écrite pour transposer directement la directive de l'UE sur la protection des données (95/46/CE). Cette loi est également nécessaire pour adhérer à l'accord de Schengen. La Grèce a aussi inclus dans son droit national l'ensemble des directives de l'UE sur la protection des données personnelles dans le secteur des télécommunications, à l'exception de la directive la plus récente sur la rétention des données.

■ Spécificités nationales

Un amendement présenté en décembre 2007 a introduit la non application de la protection des données pour les tribunaux, les procureurs lorsque nécessaire pour des enquêtes criminelles et l'administration de la justice. Cet amendement permet également l'enregistrement audio et vidéo lors de manifestations, pour confirmation de crimes, et en cas de menace imminente à l'ordre public. Cette disposition légale est, dans son principe, contraire au droit constitutionnel de liberté de réunion. En 2009, une autre modification annoncée exclut les enregistrements audio et vidéo des dispositions de la loi 2472/1997 sur la protection des données personnelles sensibles ! Enfin, un autre amendement a été examiné afin de créer une base de données d'ADN des délinquants pour la plupart des crimes du Code pénal. Fin juin 2009, le procureur de la Cour suprême du pays a déclaré que la confidentialité des communications ne s'applique pas aux communications sur Internet et aux éléments externes de communication. Les autorités de poursuite et d'enquête sont en droit de demander aux fournisseurs d'accès des éléments extérieurs à la communication. ADAE n'a pas le droit de vérifier si les exigences sont légitimes ou non. Par conséquent, toutes sortes d'autorités peuvent avoir accès au contenu des e-mails, « chats » et des conversations Skype – ce qui peut être considéré comme contraire au Code pénal, qui considère la violation de la vie privée comme un acte criminel.

La Roumanie

■ La constitution et la protection des données personnelles

La Roumanie n'a pas un long historique sur la vie privée et la protection des données personnelles. Bien qu'avant 1989, le droit à la vie privée ait été reconnu comme un droit de l'Homme fondamental, il a souvent été bafoué, notamment par les intrusions de la Sécurité roumaine. Des perquisitions sans mandat, avec ou sans raison, la réquisition de biens personnels, de revues ou de notes simplement parce qu'ils pouvaient contenir des opinions critiques sur le régime en place, et l'interception et le contrôle de la correspondance et des appels téléphoniques étaient pratique courante. Des changements majeurs dans ce domaine ne sont intervenus qu'après la révolution de décembre 1989. La première référence au droit à la vie privée est apparue dans la Constitution adoptée en 1991. Bien que l'institution d'Avocat du Peuple ait été créée par la Constitution de 1991, elle n'a pratiquement commencé ses activités qu'en 1997 et n'a traité que quelques cas relatifs au droit à la vie privée. Des modifications législatives ont commencé avec le processus d'intégration européenne qui a imposé des règlements spécifiquement pour la protection des données personnelles (2001). La Constitution de la Roumanie, adoptée en 1991 reconnaît, en vertu du titre II (Droits fondamentaux, libertés et devoirs) le droit à la vie privée, l'inviolabilité du domicile et la liberté de conscience et d'expression. Une dérogation est autorisée par la loi dans les circonstances suivantes : pour effectuer un mandat d'arrêt ou une décision de justice, pour éliminer tout danger pour la vie ou l'intégrité physique ou les biens d'une personne, pour défendre la sécurité nationale ou l'ordre public, pour prévenir la propagation d'une épidémie. Les recherches ne peuvent être ordonnées que par un magistrat et doivent être menées conformément à la procédure judiciaire. Les perquisitions de nuit sont interdites, sauf dans les cas de flagrant délit. Il existe également des dispositions constitutionnelles relatives au secret des communications et de la liberté d'expression.

■ Transposition des directives européennes

En novembre 2001, le Parlement a promulgué la loi 676 / 2001 sur le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications et la loi 677/2001 sur la protection des personnes concernant le traitement des données à caractère personnel et la libre circulation de ces données. Ces lois suivent respectivement de très près les directives de l'Union européenne sur le secret des télécommunications (1997/66/EC) et sur la protection des données (1995/46/CE). En 2004, la loi 676/2001 a été pratiquement remplacée par la loi 506/2004, qui suit de près la Directive 2002/58/CE du Parlement et du Conseil européens concernant le traitement des données personnelles et la protection de la vie privée dans le secteur des communications électroniques (publié au *Journal officiel de la Communauté européenne* N° L.201/31.07.2002).

Le Royaume-Uni

■ La constitution et la protection des données personnelles

Le Royaume-Uni n'a pas de Constitution écrite, mais le « Human Rights Act » de 1998 prévoit l'incorporation des droits énoncés dans la Convention européenne des droits de l'Homme, y compris l'article 8 sur le droit à la vie privée. Cette intégration pourrait toutefois faire l'objet de certaines dérogations et réserves.

■ Transposition des directives européennes

La protection des données est régie par la loi sur la protection des données de 1998, comme une transposition de la directive européenne sur la protection des données. Elle s'applique aux organismes publics et privés. Elle énonce huit principes de protection des données, en imposant que toute personne qui traite des données à caractère personnel doit s'assurer que ces données sont : traitées loyalement et licitement ; traitées à des fins limitées ; adéquates, pertinentes et non excessives ; exactes et à jour ; conservées pour une durée limitée à ce qui est nécessaire ; traitées conformément aux droits de la personne ; sécurisées et non transférées à d'autres pays sans protection adéquate. La loi prévoit aussi des droits individuels en ce qui concerne le traitement de données à caractère personnel, y compris le droit d'accéder à ces données.

■ Spécificités nationales

Toutefois, ces droits ont des limites dans la pratique. Par exemple, les enfants de plus de 12 ans peuvent déposer eux-mêmes des plaintes auprès des contrôleurs de données et exercer leur droit d'accès à leurs renseignements personnels en remplissant une « demande d'accès à l'objet ». Cela pourrait sembler une réelle avancée pour les droits, l'autonomie et la vie privée des enfants et des jeunes vis-à-vis de leurs parents. Cela disqualifie toutefois des plaintes et des demandes déposées par les parents, cependant, puisque dans le cadre actuel les enfants peuvent les déposer eux-mêmes. De même, lorsque le consentement est nécessaire, les enfants de plus de 12 ans peuvent donner le leur. La question de savoir si ce consentement est libre et éclairé peut évidemment être soulevée ici. La loi de protection des données personnelles (Data Protection Act) est considérée comme complexe, difficile à comprendre et à utiliser, et c'est donc une transposition concrètement peu effective de la directive européenne sur la protection des données. Le Bureau du commissaire à l'information du Royaume-Uni a élaboré une série de FAQ et autres documents pour l'application pratique de cette loi. Le droit à la vie privée et à la protection des données en ce qui concerne le traitement des renseignements personnels par le gouvernement et les organismes publics est cependant limité par d'autres textes législatifs spécifiques. L'article 12 de la loi sur l'enfance de 2004 sur les bases de données permet la mise en place de bases de données nationales des enfants par le gouvernement. D'autres textes législatifs restreignant la vie privée et les droits de protection des données sont mentionnés dans les fiches d'information données pour ce chapitre.

L'Espagne

■ La constitution et la protection des données personnelles

La Constitution espagnole (1978) reconnaît à l'article 18 le droit à la vie privée (personnelle, familiale, domicile), et le secret des communications.

« 1. Le droit à l'honneur, à l'intimité personnelle et familiale et à sa propre image est garanti. 2. Le domicile est inviolable. Aucune intrusion ou recherche ne peut être faite sans le consentement de l'occupant ou sans

un mandat judiciaire, sauf dans les cas de flagrant délit. 3. Le secret des communications est garanti, notamment en matière de communications postales, télégraphiques et téléphoniques, sauf dans le cas d'une ordonnance du tribunal. 4. La loi limitera l'usage de l'informatique afin de garantir l'honneur et l'intimité personnelle et familiale des citoyens et le plein exercice de leurs droits » (Constitution espagnole). L'article 18.4 prend explicitement en considération les responsabilités législatives en matière de TIC (traitement de données) et la première loi sur la protection des données (LORTAD, 1999) qui a développé un article de réglementation des archives contenant des traitements automatisés des données personnelles.

■ Transposition des directives européennes

Les législations nationales qui régissent l'information en ligne et la communication mettent en œuvre les directives européennes au niveau national. Les principales lois sont :

- La loi de Protection des données (LOPD, 1999) qui régit les procédures de gestion des bases de données contenant des renseignements personnels, et la vie privée en général. Elle est conforme à la directive UE CE 95/46,
- La loi sur le Commerce électronique (LSSI, 2002) qui met en œuvre la directive 2000/31/CE, la directive 98/27/CE (partiellement) et la loi 56/2007 sur les « Mesures pour le développement de la société de l'information ». Ces lois concernent les communications électroniques, ainsi que la réglementation des prestations de services électroniques, y compris les obligations concernant l'exploitation des données du client. Elles définissent entre autres, le service universel, les types d'informations publiques qui doivent être publiées, les obligations du gouvernement et celles des fournisseurs d'accès pour les obligations de service à la clientèle, ainsi que les obligations pour les sites Internet tels que l'accessibilité,
- La loi Administration électronique (LAECSP, 2007) qui reconnaît le droit des citoyens à l'interaction en ligne avec l'administration publique et oblige le gouvernement à garantir ce droit.

■ Spécificités nationales

La législation espagnole est plutôt avancée ; la LOPD est très sévère et il y a suffisamment de mécanismes de sanctions. Mais les procureurs sont dépassés et ne peuvent pas répondre immédiatement, ou prévenir les abus. L'activité proactive fait défaut notamment dans le domaine d'un pouvoir a priori de l'Autorité de protection des données (DPA) à l'égard de traitements prévenant un niveau de risques élevé pour les libertés, sauf pour le transfert des données vers des pays tiers qui sont soumis à l'autorisation de la DPA. L'actuelle loi de protection des données date de 1999 et est le résultat de la directive européenne de 1995. Il y a 14 ans que la base de ces droits a été établie. Une adaptation à la réalité actuelle est nécessaire puisque toute personne qui utilise un système basé sur Internet est dans une position dangereuse (par exemple la création d'un blog). La mondialisation brouille la notion de territorialité, et remet en question la nature même des lois et des dispositifs juridiques associés.

L'Allemagne

L'Allemagne a un développement du droit à la vie privée unique en Europe. Son interprétation par la Cour constitutionnelle a eu un impact majeur sur la législation sur la protection des données et aussi, dans une certaine mesure, sur celles des autres pays européens.

■ La constitution et la protection des données personnelles

La confidentialité des communications a été incluse dans la Constitution allemande à l'article 10 dans la version adoptée en 1949. Mais la Constitution allemande (Grundgesetz für die Bundesrepublik Deutschland) a également inclus dans les premiers articles du texte (articles 1 (1) et 2 (1)) le droit à la liberté individuelle (Persönlichkeitsrecht).

■ Transposition des directives européennes

La loi fédérale allemande sur la protection des données a été révisée à plusieurs reprises au fil des ans, avec une révision majeure en 2002 afin de transposer la directive européenne sur la protection des données. La modification la plus récente a été faite le 15 novembre 2006. L'objectif général de cette loi est de protéger les personnes physiques contre la mauvaise utilisation de leurs données personnelles. La loi couvre la collecte, le traitement et l'utilisation de données personnelles par les autorités publiques fédérales et les administrations d'Etat (tant qu'il n'y a pas de régulation par l'Etat et dans la mesure où les lois fédérales s'appliquent), et par les organismes privés, s'ils s'appuient sur des systèmes de traitement des données ou des systèmes

de classement non automatique pour un usage commercial ou professionnel. Tous les Länder allemands ont adopté une législation dans le domaine de la protection des données qui transpose la directive européenne de protection des données. La législation des Länder couvre l'administration publique régionale, mais aussi la conformité des entreprises privées avec la Bundesdatenschutzgesetz (BDSG).

■ Spécificités nationales

Le droit à la liberté individuelle a été interprété par la Cour fédérale constitutionnelle allemande comme un droit de « l'autodétermination informationnelle ». Dans une décision historique de 1983 la Cour a considéré comme inconstitutionnelles certaines dispositions de la loi allemande de recensement qui permettaient au gouvernement fédéral de recueillir des renseignements personnels et de les partager avec les collectivités locales et les gouvernements des Länder. Le tribunal a noté qu'il est maintenant possible avec les évolutions techniques de créer un profil de personnalité complète avec le traitement automatisé des données. Ainsi, la Cour a souligné : « que les personnes qui ne pourraient pas évaluer ou vérifier avec certitude les informations détenues sur elles par certains secteurs de leur environnement social seraient particulièrement gênées dans leur capacité de décision ou d'intervention. » Le droit à « l'auto-détermination informationnelle » s'oppose à un ordre social et son ordre juridique sous-jacent dans lequel les citoyens pourraient ne plus savoir qui, quoi, quand et dans quelles situations on les connaît. Encore plus récemment, en février 2008, la Cour a rendu un nouveau jugement historique, constituant un nouveau « droit fondamental à la confidentialité et l'intégrité des informations et des systèmes technologiques » dans le cadre des droits généraux individuels consacrés par la Constitution allemande. Les systèmes d'information et technologiques qui sont protégés par le nouveau droit sont tous les systèmes qui « seuls ou dans leur interconnexion technique peuvent contenir des données personnelles de l'individu concerné dans une portée et une multiplicité tels que l'accès au système permet d'obtenir un aperçu de parties pertinentes du comportement d'une personne ou même de rassembler une image significative de sa personnalité. ». Les débats sur la protection de la vie privée et l'informatique ont commencé en Allemagne dans les années 1960 et la première législation de protection des données fut adoptée dans le Land de Hesse en 1970. Elle a également abouti à la création d'un commissaire à la protection des données. Après de longs débats au sein du parlement allemand et dans l'espace public, la loi fédérale allemande de protection des données (BDSG) a été adoptée en janvier 1977.

La République tchèque

■ La constitution et la protection des données personnelles

Au niveau constitutionnel, la Charte de 1993 des droits fondamentaux et des libertés prévoit des droits à la vie privée étendus. L'article 7 (1) stipule que « L'inviolabilité de la personne et de la vie privée est garantie. Elle peut être limitée uniquement dans les cas prévus par la loi. » L'article 10 stipule que « (1) Toute personne a le droit d'exiger que sa dignité humaine, son honneur personnel, et sa bonne réputation soient respectés, et que son nom soit protégé. (2) Chacun a le droit d'être protégé contre toute intrusion non autorisée dans sa vie privée et familiale. (3) Toute personne a le droit d'être protégée contre le rassemblement non autorisé, divulgation publique ou toute autre utilisation abusive de ses données personnelles. » L'article 13 dispose que « Nul ne peut violer la confidentialité des correspondances ou autres documents ou dossiers, qu'ils soient gardés à titre privé ou envoyés par la poste ou par tout autre moyen, sauf dans les cas et selon les modalités prévues par la loi. La confidentialité des communications par téléphone, télégraphe ou tout autre dispositif sont garantis de la même manière. ».

■ Transposition des directives européennes

Définitions, concepts de base et champ d'application de la protection des données sont définis en République tchèque par la loi 101 du 4 avril 2000 sur la Protection des données personnelles et dans les amendements à certaines lois. Cette loi, conformément à la loi de la Communauté européenne et des accords internationaux liant la République tchèque, prévoit pour l'exercice du droit de chacun la protection contre les intrusions illicites dans la vie privée. Elle réglemente les droits et obligations dans le traitement des données à caractère personnel et précise les conditions dans lesquelles les données personnelles peuvent être transférées à d'autres pays.

La loi met en œuvre les exigences de la directive européenne de protection de données et accorde des exceptions sur plusieurs dispositions clés à la police et aux services secrets en matière de sécurité publique et nationale.

Les gestionnaires de fichiers ont été obligés d'enregistrer leurs systèmes et de se conformer pleinement à la loi du 1er juin 2001. En mai 2001 un amendement a exempté les partis politiques, les églises, les clubs sportifs, et autres organisations civiques engagées dans des activités normales et légitimes de certaines exigences de la loi comme l'enregistrement de leurs fichiers ou l'obtention du consentement individuel avant de recueillir des renseignements personnels sur leurs membres.

Un amendement de juin 2004 à la loi bancaire a complété l'harmonisation avec la directive européenne sur la protection des données (1995/46/CE). L'amendement affine certaines conditions et introduit de nouveaux termes en conformité avec la directive de l'UE. La modification comprend des termes qui régissent la demande de consentement pour le traitement des données à caractère personnel, la relation entre les responsables des fichiers et les personnes concernées, l'obligation de déclaration des fichiers, et l'indemnisation des personnes concernées en cas de violation des droits commises par les responsables des fichiers lors des traitements de données.

Un autre type d'obligation internationale qui affecte la vie privée sont les traités et les accords relatifs à la coopération policière et de renseignement (coopération au sein de SIS, VIS, CIS, les systèmes d'EURODAC, les transferts de données PNR aux Etats-Unis, etc.).

■ Spécificités nationales

La législation nationale « transposant » la directive européenne « rétention des données » a été adoptée avant même que la directive ait été approuvée par le Parlement européen. L'étendue des données des communications électroniques conservées n'est pas révélée, mais la police a utilisé largement ces données ces dernières années. Les citoyens tchèques, contrairement aux citoyens des autres pays de l'Union européenne, sont tenus d'obtenir un visa pour voyager aux Etats-Unis. Suite à une promesse de simplification des procédures de visa par les autorités américaines, le gouvernement tchèque a décidé en 2008 de prendre part au programme américain d'exemption de visa (programme de visa électronique) et a été contraint de signer deux traités prévoyant le transfert complet de données relatives aux citoyens tchèques aux autorités américaines.

La Finlande

■ Transposition des directives européennes

Le 1er juin 1999 la loi sur les Données à caractère personnel, qui a remplacé la loi sur les fichiers de données à caractère personnel est entrée en vigueur. Les grands principes de la protection de la vie privée sont restés largement inchangés, mais les droits fondamentaux et les libertés individuelles sont encore plus fortement soulignés, également dans le cadre du traitement des données à caractère personnel. La directive européenne de protection des données de 1995 est transposée dans cette loi.

Le 1er septembre 2004 la loi sur la Protection de la vie privée dans les communications électroniques, a été promulguée, elle protège la confidentialité et la vie privée dans les télécommunications. Elle vise à clarifier les règles pour le traitement des données d'identification confidentielles et à élargir leur champ d'application pour englober les abonnés d'entreprises ou d'associations. La loi sur la Protection de la vie privée dans les communications électroniques remplace la loi sur la Protection de la vie privée et la sécurité des données dans les télécommunications adoptée en 1999.

La directive européenne de 2006 sur la rétention des données reste encore à transposer de même que le règlement du Conseil de 2004 et la décision de la Commission de 2005, les deux sur des principes concernant les éléments de sécurité et la biométrie dans les passeports et les documents de voyage émis par des Etats de membres.

■ Spécificités nationales

En 1988, la première loi sur les fichiers de données personnelles est entrée en vigueur - la première loi sur la protection des données en Finlande. Cette loi visait à empêcher les violations de l'intégrité à toutes les étapes du traitement des données. L'objectif fonctionnel était de promouvoir le développement, et le respect des bonnes pratiques de traitement des données.

Le 1er octobre 2004, la loi sur la Protection de la vie privée dans la vie professionnelle a été promulguée, elle aborde les principales questions de protection des données en créant différentes procédures pour les

besoins de la vie professionnelle. Cette nouvelle loi comprend des dispositions sur le dépistage des drogues, les caméras de surveillance et la protection de la confidentialité pour les communications électroniques.

En 2009, « la loi Nokia » (également appelé « loi intrusive ») a été adoptée. Elle a introduit un amendement à la loi finlandaise sur la protection des données dans les communications électroniques de septembre 2004. Elle a également démoli une partie des bonnes règles de confidentialité définies par la loi sur la Protection de la vie privée dans la vie professionnelle d'octobre 2004. La nouvelle loi a été votée au Parlement en février 2009 et est entrée en vigueur début juin 2009. La loi est appelée « Loi Nokia » en reconnaissance à l'ardent soutien de l'entreprise Nokia pour celle-ci. Cette loi représente un revers important pour la protection de la vie privée et les droits de l'Homme.

Les Pays-Bas

■ Transposition des directives européennes

La directive européenne sur la protection des données a été transposée en droit national en 1999 avec la loi sur la Protection des données personnelles (Wet bescherming persoonsgegevens « Wbp »), qui est entrée en vigueur le 1er septembre 2001. Cette loi est malheureusement très vague. Par conséquent, l'étendue et la nature exactes des données qui doivent être conservées ne sont pas toujours évidentes et il y a un risque d'extension de l'accessibilité aux données.

■ Spécificités nationales

Avant que la directive européenne de protection des données soit exécutoire, la loi sur la Protection générale de 1992 couvrait les quatre domaines examinés dans cette étude.
En dehors de la loi Générale de confidentialité, il existe d'autres lois spécifiques, comme la loi sur les Télécommunications (« Telecommunicatiewet ») du 19 octobre 1998, la loi sur les Données de la police (« Wet politiegegevens ») ou la loi sur les Bases de données des municipalités (« Wet gemeentelijke basisadministratie »).

La France

■ La constitution et la protection des données personnelles

Contexte historique : la protection des droits et libertés est une tradition de longue date en France, où les droits proclamés dans la Déclaration des droits de l'Homme et du citoyen de 1789 sont garantis par la Constitution. Le droit à la protection des données est reconnu par le Conseil constitutionnel comme un droit constitutionnel sur la base, selon le cas, de la vie privée ou des libertés. Le Code pénal français punit l'usurpation d'identité ou d'autres données personnelles d'autrui dans les communications électroniques. Ceci, comme les appels téléphoniques malveillants, est passible d'un an de prison et d'une amende de 15.000 €. En 1974, une vaste campagne médiatique a mis en lumière certains projets du gouvernement visant à connecter des bases de données. En conséquence, la loi N ° 78-17 relative à l'informatique, aux fichiers et aux libertés individuelles a été adoptée en 1978. Cette loi stipule que « L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'Homme, ni à la vie privée, ni aux libertés individuelles ou publiques ». Les articles 1 et 2 établissent un cadre pour la protection des données personnelles. Ils déterminent les conditions de la légalité du traitement des données personnelles : les données à caractère personnel doivent être obtenues et traitées loyalement et licitement, pour des finalités déterminées, explicites et légitimes, elles doivent être adéquates, pertinentes et non excessives au regard des finalités, elles doivent être exactes, complètes et, le cas échéant, mises à jour. Des mesures appropriées doivent être prises afin de supprimer et de rectifier des données qui sont inexactes et incomplètes, elles doivent être conservées sous une forme qui permet l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire. L'interconnexion des bases de données constitue une nouvelle finalité et doit donc obtenir une nouvelle autorisation. L'article 7 traite du consentement préalable et l'article 8 interdit la collecte et le traitement des données à caractère personnel qui révèlent « les origines raciales et ethniques, les opinions politiques, philosophiques, religieuses ou l'appartenance syndicale des personnes, ou qui concernent leur santé ou leur vie sexuelle ».

L'autorité de protection des données, la Commission nationale de l'informatique et des libertés (CNIL) a été créée en vertu de la présente loi.

■ Transposition des directives européennes

La loi du 6 janvier 1978 a été modifiée à plusieurs reprises, plus récemment, en août 2004, afin d'assurer sa conformité avec la directive européenne du 24 octobre 1995.

La directive européenne du 8 juin 2000 a été transposée dans la loi pour la confiance dans l'économie numérique (LCEN - 2004). Cette loi a mis en place la législation française sur l'Internet et fixé des règles pour le commerce électronique. Plus important encore, la LCEN représente la première loi générale sur l'internet. En particulier, elle définit la communication par Internet en créant de nouvelles catégories juridiques et établit un régime de responsabilités des parties utilisant l'Internet.

Le Code de postes et communications électroniques (article L34-1 remplacé par loi n° 2009-669 du 12 juin 2009 - art. 14) définit la protection de la vie privée de ceux qui utilisent les réseaux et les services de communications électroniques et fixe les règles de conservation et de destruction des différentes catégories de données contenues dans les données électroniques transmises par les fournisseurs de services Internet et les opérateurs.

L'article 7 de la loi 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme autorise le ministère de l'Intérieur français à créer des traitements automatisés des données à caractère personnel (PNR et APIs) recueillies à l'occasion des déplacements internationaux.

Conformément à la loi 91-646 du 10 juillet 1991, les communications électroniques sont définies en tant que correspondance (comme les courriers). En conséquence, leur caractère confidentiel est garanti par la loi.

■ Spécificités nationales

- Passeports biométriques : les décrets (2005 et 2008), établissent respectivement les passeports électroniques et biométriques. La LDH estime qu'ils violent les principes contenus dans les principes énoncées dans la Loi informatique et libertés de 1978. En outre, il n'existe pas de cadre juridique pour l'utilisation des données biométriques.
- Afin de renforcer la sécurité, il y a une tendance à l'utilisation accrue des TIC pour surveiller tous les aspects de la vie des individus. Surveillance et suspicion généralisées sont de plus en plus communes.
- La loi « Création et Internet », connue sous le nom de loi « Hadopi » (Haute Autorité pour la diffusion et la protection des œuvres de création sur l'Internet) est conçue pour protéger les artistes et l'industrie du divertissement contre le partage illégal de fichiers par les utilisateurs de l'Internet. Les fournisseurs de services Internet sont tenus de remettre les adresses associées aux adresses IP des ordinateurs en cause. Cela soulève la question de la « proportionnalité » entre une violation de la vie privée de l'internaute (par la collecte des adresses IP, considérées comme des données personnelles, et en coupant l'accès Internet) et la protection de la propriété privée (protection des artistes).
- LOPPSI 2, projet de loi sur l'Orientation de programmation pour la performance de la sécurité intérieure : cette loi, en cours de discussion au début de 2010, pousse la surveillance des citoyens encore plus loin. En particulier, elle autorise l'utilisation de cookies par les pouvoirs publics pour accéder, collecter, enregistrer, stocker et échanger les données informatiques des personnes à leur insu et ceci sans contrôle judiciaire.
- La création d'une base de données centrale (PERICLES) rassemblera toutes les bases de données judiciaires et combinera les informations disponibles pour lutter contre toutes les formes de la délinquance et la pornographie impliquant des enfants en particulier. À cette fin, la base de données contiendra une grande variété de données à caractère personnel.

5. LES AUTORITES NATIONALES DE PROTECTION DES DONNEES

Tous les pays ont maintenant des autorités nationales de protection des données personnelles (Data Protection Authorities - DPAs). Bien que leur création, rôle et missions soient liés aux directives européennes et soient à l'origine définis par celles-ci (directive protection des données de l'UE), il reste que leur rôle, les moyens qui leur sont donnés, et leur capacité d'intervenir et de sanctionner varie considérablement d'un pays à l'autre.

Toutefois, la majorité de ces DPAs manque cruellement de moyens par rapport à l'étendue des missions qu'elles doivent assurer. En outre, un certain nombre d'entre elles n'ont pas le pouvoir de sanction, qui leur permettrait de faire respecter les lois concernant la protection des données de façon plus efficace. Enfin, ces autorités ne sont pas toujours indépendantes à l'égard des pouvoirs politiques.

L'analyse dans les neuf pays montre des différences significatives en termes de rôle des DPAs dans le fonctionnement général du contrôle de la protection des données : elles peuvent avoir la prééminence dans ces opérations avec une autorité établie et reconnue dans le domaine, ou alors exercer leur activité avec une portée plus limitée en raison de la répartition des rôles avec d'autres autorités.

Il est clair que dans la plupart des pays, même si le battage médiatique entourant leur création et leur fonctionnement est révélateur d'un système démocratique qui garantit que les infractions à la législation de protection des données sont contrôlées - et c'est un progrès - leur champ d'application réel est insuffisant pour :

- **influencer les décisions prises par les pouvoirs publics, au moins par un avis préalable rendu public ou une autorisation dans des cas particuliers ;**
- **faire face à toutes les demandes ;**
- **lutter contre les abus dans les administrations tout comme dans les entreprises privées ;**
- **encourager le débat public et assurer la communication nécessaire à destination du public (informer les personnes de leurs droits et de leurs droits de déposer plainte) ;**
- **promouvoir l'autorégulation et émettre des recommandations en ce qui concerne les nouveaux développements technologiques.**

En outre, les citoyens ne sont pas suffisamment conscients ou informés du rôle des DPAs et des mesures qu'elles peuvent prendre.

La Grèce - L'Autorité de Protection des données grecque (HDPA)

Mise en place de la HDPA

Conformément à l'article 15 § 2 de la loi 2472/97, « L'Autorité constitue une autorité publique indépendante et sera assistée par son propre secrétariat. Elle ne doit être soumise à aucun contrôle administratif. Dans le cadre de leurs fonctions, les membres de l'Autorité jouissent d'une indépendance personnelle et fonctionnelle. L'Autorité rend compte au ministre de la Justice et son siège est à Athènes ».

■ Les missions

Sa mission est la protection des données personnelles et de la vie privée des personnes, conformément aux dispositions des lois 2472/97 et 3471/2006. L'objectif principal de la HDPA est la protection des citoyens contre tout traitement illicite de leurs données personnelles et l'assistance lorsque leurs droits ont été violés dans tout secteur. Un autre objectif de la HDPA est d'offrir soutien et conseils aux gestionnaires de fichiers dans leurs efforts pour se conformer à leurs obligations vis-à-vis de la loi. La HDPA a des pouvoirs de réglementation et de consultation et des compétences telles que l'octroi de licences et l'enregistrement, l'examen des plaintes, la capacité de sanctionner et l'application des accords internationaux (Schengen, Europol). Elle publie un rapport annuel et coopère avec les organismes internationaux.

■ Activités et réalisations

Les mesures réglementaires et les directives

- Les mesures règlementaires

408/1998 : Donner l'information sur la thématique de la protection des données personnelles par la presse, 1/1999 : informer la personne concernée (conformément à l'art. 11 de la loi 2472/97) ; le décret présidentiel 79/2000 : ratifie la possibilité pour l'Autorité d'attribuer aux catégories de fichiers les plus usitées et traitées une réglementation spéciale ou simplifiée ; 24 et 25/2004 : la collecte des données, la maintenance et le traitement seront effectués par TEIRESIAS SA (système interbancaire afin de minimiser les risques encourus lors de la saisie des contrats de crédit avec des clients insolvables et, en général, de réduire au minimum la création de créances douteuses, pour la protection du crédit commercial ainsi que dans l'amélioration des transactions économiques) ; 26/2004 : conditions pour le traitement licite des données à caractère personnel à des fins de publicité ou de marketing direct et la détermination de la crédibilité.

- Les directives

Cinq directives ont été émises concernant par exemple les conditions de licéité du traitement des données à caractère personnel des nouvelles mères dans un but de marketing direct et de publicité dans les maternités, la vidéosurveillance ; la transcription en caractères latins du nom des personnes figurant sur les cartes d'identité et les passeports ; la destruction sécurisée des données à caractère personnel après la fin de la période requise pour la réalisation de la finalité du traitement.

Les plaintes

En 2008, la HDPA a traité 859 cas, dont 263 étaient des plaintes ou des appels et 596 des questions. 22 décisions ont été prises en 1999 (première année de fonctionnement de la DPA), 68 en 2006, 65 en 2007 et en 2008, le nombre atteint 69. Le nombre total de dossiers reçus en 2008 a été 6706. 818 étaient des plaintes, 216 portaient sur des questions spécifiques, en particulier 64 sur la vidéosurveillance, 4 sur la biométrie, 79 sur le spam et 69 sur le marketing direct. Seuls 55 cas de plaintes ou d'appels sur les questions mentionnées ci-dessus ont été résolus alors qu'il y a encore 516 cas en suspens. 224 questions restent en suspens des années précédentes. Ces chiffres montrent les graves difficultés de la HDPA pour faire face à l'augmentation du nombre de cas et des questions reçues, difficultés qui s'aggravent du fait de l'accumulation des affaires en suspend des années précédentes.

Les sanctions mises en œuvre

La HDPA peut imposer des sanctions administratives (art. 21), comme des avertissements, des amendes, la révocation temporaire ou définitive de permis, la destruction de fichiers, le verrouillage des données, etc. La loi prévoit également des sanctions pénales (art. 22) et la responsabilité civile (art. 23). Les amendes sont significatives et efficaces lorsqu'elles visent des entreprises privées ou des particuliers, mais certaines amendes imposées au ministère de l'Ordre public ne sont pas effectives et montrent que la HDPA ne peut pas faire valoir ses opinions. En 2008, la HDPA a infligé 18 amendes, 8 avertissements et 3 autres mesures (destruction de données ou de dossiers).

La communication

La HDPA publie un rapport annuel. En 2008, la HDPA a publié 4 communiqués de presse, organisé un événement pour la Journée européenne pour la protection des données à caractère personnel et un séminaire. Elle est intervenue dans des séminaires nationaux et internationaux, et a publié des articles dans la presse grecque. Le site de la HDPA est pleinement opérationnel depuis décembre 2007. Les citoyens peuvent déposer des plaintes, poser des questions, s'abonner à la liste de l'article 13 etc. par le site internet de la HDPA. Les médias grecs demandent régulièrement des informations à l'Autorité. Selon une étude sur la perception des citoyens sur la protection des données, publiée par l'Eurobaromètre en février 2008, 51% des Grecs sont au courant de l'existence de la HDPA, ce qui est le taux le plus élevé dans l'UE (+ 25% depuis 2003). Cinq pour cent de ces personnes a déjà contacté la HDPA pour une plainte ou pour obtenir des renseignements.

Le Royaume-Uni

Mise en place de la DPA

Le Bureau du Commissaire à l'information du Royaume-Uni (ICO) est l'Autorité indépendante de protection des données du Royaume-Uni comme il est prévu dans la directive européenne de protection des données.

■ Les missions

Il a moins de pouvoir que certains de ses homologues d'autres pays de l'UE. La conformité avec la directive est discutable : par exemple, bien qu'une nouvelle législation soit en projet, le gouvernement n'a actuellement aucune obligation de demander l'autorisation de l'ICO ni même un avis avant d'installer une nouvelle base de données. L'ICO couvre quatre principaux domaines, en relation avec les lois et règlements suivants : loi sur la protection des données, vie privée et règlements des communications électroniques, loi sur la liberté de l'information, règlements sur l'environnement de l'information. Il publie des rapports annuels d'activité. Il ne

couvre pas des aspects importants liés à la vie privée et la protection des données, y compris l'Internet, qui relève du champ d'application d'autres autorités de contrôle, qui sont : le commissaire directeur général de la surveillance (contrôle de la surveillance secrète et du renseignement), le commissaire à l'interception des communications (contrôle des écoutes et des acquisitions des données de communications), le commissaire des services de renseignement, le commissaire du projet d'identité nationale (contrôle des cartes d'identité et autres éléments du shéma de l'identité nationale). En outre, des autorités plus spécifiques existent, tels que le médiateur des enfants. Cette répartition des rôles entre les différentes autorités pourrait être une préoccupation en termes de sensibilisation du public aux enjeux et risques, et en ce qui concerne la transparence et un accès facile à l'information. Par exemple, le contrôle de l'acquisition de données de communication de la part des opérateurs télécoms et fournisseurs de services Internet dans le cadre de la conservation des données est couvert par le commissaire à l'interception des communications et non par l'ICO. De même, les questions de projet d'identité nationale ne sont pas de la compétence de l'ICO, mais plutôt de celles du commissaire spécialement nommé.

■ Les moyens

Comme indiqué par le représentant de l'ICO lors d'un entretien, l'ICO est une petite organisation, bien que sa taille ait récemment doublé.

■ Activités et réalisations

Communication

L'ICO a développé et mis à disposition sur son site Internet une série de documents d'information et de boîtes à outils, et fait des efforts sur la sensibilisation. Toutefois, selon une étude 2008 par l'Eurobaromètre, 80% des citoyens du Royaume-Uni n'avaient pas entendu parler d'une autorité indépendante assurant la mise en œuvre et le respect des lois de protection des données dans leur pays.

L'Espagne - Agence de protection des données espagnole et catalane

Mise en place de la DPA

L'Agence espagnole pour la protection des données (AEPD) est l'organisme de contrôle créé en 1994 en conformité avec la loi organique de protection des données personnelles de l'Espagne. Ses pouvoirs ont été renforcés avec la mise en œuvre de la directive.

■ Les missions

Il s'agit d'une entité de droit public doté de la personnalité juridique et de la capacité à s'engager dans des actes publics et privés de manière indépendante du gouvernement dans l'exercice de ses fonctions. Elle veille au respect des lois sur la protection des données par les responsables des fichiers (entités publiques, entreprises privées, associations, etc.). Les travaux de l'AEPD s'étendent des lois et normes des fichiers publics et privés, à la dissémination de supports d'information : cours éducatifs, manuels adressés aux différents publics cibles, etc.

■ Les moyens

Son siège est à Madrid et elle intervient dans toute l'Espagne, bien qu'il existe d'autres organismes de protection des données dans les communautés autonomes dans la Communauté de Madrid, la Catalogne et le Pays basque, avec une portée limitée pour les fichiers publics qui existent dans leurs communautés autonomes respectives.

■ Activités et réalisations

Les mesures réglementaires et les directives

L'AEPD a demandé à plusieurs reprises que les fournisseurs observent une plus grande transparence et soient plus précis dans leurs mesures. Elle estime que le gouvernement devrait être plus exigeant à cet égard.

Les plaintes

Il n'y a pas de chiffres cumulés, car il existe plusieurs organismes régionaux. En 2008, le nombre d'incidents signalés à l'AEPD a augmenté de plus de 45%, atteignant le chiffre de 2.362.

Les sanctions mises en œuvre

En 2007, l'AEPD a décidé 399 procédures de sanction, soit une augmentation de 32,5% par rapport à l'année précédente. Les sanctions économiques imposées par l'AEPD s'élevaient à 19,6 millions d'€.
L'AEPD a décidé en 2008 un total de 630 procédures de sanctions, près de 58% de plus qu'en 2007, dont 535 ont conduit à l'imposition effective de sanctions. Les amendes se sont élevées à 22,6 millions d'€ soit une augmentation de 15% par rapport à l'année précédente.

La communication

L'AEPD se concentre sur le renforcement de l'information et des services de formation afin d'aider autant que possible les jeunes à gérer leur propre prévention des risques. Le travail accompli par la CLI (Commission

de l'informatique et des libertés) au cours de ces derniers mois doit être mis en évidence (cela a été fait en collaboration avec tous les organismes espagnols de protection des données et les ministères de l'éducation) : préparation de manuels pour les jeunes de différentes classes d'âge, destinés à initier des discussions et réflexions avec les enseignants dans les écoles. L'AEPD a récemment lancé une consultation en ligne sur son site Internet pour familiariser les gens avec les fichiers de données personnelles qui les concernent, afin qu'ils puissent en connaître les objectifs, qui en est responsable, etc.

La Roumanie

Mise en place de la DPA

L'autorité de surveillance de la loi N ° 677/2001 est l'Avocat du Peuple (ou « Ombudsman » ou médiateur). Les règles organisationnelles et fonctionnelles de l'Avocat du Peuple ont été modifiées afin de permettre la création d'un Bureau de protection des informations privées (PIPO), pour la protection des personnes physiques en ce qui dans le champ du traitement des données privées. En réalité, la mise en œuvre a fait apparaître des lacunes importantes et l'autorité désignée n'a que très modestement appliqué les lois. Cela a été l'objet de critiques dans plusieurs rapports d'avancement relatifs à l'adhésion à l'Union européenne tels que le « Rapport périodique 2004 sur les progrès de la Roumanie vers l'adhésion », qui souligne : « Toutefois, les progrès accomplis dans la mise en œuvre des règles de protection des données personnelles ont été limités. Il existe des motifs de préoccupation concernant l'application de ces règles : les actions pour l'application sont bien en deçà des niveaux des Etats membres actuels et des postes supplémentaires n'ont pas été pourvus au cours de la période considérée ». Après plusieurs nouveaux retards, le gouvernement roumain a décidé de résoudre le problème en mettant en place une nouvelle autorité indépendante, qui a été créée par la loi N° 102/2005. La nouvelle autorité de protection des données personnelles - l'Autorité nationale pour la supervision du traitement des données personnelles (ANSPDCP) - a été créée sur le papier uniquement. La loi N° 102/2005 est entrée en vigueur le 12 mai 2005. Bien que la loi ait précisé que l'activité de la nouvelle autorité devrait commencer 45 jours après son entrée en vigueur, le président de la nouvelle autorité ne fut nommé par le Sénat que le 22 septembre 2005. Le même jour, le Sénat a approuvé la nomination du premier président de l'ANSPDCP qui avait participé au Bureau de l'Avocat du Peuple en tant que directeur adjoint responsable des questions de la protection des données personnelles. En raison du retard important dans la création de l'autorité, le gouvernement roumain a publié une ordonnance d'urgence N° 131/2005, qui a prorogé le délai imparti pour créer l'autorité au 31 décembre 2005. Le règlement intérieur de la nouvelle autorité a été adopté le 2 novembre 2005.

■ Les missions

L'activité de la nouvelle institution a commencé seulement en février 2006. Il y a eu un communiqué de presse officiel annonçant le 20 février 2006 que la nouvelle institution pourrait fournir conseils et aides dans les cas où les lois sur les données personnelles ont été violées. La nouvelle autorité est dirigée par un président et un vice-président qui sont élus par le Sénat pour un mandat de cinq ans. L'autorité est indépendante, elle a uniquement l'obligation de présenter un rapport annuel au Sénat roumain.

■ Les moyens

La DPA roumaine n'a pas de bureaux locaux et pas de budget spécifique pour la communication en direction du public. Même si l'autorité roumaine a reçu de nouvelles attributions avec l'adoption de la loi sur la rétention des données, le nombre d'employés est resté le même (seulement 35 postes pourvus en août 2009) et le budget est très limité.

■ Activités et réalisations

Les mesures réglementaires et les directives

L'autorité peut être saisie pour avis sur les actes normatifs. En 2008, la DPA roumaine a été consultée pour 17 actes normatifs. Toutefois, l'avis n'est pas obligatoire et il n'est pas publié. L'autorité a pris deux décisions importantes en 2007, afin de promouvoir une notification plus facile des fichiers de données à caractère personnel à l'autorité. L'une était la mise en œuvre d'un système en ligne qui permet la notification des fichiers à la DPA et la seconde a été la suppression de la taxe de notification. Il y a eu une augmentation du nombre de fichiers enregistrés.

Les plaintes

Dans le domaine des plaintes reçues, le nombre a augmenté, passant de quelques-unes avant 2006 à 550 en 2008.

La communication

La DPA a aussi été impliquée dans des activités de sensibilisation, généralement grâce à des partenariats avec le secteur public (les bureaux des préfets dans plusieurs comtés, les inspections de police), le secteur

privé (association professionnelle de l'immobilier, les notaires, les chambres de commerce) et le secteur de l'éducation (universités de Sibiu et Tg. Jiu). La DPA a organisé un événement « portes ouvertes » et plusieurs manifestations à l'occasion de la Journée européenne de la protection des données. Mais le manque de moyens est évident. Dans ces conditions, il n'est pas surprenant que la protection des données ne soit pas un sujet bien connu pour le moment. L'étude d'avril 2008 de l'Eurobaromètre de l'UE portant sur les perceptions de la protection des données parmi les citoyens de l'UE montre que 79% des Roumains ne savent pas qu'il existe une loi dans le domaine des données à caractère personnel. La même étude révèle que la Roumanie a le plus grand nombre de personnes dans tous les pays de l'UE (47% de la population) qui ne savent pas qu'il y a des lois permettant d'avoir accès à ses données personnelles dans les divers fichiers existants.

L'Allemagne

Mise en place de la DPA

L'Autorité fédérale allemande de protection des données, telle que définie par le BDSG, est le Commissaire fédéral à la protection des données et à la liberté de l'information (Bundesbeauftragter für den Datenschutz), compétent pour les deux législations fédérales de protection des données - l'administration publique fédérale et le secteur privé de compétence fédérale - et pour la législation d'accès aux documents publics. L'Autorité est considérée comme un organisme fédéral indépendant et publie un rapport semestriel. Elle est gérée par un commissaire qui est élu par le Parlement allemand (Bundestag) sur proposition du gouvernement fédéral pour un mandat de cinq ans. Le Commissaire est indépendant dans son travail et ne reçoit pas d'instructions au sujet de son travail. La législation spécifique des Länder pour la protection des données prévoit un commissaire dans chaque Land, dont la fonction est la mise en œuvre de la législation régionale. Par conséquent, il y a aussi 16 commissaires à la protection des données régionales en Allemagne. Certains sont compétents pour la législation du Land sur la protection des données du secteur public et du secteur privé (et parfois pour l'accès à la législation des documents publics) tandis que dans d'autres Länder le contrôle de la législation sur la protection des données dans le secteur privé est entre les mains d'un officier de protection de données interne en relation avec le département des affaires intérieures du Land. Il y a une étroite collaboration entre les commissaires fédéraux et régionaux qui se réunissent régulièrement pour discuter de questions d'intérêts communs et pour adopter les résolutions des conférences nationales de protection des données. Ils se réunissent aussi régulièrement dans ce qu'on appelle le « Kreis Düsseldorfer », une association informelle des principaux acteurs de la protection des données en Allemagne, qui traite de l'application des principes de protection des données par le secteur privé.

■ Les missions

Ses principales attributions sont prévues dans le BDSG. Il vérifie la conformité de l'administration fédérale avec la loi fédérale sur la protection des données, mais peut également être impliqué dans les procédures législatives en donnant des avis et des conseils sur des textes ayant potentiellement un impact sur la vie privée des citoyens. La DPA fédérale est aussi impliquée dans les activités de sensibilisation à la vie privée.

■ Activités et réalisations

Communication

La DPA fédérale a organisé des manifestations pour célébrer la Journée européenne de protection des données et à l'échelle locale a célébré le 25e anniversaire de la décision de la Cour constitutionnelle qui a créé la jurisprudence en matière d'autodétermination de l'information. La DPA fédérale organise également des conférences annuelles sur des sujets d'actualité liés à la vie privée (les questions des moteurs de recherche en 2007 ; les bases de données relatives aux télécommunications et à la révision de la directive vie privée et communications électroniques). Certaines DPA des Länder sont actives dans le domaine de la sensibilisation à la vie privée, à commencer par des campagnes sur les différents sujets « chauds », des guides sur la façon de protéger la vie privée et participent à des projets européens inter secteurs sur la vie privée. Il est également important de noter leur implication dans la création et le soutien à l'amélioration des techniques de confidentialité. Depuis 2001, la DPA du Schleswig-Holstein a été impliquée dans un projet conjoint avec l'Université de technologie de Dresde, afin de créer des logiciels libres qui pourraient permettre à chaque utilisateur de protéger sa vie privée sur Internet. Le logiciel client JAP fournit une communication anonyme et non observable sur l'Internet. JAP fonctionne sur une plateforme Java et est facile à installer et à utiliser, pour permettre aux utilisateurs de l'Internet néophytes de protéger leur vie privée. Elle met également en œuvre un système de certification dans le pays et promeut de tels systèmes au niveau de l'UE via un projet soutenu par la Commission européenne dans lequel des DPA d'autres pays sont impliqués.

La République tchèque

Mise en place de la DPA

L'Office de protection des données personnelles a été créé en 2000 comme un organisme de contrôle indépendant de l'Etat.

■ Les missions

La DPA contrôle le respect des obligations prescrites par la loi dans le traitement des données à caractère personnel ; elle enregistre les notifications données aux organismes pour le traitement des données personnelles ; elle traite des plaintes de citoyens concernant des infractions à la loi ; elle propose des consultations dans le domaine de la protection des données personnelles ; et dans le système de l'administration en ligne établit les identifiants « origine » et « programme » des personnes physiques (à partir du 1er juillet 2010).

■ Les moyens

La DPA est composée de sept inspecteurs nommés pour une période de 10 ans par le président de la République tchèque sur la base d'une proposition du Sénat et du Parlement de la République tchèque. L'Office a son président et environ 95 employés (au mois de décembre 2009). L'Office gère le registre des notifications et des fichiers. Il effectue des inspections dans le but de prévenir le traitement illégal de données à caractère personnel.

■ Activités et réalisations

Les mesures réglementaires et les directives

À certaines occasions, la DPA émet des remarques sur la législation proposée. Toutefois, elle n'a pas encore de pouvoir d'initiative en matière législative et « s'est souvent trouvée dans une situation difficile entre d'une part, les attentes du public qui souhaite à juste titre, une intervention rapide et efficace de sa part, particulièrement en ce qui concerne les pouvoirs de l'Etat et l'administration publique exercée par des organismes gouvernementaux et, d'autre part, les réglementations juridiques qui, en dépit des principes généralement applicables pour la protection de la vie privée élargissent les autorisations ou des exemptions, tant en droit public que droit privé. En effet, lorsque la DPA tente de faire valoir ses opinions et les conclusions de ses contrôles en ce qui concerne les conditions particulières de traitement des données personnelles dans certains domaines, elle doit souvent renoncer à son point de vue étant donné l'existence d'une réglementation spéciale qui prime sur la loi sur la protection des données personnelles. En effet, les principes juridiques de base sont inégalement appliqués au traitement et à la protection des données et certains organismes sont favorisés uniquement parce que leurs activités sont définies par un règlement spécial, même si de tels règlements ne devraient pas exister de fait dans le cadre des principes généraux de la protection de la vie privée et la protection des données personnelles. »

Les plaintes

879 plaintes ont été reçues en 2009, 129 visées pour le contrôle.

Les sanctions mises en œuvre

89 sanctions administratives en 2009, 112 décisions administratives ont conduit à une amende pour des communications commerciales non sollicitées.

La communication

La DPA publie son rapport annuel en tchèque et en anglais, publie un bulletin et gère des pages web avec des informations sur ses conclusions, ses positions, ses commentaires, la législation, le registre des fichiers, etc. Elle organise des conférences, des ateliers et des cours pour les enseignants et un concours pour les jeunes enfants dans le cadre scolaire.

La Finlande

Mise en place de la DPA

Le médiateur pour la protection des données est une autorité indépendante agissant en relation avec le ministère de la Justice. La Finnish Communications Regulatory Authority (FICORA) est une autorité administrative générale du ministère des Transports et des communications pour les questions concernant les communications électroniques et les services de la société de l'information en Finlande. C'est l'autorité de sécurité nationale en Finlande. CERT-FI, qui est une partie de la FICORA, est l'équipe nationale finlandaise de réponse aux urgences informatiques dont la tâche est de promouvoir la sécurité dans la société de l'information en empêchant, observant, résolvant les incidents de sécurité et aussi de diffuser des informations

sur les menaces à la sécurité de l'information. Cet organisme supervise principalement la conformité à la loi sur la protection de la vie privée, des communications électroniques et de ses dispositions d'application.

■ Les missions

Le médiateur à la protection des données oriente et contrôle le traitement des données à caractère personnel et propose des consultations connexes. Il exerce un pouvoir sur les questions liées à la mise en œuvre du droit à la vérification et à la correction des données à caractère personnel. Il suit aussi l'évolution générale dans le traitement des données à caractère personnel, et lance des initiatives si nécessaire. Il veille à la diffusion d'informations relatives au domaine de l'exploitation et participe à la coopération internationale. Il doit accomplir sa mission dans les conditions prévues par la loi sur la confidentialité. Cette entité supervise également le traitement des données de localisation, les annuaires et les renseignements téléphoniques, veille au respect des dispositions relatives à la prospection directe au moyen de systèmes automatisés ainsi qu'au respect des dispositions relatives au droit spécial d'accès à l'information d'un utilisateur.

■ Activités et réalisations

La communication

Récemment, le médiateur à la protection des données a été très actif dans la campagne d'information sur les cartes de transport.

Les Pays-Bas

■ Les missions

La DPA néerlandaise surveille la conformité aux lois qui régissent l'utilisation des données personnelles. Cela signifie que la DPA néerlandaise veille au respect et à l'application de la loi sur la protection des données personnelles, de la loi sur les données de police et de la loi sur les bases de données municipales. Le cadre de l'accomplissement de ses tâches a été énoncé dans la loi sur la protection des données personnelles et d'autres lois connexes. Dans ce contexte, le législateur a mis en œuvre l'article 28 de la directive européenne Vie privée 95/46/CE, qui prévoit expressément l'existence d'une telle autorité de contrôle et aussi que cette autorité doit s'acquitter de sa tâche en toute indépendance. La DPA néerlandaise a également un rôle de veille qui lui permet de fournir des informations et mener des études sur différents sujets.

Ses tâches incluent : la formulation de recommandations quant à législation, les tests de codes de conduite et règlements, les examens préliminaires, l'information des citoyens sur leurs droits et obligations, la médiation et le traitement des plaintes, les enquêtes officielles, et des tâches internationales.

Afin de remplir son rôle efficacement, la DPA néerlandaise a à répondre à plusieurs garanties comme la possibilité d'opposition et d'appel à l'encontre de ses décisions devant les tribunaux de droit administratif et la possibilité de déposer une plainte auprès du Médiateur national. En outre, en tant qu'organe administratif, la DPA néerlandaise est bien sûr également liée par les principes généraux de bonne administration.

■ Activités et réalisations

La DPA néerlandaise est active dans cinq domaines principaux : le commerce et les services, le travail, la sécurité sociale, les services médicaux et d'assistance sociale, la police et la justice et les questions gouvernementales et internationales.
Tous les ans, la DPA néerlandaise publie un rapport public, expliquant ses travaux et conclusions. Son site web contient des résumés des rapports annuels des années précédentes.

La France

Mise en place de la DPA

La Commission nationale de l'informatique et des libertés ou CNIL, a été créée en 1978 par la loi Informatique et libertés. Elle est composée de 18 membres, nommés pour cinq ans. Parmi ces 18 membres, il y a quatre membres du Parlement, huit hauts fonctionnaires et six membres qualifiés. L'actuel président est également sénateur, ce qui signifie qu'il peut exprimer une opinion à la CNIL, critiquant les projets de loi, et voter différemment au Sénat.

■ Les missions

Pour atteindre les objectifs énoncés dans la loi, à savoir prévenir les menaces éventuelles que les technologies de l'information peuvent présenter pour les libertés civiles et protéger la vie privée, les libertés individuelles et publiques, la CNIL peut faire appel à ses pouvoirs de décision pour imposer des sanctions, ainsi qu'à ses pouvoirs de contrôle et de recommandations. En 1978, ces pouvoirs ont été définis pour six missions principales :

- Accorder ou refuser l'autorisation préalable à la création de fichiers de traitement de certaines données à caractère personnel ;
- Informer les personnes des fichiers existants et les traitements pour lesquels ils ont été déclarés et pour les informer de leurs droits concernant leur vie privée ;
- Garantir le droit d'accès aux fichiers de police et militaires ;
- Contrôler la sécurité des systèmes d'information en ce qui concerne le traitement des données. La CNIL peut imposer des mesures nécessaires, telles que la correction ou l'effacement des données inexactes ;
- Sanctionner des gestionnaires de fichiers qui ne respecteraient pas la loi, par l'émission d'avertissements, des mises en demeure, des sanctions pécuniaires et des ordres pour l'arrêt des traitements, et même en informant le Parquet de toute violation ;
- Réglementer. La CNIL établit des normes simplifiées afin que les opérations de traitement les plus courantes qui mettent le moins en danger les libertés civiles soient soumises à des formalités réduites.

Toutefois en 2004, lorsque la France a été obligée de modifier la loi de 1978 pour se conformer à la directive européenne du 24 octobre 1995 sur la protection des données à caractère personnel, elle a modifié les pouvoirs de la CNIL en abaissant le niveau de protection contrairement à ce qu'exige la directive. En conséquence, la CNIL ne peut plus s'opposer à la création des fichiers de police, mais seulement fournir un avis consultatif publié au *Journal officiel* qui n'a pas d'influence sur la création ou pas de ces fichiers.

En théorie, ces procédures simplifiées sont compensées par l'attribution de nouveaux pouvoirs qui lui permettent de mener des enquêtes et d'imposer des sanctions. En conséquence, la CNIL peut infliger des sanctions pécuniaires pouvant aller jusqu'à 300.000 €.

■ Les moyens

120 agents effectuent les missions quotidiennes de la CNIL, constituant une équipe beaucoup trop faible compte tenu de ses responsabilités. Enfin ses enquêtes sont rendues incertaines par un manque de ressources.

■ Activités et réalisations

En 2008 la CNIL a adopté 586 décisions et mené 218 inspections. Depuis 1978, 1.288.394 fichiers ont été déclarés à la CNIL. En 2008, en matière de formalités de déclaration : 391 autorisations, 18 refus, 23 décisions rendues sur des affaires sensibles ou à haut risque de traitement, 700 autorisations liées à des systèmes biométriques (515 en 2007), 2588 déclarations relatives aux systèmes de vidéo surveillance (1317 en 2007), 2607 transferts internationaux (1938 en 2007). Elle a rendu 12 avis sur des projets de lois ou de décrets.

En 2008, il y avait 989 correspondants informatique et libertés dans 3.679 organisations.

Les plaintes

En 2008, 71.990 fichiers ont été déclarés, 4.244 plaintes ont été déposées, 2.516 demandes d'accès aux fichiers de police ont été reçues. Cela représente 116% de plus qu'en 2007, et 3.500 demandes n'ont pas pu être traitées ! Les secteurs d'activité à partir desquels la plupart des plaintes ont été reçues sont (par ordre décroissant) : le marketing commercial, le secteur bancaire et organismes de prêts, et l'emploi.

Les sanctions mises en œuvre en 2008

1 avertissement, 9 amendes, 5 cas d'action en justice.

La communication

Le site de la CNIL fournit toutes les décisions, les avis officiels, les résultats d'enquête et son rapport annuel. Il fournit des conseils, des modèles de lettres pour les particuliers qui veulent déposer une plainte auprès de la CNIL. La CNIL estime qu'à peine un tiers de la population française est consciente des menaces que font peser sur les libertés individuelles, le développement des technologies d'enregistrement des données. Les jeunes représentent une grande majorité des deux tiers de la population qui n'est pas au courant.

6. THEME : MOBILITE ET TRANSPORTS

Deux thèmes principaux ont été analysés dans cette rubrique : les données PNR (Passenger Name Records ou enregistrement des données des passagers aériens) et les « cartes de transport ».
Le dossier des données PNR soulève la question d'un équilibre entre la sécurité, la lutte contre le terrorisme et la protection des données personnelles, les cartes de transport soulèvent la question d'un équilibre entre la facilité qu'elles procurent aux utilisateurs et la protection de leurs données personnelles.
Néanmoins, dans les deux cas, nous pouvons souligner une question de sécurité dans la mesure où des fichiers de données personnelles sont traités par des entreprises privées : ces données pourraient-elles être volées ou vendues ? Ou utilisées à des fins autres que celles qui sont annoncées : profilage, utilisation marketing ?
L'autre problème est l'utilisation qui peut être faite par la police ou toute autre institution d'Etat : qui a effectivement accès aux données ? Pour quel usage ?

Passenger Name Record : dossier des données passagers

Le dossier PNR est lié en particulier à un accord négocié avec les Etats-Unis pour leur fournir toutes les données personnelles contenues dans les systèmes de réservations aériennes pour chaque voyageur désireux de se rendre aux Etats-Unis ou d'en partir. Deux programmes sont décrits dans les études nationales : le programme américain PNR avec les accords négociés avec l'UE, et parfois des accords spécifiques avec l'un des pays européens (par exemple, un « protocole d'entente » avec la République tchèque) et le programme du Royaume-Uni « e-border ».

L'objectif est pour les Etats de collecter et analyser les données provenant des compagnies aériennes ou agences de réservation (ou même au Royaume-Uni, de tous types de transporteurs : les compagnies aériennes, les ferries et les compagnies ferroviaires) concernant les passagers qui ont l'intention de voyager vers les Etats-Unis (ou vers le Royaume-Uni pour les PNR du Royaume-Uni). L'objectif déclaré est la sécurité et la lutte contre le terrorisme.

■ Accord PNR UE - USA

Après le 11 septembre 2001, les Etats-Unis ont estimé que les PNR pourraient fournir les outils nécessaires pour enquêter sur les attaques terroristes. Ainsi, le gouvernement américain a demandé la collecte, le transfert et la rétention des données PNR par le Département de la sécurité intérieure (DHS) des Etats-Unis, le Bureau des douanes et la protection aux frontières. Les Etats-Unis ont donc exigé des compagnies aériennes qu'elles donnent accès au système de réservation commun à différentes compagnies aériennes en échange du droit à atterrir aux Etats-Unis. À la suite de plaintes déposées par l'association des compagnies aériennes auprès des autorités de protection des données, les Etats-Unis ont négocié un accord de transfert avec l'UE en 2004, puis en 2007.

Effectivement, les dossiers PNR contiennent des données sensibles (voir dans la liste des études nationales les données recueillies - bases de données associées) : le but de l'accord est censé assurer un niveau de protection qui pourrait satisfaire à la norme d'adéquation requise par la directive 95 de l'UE, pour autant que les données seront utilisées uniquement aux fins pour lesquelles elles ont été recueillies.

■ Mais de nombreuses questions se posent

- L'adoption du transfert des données PNR n'a pas fait l'objet de procédures démocratiques : pas d'appro-

bation du Parlement national, les objections de la DPA ignorées (CZ).

- Disproportion de la quantité de données transférées par rapport à l'objectif (données sensibles, en particulier).
- L'accès direct des autorités américaines dans les systèmes de réservations (pull : tirer) au lieu de transferts des données envoyés par les opérateurs des systèmes de réservation (push : pousser).
- Exonération du DHS, pour le système d'arrivée et de départ (ADIS) et pour le système de cible automatisé, de la loi de 1974 sur la vie privée alors que cette loi de ne tout façon ne protège toujours pas les étrangers.
- Pas de contrôle adéquat sur les PNR transférés au DHS (ces dysfonctionnements majeurs prouvent que le DHS ne respecte pas l'accord avec l'UE).
- Les procédures de sécurité : les compagnies aeriennes maintiennent des sites web qui permettent un accès presque illimité aux données PNR (informations accessibles par le numéro de réservation par exemple). Les données PNR sont traitées comme une forme de données de transactions commerciales, en dépit du caractère sensible des informations qu'elles contiennent (et bien que ces informations aient un statut spécial de protection dans l'UE). La sécurité des données devrait être traitée avec une attention particulière afin d'éviter les pertes ou les erreurs et la divulgation à des tiers non autorisés lors de la transmission. (+ le problème « push / pull »).
- Conservation des données : 7 ans dans une base d'analyse active, puis 8 ans dans un état dormant (base de données du DHS). Aucune garantie que les données collectées et stockées de cette manière seront détruites.
- L'administration américaine ne fournit aucune information au sujet des fichiers créés. Apparemment, trois fichiers sont mis en œuvre : « No fly list » = liste des passagers interdits de vol ; « Banned from U.S. territory » = liste des passagers interdits sur le territoire des Etats-Unis ; « Selectee list » = liste des passagers à surveiller : fichiers à vérifier avant de prendre une décision, fichiers de données collectées sur les passagers.
- Les autorités américaines ont adopté une attitude laxiste concernant l'orthographe des noms des individus inscrits sur ces listes (plusieurs orthographes acceptées pour un même nom) ce qui conduit à des doutes quant à la fiabilité de la liste et le risque d'erreur d'identité.
- Les individus portant des noms apparaissant sur les listes (sans raison, erreurs, etc.) sont tenus de remplir un formulaire de vérification d'identité des passagers fourni par l'administration américaine et de produire un certificat de naissance, mais leur nom n'est toujours pas retiré de la « No Fly List », ils sont simplement déplacés dans la « Selectee list ».
- La durée de conservation des listes - 30 jours en ligne et puis indéfiniment dans le fichier - est excessive.
- Des exemples montrent que le droit de connaître ou de modifier ses données n'est pas efficace (accès par les individus à leurs données sur demande, à : Office of field operations, US Customs and Border Protection, Room 5.5-C, 1300 Pennsylvania Avenue, NW Washington, DC 20229).
- Les autorités américaines sont susceptibles de partager les données PNR européennes avec des pays tiers.

■ Législations nationales en application

A ce jour, le nouvel accord PNR USA-UE a été approuvé par le gouvernement tchèque avec d'importantes réserves ; le droit français se dirige vers l'utilisation des données PNR : l'article 7 de la loi N ° 2006-64 du 23 janvier 2006 sur la lutte contre le terrorisme autorise la collecte et l'utilisation des données PNR et APIS (Advance Passenger Information System). Le ministre de l'Intérieur est donc autorisé à introduire un traitement automatisé de données à caractère personnel collectées dans le cadre de voyages internationaux. Nous devons souligner que l'accord l'UE - USA viole la réglementation européenne sur la protection des données. Selon le Groupe 29, le Contrôleur européen de la protection des données et le Parlement européen, cet accord est loin d'offrir un niveau adéquat de protection des données pour les données PNR transmises. On ne peut que regretter le manque de dispositions claires et proportionnées de protection des données relatives au partage des données, la conservation et le transfert de données supplémentaires, le manque de vérifications effectuées par l'autorité de protection des données et aussi être préoccupé par le fait que la mise en œuvre de nombreuses dispositions soit à l'entière discrétion des Etats-Unis.

■ Le programme « e-border » (Royaume-Uni)

Le programme « e-border » collecte toutes les informations des transporteurs sur les passagers, les équipages et les marchandises qui ont l'intention de voyager vers le Royaume-Uni ou d'en partir. Cette liste est

comparée à une liste de surveillance. Tout le monde est concerné à l'exception des personnes du CTA. La mise en œuvre est prévue de 2008 à 2014. Les dangers de ce programme sont les mêmes que pour le système PNR USA-UE, avec en sus les mêmes risques que pour les autres bases de données du Royaume-Uni dont la sécurité est « indigente », conduisant à des pertes d'énormes quantités de données personnelles.

Questions spécifiques : les citoyens britanniques et résidents sont également concernés. Le programme vise aussi des objectifs de police interne et de contrôle des revenus (risque de partage de données avec d'autres organismes d'Etat) qui pourrait conduire à contrôler totalement de façon illégitime et disproportionnée les citoyens britanniques et les résidents, en raison de leur profil de voyage. Les objectifs du programme sont suffisamment larges pour permettre toutes les utilisations possibles des données recueillies, bien au-delà des objectifs proclamés. Le programme peut également porter atteinte au droit de libre circulation inscrit dans la législation de l'UE.

■ Les bonnes pratiques et les campagnes

Au niveau européen, l'AEDH a dénoncé la violation de la vie privée et les dangers pour la démocratie de l'accord PNR. La LDH lui a emboîté le pas en 2003 et a réitéré son action lors de son congrès tenu en 2009 (voir résolution du congrès). Une campagne de sensibilisation a été menée par IuRe, mais il n'y a pas eu de véritable campagne et peu de prise de conscience au Royaume-Uni.

Une campagne au niveau de l'Union européenne faisant le lien entre les accords PNR USA-UE, les plans de l'Union européenne et les systèmes nationaux irait probablement dans la bonne voie pour une prise de conscience. Le thème principal de la campagne pourrait être la liberté de mouvement et la vie privée, tandis que la campagne devrait le mettre en évidence que des données sensibles sont rassemblées et analysées.

■ Conclusions et recommandations

1 - Tout d'abord : le principe de l'accord PNR, en soi, n'est pas bon, il doit être totalement reconsidéré. Nous nous interrogeons sur l'utilisation des données PNR (à l'origine utilisées pour la fourniture de services par des opérateurs) pour assurer la police alors que l'efficacité pour cette fin n'est pas prouvée. Aucune évaluation d'impact réel n'a jamais été effectuée. Nous visons ici non seulement les accords PNR USA - UE, mais aussi tous les accords PNR. Mais nous ne rejetons pas la nécessité pour certains cas particuliers, de transmettre des informations PNR.

2 - Compte tenu de la mise en œuvre actuelle des accords PNR, en admettant qu'il existe des besoins de sécurité, de meilleures garanties sont nécessaires :

• Les Etats-Unis doivent assurer un niveau de protection au minimum égal à ce qui est requis par les normes européennes ;

• Les Etats-Unis doivent signer la Convention 108 du Conseil de l'Europe sur la protection des données à caractère personnel (ouverte aux pays tiers) ;

• L'accord PNR UE/USA prévoit des recommandations qui ne sont pas réellement appliquées : ces recommandations doivent être mises en œuvre.

En s'appuyant sur les nouveaux pouvoirs conférés au Parlement européen par le traité de Lisbonne, il faudrait :

- **Veiller à ce que le principe de proportionnalité et que la règle de la nécessité dans les termes du contrat soient respectés ;**
- **Créer un cadre juridique sûr ;**
- **Obtenir une synthèse des résultats concrets découlant de l'utilisation d'un tel arrangement ;**
- **Exclure toute utilisation des données sensibles liées à : l'origine raciale ou ethnique, les croyances religieuses, les opinions politiques, l'appartenance à un syndicat, l'état de santé, l'orientation sexuelle, et les données qui peuvent être considérées comme excessives par rapport à la vie privée ;**
- **Obtenir l'utilisation du système « push » pour transférer les données à inclure dans ce nouvel accord ;**
- **Réduire la durée totale de la rétention des données, actuellement disproportionnée, à une période de rétention plus raisonnable ;**
- **Informer les passagers sur la façon dont leurs données personnelles sont utilisées ;**

- **Que des corrections efficaces et rapides en cas d'erreurs, des mécanismes de recours, y compris des recours administratifs et judiciaires, soient disponibles pour tous les individus, indépendamment de leur nationalité et de leur résidence.**

3 . Les personnes doivent être informées des accords PNR et mises en garde sur les risques induits pour la protection des données personnelles.

Les autorités de protection des données doivent, avec le concours de la société civile (cf bonnes pratiques et campagnes) informer les citoyens sur les risques pour la protection des données personnelles et la vie privée liés à la nature de toutes les données contenues dans les accords PNR.

Si suffisamment de citoyens demandaient l'accès à leurs données PNR, le coût supplémentaire pourrait conduire les compagnies de transports aériens à demander une révision ou une annulation des accords PNR.

Les « cartes de transport »

Basées sur la technologie RFID, ces cartes ont un périmètre d'utilisation plus ou moins étendu selon les cas, de la ville à l'ensemble du pays. Elles deviennent plus ou moins obligatoires pour les transports en commun, l'option billet n'étant parfois plus disponible (ex : Pays-Bas) ou plus cher, avec deux grandes tendances : l'interopérabilité et l'extension à d'autres services (par exemple : l'Opencard en République tchèque, utilisée également comme carte de bibliothèque et carte prépayée pour le stationnement). Un autre développement prévisible est l'utilisation de la puce du telephone portable comme carte pour de la billeterie ou des opérations de paiement, les cartes de transports étant alors incluses dans le téléphone portable.

Ces cartes de transport peuvent être, selon les cas, anonymes ou personnelles (OV carte à puce - République tchèque), mais les cartes anonymes (ne laissant pas de traces d'itinéraires) ne permettent généralement pas l'accès aux mêmes services que les cartes personnelles.

Toute la population est potentiellement utilisatrice de ces cartes à puce et le nombre d'utilisateurs augmente très rapidement : de 8 000 en 2008 à 330 000 mi-mars 2009 pour l'Opencard à Prague (puce RFID obligatoire pour la carte annuelle à tarif réduit) ; de 150 000 en 2007 à 400 000 en avril 2009 pour In-karta ; 2 750 000 utilisateurs de cartes de transport en Finlande, 4. 536.000 utilisateurs pour le Passe Navigo dans la région d'Ile de France (Paris et ses environs).

■ Interrogations sur l'utilisation des « cartes de transport intelligentes »

Les risques pour la liberté de mouvement, la vie privée et la sécurité sont élevés pour de nombreuses raisons :

- La possibilité de lire les données qu'elles contiennent à une certaine distance, avec un lecteur RFID banal, à l'insu de l'utilisateur, ce en raison du manque de cryptage approprié (au début l'Opencard à Prague) ; la sécurité est minime, car les cartes doivent être rentables ;
- La possibilité de « tracer » les usagers ; les puces RFID présentent une menace en terme de profilage des individus ;
- Les utilisateurs ne sont pas informés que des données sensibles peuvent être recueillies et traitées, et ne savent pas toujours à quoi ils consentent.

Les opérateurs font valoir que les cartes à puce avec les bases de données générées (toutes les données sont stockées dans les bases de données de l'exploitant, comportant toujours des informations sensibles, comme : nom, adresse, montant d'argent transféré, les services utilisés, ou même parfois le numéro de sécurité sociale...) permettent de rendre un meilleur service, le contrôle de l'utilisation autorisée, l'aide à la planification des capacités de transports, d'éviter les erreurs, d'améliorer les temps de réponse, et aussi, pour les cartes utilisées comme clé d'accès, d'améliorer la sécurité (personne ne peut accéder s'il n'est pas autorisé - il faut néanmoins souligner que la copie des cartes est possible, d'autant plus lorsque la technologie utilisée est la moins chère possible). C'est aussi bien sûr un choix économique.

Les propiétaires de fichiers sont les entreprises, seuls les contrôleurs ont accès aux données, mais dans certains cas, les conditions de l'accès ne sont pas si claires. D'ailleurs, par exemple aux Pays-Bas, il est arrivé que les données personnelles aient été vendues à des fins marketing. Il y a aussi le risque d'une utilisation accrue de ces informations par les pouvoirs publics (voir le dossier Finlande). Ainsi, l'utilisation et l'accès non autorisé aux informations stockées peuvent être en jeu.

L'établissement de cartes à puce dans une version non anonyme force les possesseurs à les utiliser pour des services offerts auparavant sur une base anonyme et sans traitement des données. Le consentement libre demeure illusoire alors que les avantages financiers et pratiques sont généralement liés à la version personnelle.

La conservation des données varie selon la carte de transport : 30 jours après la fin du contrat, 6 mois, 2 ans après la fin du contrat (à des fins commerciales et statistiques relatives aux clients et prospects), 5 ans. Parfois cette durée n'est pas connue (Pays-Bas).

■ Le cadre législatif

Globalement il n'y a pas de législation spécifique sur l'utilisation de la RFID, la loi sur la protection de la vie privée et des données personnelles s'applique comme pour toute autre utilisation des TIC. Les pratiques peuvent enfreindre la directive 95/46 et la convention 108 du Conseil de l'Europe pour la protection des personnes physiques à l'égard du traitement automatisé des données à caractère personnel.

■ Campagnes de sensibilisation

La sensibilisation du public semble être faible en dépit de quelques campagnes ou critiques dans différents pays : une campagne menée par IuRe a entraîné un meilleur cryptage des données dans les cartes RFID, avec aussi une enquête par la DPA, des articles, une reprise par des élus de la ville (Prague) et une pétition pour l'introduction de cartes anonymes. Le contrôle de la DPA a conduit à une modification des bases de données et à une meilleure information (In karta) ; en Finlande, le Médiateur à la protection des données a critiqué le système et a informé le public, mais le débat s'est rapidement éteind ; aux Pays-Bas, après la critique par la DPA néerlandaise, les entreprises de transport ont modifié leur système, mais néanmoins le débat ne portait que sur le manque de sécurité. Par contre, 5 organisations de consommateurs néerlandais ont déclaré qu'elles ne soutiendraiennt pas l'usage de la carte de transport considérant qu'elle présente plus de problème que d'avantages pour les utilisateurs (prix, questions de confidentialité). Une vérification indépendante sera effectuée tous les deux ans. En France la CNIL a déjà classé les étiquettes (ou puces) RFID comme une technologie qui menace les libertés individuelles, car elle considère ces données comme personnelles au sens de la loi l'Informatique et libertés de 1978. La CNIL a également assuré que les cartes anonymes doivent être disponibles, mais la compagnie de transport les fait payer plus cher et n'en fait pas d'information.

■ Recommandations et conclusions

Au niveau européen, le rapport sur la RFID ainsi que les recommandations de la Commission sont satisfaisants, quelques recommandations complémentaires sont néanmoins nécessaires.

1. Quatre recommandations principales

- **Les cartes ont été introduites sans une véritable évaluation publique des risques. L'évaluation des atteintes à la vie privée doit être obligatoire (au niveau de l'UE), les DPA doivent vérifier ces évaluations, d'autant plus que la surveillance ou le profilage basés sur la RFID peuvent être étendus à l'excès et que la sécurité des cartes peut être minimale, pour qu'elles soient rentables.**
- **Utilisation de puces RFID de haute technologie pour réduire les risques.**
- **La liberté de circulation implique des cartes de transport anonymes : c'est possible, mais rarement proposé par les compagnies. La possibilité d'obtenir des cartes de transport anonymes doit être obligatoire (au niveau de l'UE). Nécessité d'une initiative de l'UE ou d'une politique visant à mettre en œuvre d'une manière non optionnelle des cartes de transport anonymes sécurisées.**
- **Les cartes à puce « multi usages » conduisent à l'interopérabilité des fichiers et à l'utilisation interdépendante des données générées : toutes les fonctions doivent être strictement définies et non mélangées sur un même support (prestations bancaires, cartes de transport, cartes d'achat, cartes d'identité ou e-passeport) ceci également pour des raisons de sécurité ordinaire : si vous perdez votre carte vous ne perdrez pas tout à la fois.**

2. La sensibilisation du public

D'autres campagnes doivent être lancées sur les thèmes :

- **Choisir des cartes anonymes.**
- **Se méfier des cartes « multi usages » !**
- **Connaître les risques pour la protection des données personnelles et les libertés induits par les cartes à puce RFID.**

7.THEME : IDENTITE BIOLOGIQUE

L'utilisation de l'identité biologique pose plusieurs questions, selon que ces données biologiques sont utilisées pour identifier les personnes par les pouvoirs publics (à des fins sécuritaires ou non), ou pour l'accès à des locaux et/ou à des services privés (cantines, centres de loisirs, etc.). Toutefois, il est important de noter la tendance à réunir dans un seul support basé sur cette identité biologique (exemple : la carte d'identité en Espagne), de nombreuses fonctions pour l'accès à des services tant administratifs (incluant les contrôles frontaliers) que privés. Ce support devient alors un « sésame » valable aussi bien pour les contrôles d'identité par les administrations que pour l'inscription et l'accès à un certain nombre de services. Cette tendance « tout-en-un » apparaît comme simple pour les utilisateurs, qui le plus souvent ne sont pas assez conscients des dangers potentiels d'une telle interopérabilité.

Nous ne pouvons partager d'autre part la confiance excessive que les administrations et les services publics et privés placent dans l'utilisation des données biométriques comme preuve d'identité : les possibilités de dommages, de modification de ces détails biologiques, la possible usurpation d'identité signifient que, comme toute autre preuve d'identité, ces données ne sont pas fiables à 100%. Nous devons lutter contre l'idée que l'identité biologique serait totalement fiable (contrairement à d'autres méthodes de vérification de l'identité), puisque que son développement est également lié à cette prétendue qualité de fiabilité totale (qui n'en reste pas moins élevée).

Deux difficultés sont à souligner en ce qui concerne l'utilisation de l'identité biologique :

- **Une centralisation des fichiers qui semble obligatoire alors qu'elle ne l'est pas, sinon dans une perspective de contrôle de l'ensemble de la population: l'exemple de l'Allemagne pour le passeport biométrique montre que le système peut fonctionner sans un stockage centralisé de données ;**
- **La question des fichiers détenus par les structures publiques et privées : quelle sécurité, quelles procédures d'accréditation, dans quelle mesure peuvent-ils devenir une marchandise, quels sont les risques dans la mesure où les structures privées, inscrites dans une logique sur le marché et pour lesquels la sécurité n'est pas la principale préoccupation, peuvent avoir accès à des fichiers centraux ?**

Un des points clés est la question de la proportionnalité de la technologie utilisée par rapport à l'objectif, puis une fois encore, comme précédemment, la question de la sécurité du traitement des données.

En outre, deux questions se posent à long terme :

- **Quel est le sens d'une société dans laquelle les relations sont de plus en plus fondées sur le contrôle de données biométriques plutôt que sur des relations humaines ou « l'identité déclarée » ?**
- **Que se passerait-il pour les personnes concernées si un pays perdait ses fondements démocratiques ou s'il était envahi ou encore si un pays étranger ou des groupes violents s'emparaient de la base de données biométriques de tous les habitants ?**

Passeports électroniques, registre des Identités (Royaume-Uni) et DNIE (Espagne)

Les passeports électroniques sont basés sur deux technologies : une puce RFID et des données biométriques, ainsi que la mise en place d'une base de données. Le passeport électronique est basé sur le règlement du Conseil de l'Union européenne (décembre 2004) et la décision du 28 février, qui est plus intrusive même que la recommandation de l'OACI de 2003 (adoptée sous la pression des Etats-Unis, suite au 11 septembre 2001), car il rend obligatoire dans la puce non seulement la photographie du titulaire, mais aussi 2 empreintes digitales. L'objectif déclaré est de protéger les passeports contre la falsification et d'identifier le titulaire à un niveau supérieur de sécurité. Les Etats membres ont donc pris ce cadre en compte dans l'établissement de leurs systèmes nationaux administratifs et techniques pour les passeports électroniques. Certains pays n'ont pas encore mis en œuvre le passeport électronique à l'échelle de tout le pays (exemple : la Roumanie a reporté à novembre 2009, en raison de problèmes financiers). Dans d'autres, comme la Finlande, la mise en œuvre ne fait que commencer (passeport électronique délivré depuis le 28 juin 2009). L'application commence à peine à être mise au point en Grande-Bretagne. L'Allemagne a été le premier pays à adopter le passeport biométrique en 2005.

Ce passeport concerne toute la population dans chaque pays, à l'exception, selon les pays, des enfants de moins de 16 ans (Royaume-Uni), 12 ans (Finlande) ou 6 ans (Grèce, Roumanie, France). Son objet est « l'utilisation normale du passeport », document de voyage et d'identification. Au Royaume-Uni, le registre des identités est la base de l'état civil, du passeport biométrique, de l'accès aux e-services de l'Etat ainsi qu'aux transactions électroniques privées. Le DNIE espagnol, délivré par le ministère de l'Intérieur de l'Espagne est utilisé non seulement pour identifier chaque citoyen, mais également pour les fonctions administratives ainsi que les opérations bancaires, les études, les services domestiques (électricité, eau, téléphone) et les opérations commerciales.

Les éléments de biométrie contenus dans le passeport électronique et dans les bases de données

- **Finlande :** la puce RFID contient la photographie numérique et deux empreintes digitales. La base de données centralisée est contrôlée par la DPA Finlandaise. Les informations contenues dans la base de données peuvent cependant être utilisées à d'autres fins (par exemple : l'identification de personnes dans les accidents).
- **Allemagne :** la puce RFID contient la photographie numérique et deux empreintes digitales depuis 2007. Aucune base de données centralisée (la loi l'interdit). Les empreintes digitales ne sont que sur la puce RFID du passeport et détruites après leur inclusion dans la puce. Ainsi, l'expérience allemande présente une transposition pour les epasseports particulièrement respectueuse de la vie privée.
- **Roumanie :** la puce RFID contient la photographie numérique et deux empreintes digitales, mais dix empreintes ont été recueillies dans le projet pilote. Aucune base de données centralisée. Les empreintes digitales ne sont que sur la puce RFID du passeport et détruites après leur inclusion dans la puce, après une durée limitée pendant laquelleles données peuvent être corrigées
- **France :** la puce RFID contient la photographie numérique et deux empreintes digitales, mais 8 empreintes sont recueillies – Une base de données centralisée régie par le ministère de l'Intérieur (profilage avec le SIS et INTERPOL). Ce e-passeport va au-delà des dispositions de la législation européenne.
- **Royaume-Uni :** la base de données est centralisée (registre de l'état civil), régie par le bureau de l'identité et des services des passeports du ministère de l'Intérieur. Il semble que d'autres organismes gouvernementaux et des entreprises privées soient en mesure d'accéder à la base de données afin de vérifier les identités (clients et personnel).
- **Espagne :** une photographie numérique et les empreintes digitales avec deux certificats numériques (certificat d'authenticité et certificat de signature numérique) + nom, prénom, lieu de résidence et un numéro d'identification unique.

■ Interrogations

- Les dangers habituels liés à l'identification biométrique, aux puces RFID et aux bases de données.
- Les données biométriques combinées avec la puce RFID donnent une image très détaillée d'une personne.
- Le choix de la puce RFID pose un problème d'utilisation des données (localisation et profilage possible).
- Les mesures prises dans certains Etats membres pour assurer le chiffrement des informations stockées peuvent être facilement contrées.
- La question du recoupement de l'information avec d'autres bases de données publiques ou privées (en particulier au Royaume-Uni).
- La fiabilité du système : le vol d'identité, les changements de ses données pour l'individu (le vieillissement, les modifications, les blessures).
- Accès probable à l'avenir à la base de données pour des raisons d'application des lois et de maintien de l'ordre.
- Des risques d'interconnexion avec d'autres fichiers à l'avenir, en particulier avec ceux contenant des données biométriques (si les bases de données sont centralisées).

■ Le cadre législatif

- En Finlande, le règlement du Conseil de 2004 et la décision de la Commission du 28 février 2005 ne sont pas encore transposés. Cela signifie un revers important pour la vie privée et des droits de l'Homme. La Finlande prendra probablement des mesures de sécurité afin d'assurer une protection contre la falsification et la lecture non autorisée, mais ces mesures ne sont pas encore décidées.
- Au Royaume-Uni, le projet est classé « rouge » dans le rapport sur les bases de données d'Etat, ce qui signifie que la base de données concernée est « presque certainement » illégale au regard des droits de l'Homme ou du droit de la protection des données et doit être supprimée ou revue en profondeur. La collecte et le partage de données personnelles sensibles peuvent être disproportionnés ou effectués sans consentement, ou sans une base juridique appropriée, il peut aussi y avoir d'autres problèmes majeurs concernant la vie privée.

- En Roumanie, la loi 2004/2005 concernant la libre circulation des citoyens roumains à l'étranger, a été modifiée à plusieurs reprises, notamment par le biais de l'ordonnance d'urgence 207/2008. Cette ordonnance a été approuvée par le Parlement par la loi 264/2009. Le ministère de l'Intérieur doit adopter la législation secondaire (normes méthodologiques) qui précise comment les données biométriques sont recueillies et qui doit respecter la législation sur la protection des données.
- En Allemagne : dans la loi allemande sur les passeports de 1986, modifiée en juillet 2005, la mise en place d'un fichier centralisé des données biométriques est interdite.
- En France : Les décrets de décembre 2005 et d'avril 2008 concernant les passeports électroniques ont été attaqués par des associations devant le conseil d'Etat qui a décidé de diligenter une enquête approfondie afin d'éclairer les points contestés par les associations.

■ Sensibilisation, campagnes, réactions

- En Roumanie, la DPA a souligné que le projet pilote a violé la loi sur la protection des données. Tous les principaux problèmes identifiés par la DPA ont été corrigés par les autorités après cette inspection. La conscience des questions de protection des données est limitée mais le epass suscite une forte opposition d'une partie de la population. Cela est dû aux croyances religieuses, mais aussi à une réelle préoccupation de savoir si la mise en œuvre des passeports électroniques respectera la législation sur les données personnelles, compte tenu de l'absence de formation dans ce domaine de tous les acteurs impliqués.
- En Finlande : les médias ont signalé d'une manière très positive l'introduction des passeports biométriques, car ils les considèrent et les représentent comme une amélioration dans la lutte contre l'usurpation d'identité. On ne sait pas si les citoyens finlandais sont conscients ou non des enjeux et des risques de passeports biométriques. Certaines ONG nationales s'y sont opposées dans la campagne « Stop RFID ».
- Au Royaume-Uni : la sensibilisation au risque est forte avec une énorme opposition depuis le début de proposition du projet. Le Royaume-Uni n'a pas de carte d'identité depuis 1952. Une campagne principale a été menée conjointement par plusieurs ONG, des députés et la presse ont également joué un rôle majeur : la population ne soutient plus majoritairement le projet. Un sondage effectué en juin 2008 indique que seulement 50% de la population soutient le projet. La Cour des droits de l'Homme de Strasbourg le 4 décembre 2008 a condamné le Royaume-Uni pour le stockage des empreintes digitales pour une trop longue durée dans la base de données de la police.
- En Allemagne : pas de prise de conscience des risques, sauf par certaines associations défendant la vie privée, aucune véritable campagne, mais le Chaos Computer Club a publié « Comment falsifier des empreintes digitales ». Toutefois, la mise en œuvre du passeport électronique en Allemagne est une des plus favorables à la protection des données personnelles.
- En France : en 2008, la LDH et IRIS ont déposé un recours auprès du Conseil d'Etat visant à l'annulation de l'ordonnance de 2008 étant donné que ce décret viole le principe de proportionnalité prévu à l'article 6, 3 ° de la loi du 6 janvier 1978.

■ Recommandations et conclusions

Certains pays mettent en œuvre le passeport électronique, allant plus loin que ce que demande l'UE, d'autres ont des pratiques plus favorables à la protection des données : à partir de la même demande de l'Union européenne, différentes façons de la mettre en œuvre sont possibles. Toutefois, pour une majorité de gouvernements, la réglementation de l'UE a été l'occasion de mettre en œuvre ou d'élargir l'utilisation de la biométrie à un niveau national. Néanmoins, l'identification au moyen de données corporelles est une rupture par rapport à l'utilisation antérieure de l'identité déclarative. Nous changeons de paradigme, sans que la plupart des gens ne le remarquent.

1 . Tout d'abord, nous mettons en question le principe de nécessité pour le passeport électronique. Aucune évaluation ne montre la nécessité du passeport électronique ainsi notre premier point est de contester la décision européenne, qui d'ailleurs va au-delà de la recommandation de l'OACI, qui ne requiert que la photo obligatoire. Il convient de souligner que la méthode n'est pas fiable à 100%.

2 . Dans le cadre actuel de la mise en œuvre du passeport électronique, nous avons formulé plusieurs recommandations

- **Ne pas utiliser le passeport pour des questions autres que la déclaration de son identité (par exemple pas de services offerts grâce à une pièce d'identité) ;**
- **Garantir la non-interopérabilité des fichiers ;**
- **Imposer des limitations au niveau européen sur l'utilisation des passeports biométriques à l'égard des enfants ;**
- **Assurer un niveau adéquat de sécurité : pas de bases de données centralisées, les données biométriques collectées pour les passeports (photo et empreintes digitales) doivent être stockées**

uniquement sur la puce RFID du passeport (comme en Allemagne) ;

- **L'existence des bases de données centralisées étant déjà effective, des mesures de sécurité doivent veiller à ce que ces bases de données ne puissent être piratées, y compris par d'autres états, et aussi qu'il ne puisse pas y avoir d'interopérabilité entre les fichiers. La sécurité concerne aussi les utilisations diverses (les hôtels par exemple) qui doivent être basées sur la nécessité. Des garanties doivent être données sur les procédures d'autorisation pour les personnes ayant accès aux bases de données.**

3 . La sensibilisation du public

- **Une meilleure information est nécessaire sur le risque supplémentaire induit par les informations numériques contenues dans la carte.**
- **Informer les citoyens des (bonnes) pratiques dans d'autres pays.**

Bases de données ADN

Chaque pays dispose d'une base nationale de police pour les données ADN. La population concernée diffère d'un pays à l'autre ainsi que les conditions pour les collectes d'échantillons, leur conservation, les données, et leur utilisation. La tendance est souvent d'élargir les cas pour lesquels l'ADN est prélevé et conservé.

■ Cadre d'utilisation

- **Royaume-Uni :** l'ADN est prélevé sans consentement, et la population ciblée est toute personne de plus de 10 ans, soupçonnée d'une infraction enregistrable. En outre, la police peut demander à des personnes suspectées de donner volontairement des échantillons afin de les exclure d'une enquête. Elle peut aussi demander de donner des signatures complémentaires pour que leur ADN soit ajouté à la base de données. Ainsi le National DNA Database (NDNAD) est la plus grosse base de données de tous les pays et le Royaume-Uni a la plus grande proportion de population dont l'ADN est enregistré dans une base de données (7% en 2008). La base de données montre des différences de traitement selon l'appartenance ethnique : 30% des hommes noirs sont enregistrés dans la base de données, alors que seulement moins de 10% des hommes blancs y sont enregistrés.
- **Roumanie :** le prélèvement d'échantillons se fait uniquement avec le consentement du sujet, sinon la décision d'un juge est nécessaire. Pour les enfants de moins de 14 ans, l'accord d'un parent ou tuteur est requise. La population ciblée est celle des suspects et des condamnés pour des crimes spécifiques dont la liste est prévue par la loi. Les échantillons peuvent être prélevés sur d'autres personnes qui pourraient être suspectes, mais ils sont juste comparés au contenu de la base de données et non enregistrés dans celle-ci. Aucune connaissance exacte de l'importance de la base de données.
- **Grèce :** les échantillons d'ADN sont obligatoires, selon une décision de justice pour toute personne condamnée à une peine de prison d'au moins 3 mois. Si l'analyse est négative, le matériel est immédiatement détruit. Si l'analyse est positive, le matériel est détruit, mais les empreintes génétiques seront conservées dans un fichier spécial jusqu'à la mort de la personne et utilisées pour enquêter sur d'autres crimes.
- **République tchèque :** sont ciblées toutes les personnes accusées et reconnues coupables d'avoir commis délibérément des actes criminels, et les personnes condamnées à un traitement médical obligatoire. En mars 2009, la base de données contenait 45 000 profils génétiques. Ce nombre a augmenté de manière significative lorsque la police et les autorités pénitentiaires ont été autorisées à collecter des données sans le consentement de citoyens accusés ou condamnés.

Les gestionnaires des fichiers diffèrent également selon les pays : au Royaume-Uni, c'est l'Agence nationale de police avec un conseil stratégique du NDNAD qui est gestionnaire, et la maintenance est assurée par le Service médico-légal scientifique ; pour la Roumanie, c'est l'institut médico-légal et l'Institut de police générale qui sont en charge de ce fichier ; en Grèce, le siège de la police a accès au fichier, alors que la gestion des fichiers est supervisée par le procureur de la cour d'appel ; en République tchèque c'est l'Institut de criminologie qui est gestionnaire. Les durées de rétention des données sont variables : rétention permanente au Royaume-Uni (sauf en Ecosse) y compris pour les personnes acquittées, rétention jusqu'à l'âge de 60 ans pour les criminels (Roumanie) ou permanente pour des crimes spécifiques, mais l'enregistrement est supprimé si la personne est innocente, rétention autant que nécessaire pour les personnes condamnées en République tchèque, mais on ne sait pas si les enregistrements pour les personnes acquittées sont réellement effacés ou pas.

■ Interrogations

Nous devons souligner les nombreux dangers et des risques :

- Certains sont inhérents à l'ADN et aux autres bases de données biométriques : des correspondances peuvent être trouvées avec l'ADN de victimes ou de passants et peuvent mener à des erreurs ;

- Les échantillons sont analysés par des laboratoires privés : même s'il y a agrément cela soulève des questions ;
- Il peut y avoir des risques de révélations de cas de « non paternité » pour des personnes concernées, ainsi que de possible maladies ;
- Le transfert de profils à d'autres pays est en augmentation : la législation et la surveillance de la sécurité des données partagées et traitées à l'étranger sont insuffisantes ;
- Des innocents poursuivis sont traités de la même manière que les auteurs de crimes graves ;
- Des cas particuliers au Royaume-Uni où l'utilisation de la base de données par la police relève de la routine et où des arrestations sont faites en vue de stocker toujours plus de profils d'ADN, considérant tout jeune comme un criminel, avec des préjugés ethniques.

■ Cadre juridique

Au Royaume-Uni l'agggravation est constante, chaque révision permettant le recueil de plus en plus d'échantillons avec une conservation permanente des données. Il convient de souligner que la Cour européenne des droits de l'Homme a jugé illégal que le gouvernement du Royaume-Uni conserve toutes ces données pour les personnes innocentes. Le gouvernement a lancé une consultation en mai 2009 pour prendre en compte cet arrêt dans le droit national.
En République tchèque une législation spécifique est manquante et n'est pas conforme à l'article 8. La législation en est au stade précoce de préparation.
En Roumanie, la législation secondaire (concernant la mise en œuvre pratique) est toujours absente : conformément à la loi initiale, elle devait être prête pour le 14 novembre 2008.
En Grèce l'amendement récemment proposé met la base de données ADN sous la supervision du procureur, par conséquent, cela l'exclut du champ d'application de la protection des données dans le traitement de l'ADN. C'est une non-conformité avec le droit européen et les normes européennes

■ Sensibilisation et campagnes

Dans l'ensemble des pays étudiés, la prise de conscience sur cette thématique est faible : début de réaction au Royaume-Uni lié à la campagne « Récupérez votre ADN » ; en Grèce les partis d'opposition n'ont pas empêché le vote de la mesure.

■ Recommandations et conclusions

1. De fortes garanties devraient être adoptées au niveau européen. Le principe constitutionnel de proportionnalité exige que les législateurs limitent les prélèvements d'ADN aux crimes graves tels que l'assassinat, le crime organisé, le trafic de drogue, etc., et aux infractions qui de par leur nature rendent nécessaire la prise, l'utilisation et la comparaison des matériels génétiques afin de trouver l'auteur d'un acte pour lequel une poursuite est déjà engagée ;
2 . Soutien à l'appel des DPA pour une nouvelle législation portant spécifiquement sur les bases de données ADN ; établir un groupe d'experts incluant des spécialistes des questions de vie privée afin de travailler sur la nouvelle législation ;
3 . Une campagne de sensibilisation du public est nécessaire.

Contrôles biométriques pour l'accès aux établissements privés ou aux services

Sept fiches dans les études nationales portent sur ce sujet. Les contrôles biométriques dans les exemples choisis sont mis en œuvre par des discothèques, piscines, gymnases, clubs privés, des centres sportifs, le secteur de la restauration, l'accès à des entreprises ou des restaurants d'entreprises. Chaque établissement a 5 à 10 000 cartes d'accès enregistrées. Sauf pour l'accès aux entreprises les jeunes utilisateurs sont le principal groupe cible. Le développement de cette technologie pour les services privés ou l'accès aux entreprises est fondé sur des arguments tels que :

- Prévenir la violence (l'anonymat n'est pas possible, la direction sait qui est là à tout moment, la possibilité de créer des « listes noires » - les empreintes peuvent être comparées à celles de la liste noire) ;
- Rapport coût-efficacité (coûts de personnel réduits en raison de moins de confrontations) ;
- Eviter des amendes pour avoir servi de l'alcool aux mineurs ;
- Facile à mettre en œuvre.

Partout le système est considéré comme un succès, malgré les dangers potentiels des technologies utilisées.

■ Interrogations

- Le traitement et le stockage de données biométriques ne devraient intervenir que lorsque c'est absolument nécessaire, quand c'est proportionnel à la finalité, et avec le plus grand soin. Est-ce le cas ?
- Puisque ce genre d'informations sensibles sont collectées et stockées par les entreprises privées dont l'objectif premier est la rentabilité, il existe un risque considérable qu'elles ne mettent pas en œuvre les mesures de sécurité les plus efficaces (et donc coûteuses) contre les failles de sécurité et l'utilisation non autorisée de l'information. Beaucoup d'entreprises stockent des informations dans une base de données centrale ;

- De tels systèmes ne donnent pas droit à l'erreur ;
- La durée de conservation des données reste souvent obscure. En France, la conservation des données dépend des données recueillies (période définie par l'autorisation de la CNIL) ;
- Les données recueillies peuvent être utilisées à d'autres fins que celles initialement envisagées, en particulier à des fins commerciales (marketing par exemple). Possibilité de suivi et de profilage. Risque de vol d'identité.

■ Cadre législatif

Aux Pays-Bas il n'existe pas de législation spécifique sur l'utilisation de la biométrie. Les règles générales pour la protection des données à caractère personnel s'appliquent aussi à la biométrie et en déterminent les conditions d'utilisation. Par exemple, les principes de proportionnalité et de nécessité s'appliquent et il doit être établi que l'utilisation de la biométrie est en relation avec le problème. La loi sur la protection générale de 1992 s'applique.
En France tous ces systèmes sont soumis à l'autorisation préalable de la CNIL (DPA française), à l'exception des trois systèmes suivants qui font l'objet d'autorisations spécifiques : les empreintes palmaires pour contrôler l'accès aux cantines scolaires - Autorisation n ° AU-009 ; empreintes palmaires pour le contrôle d'accès aux cantines et aux lieux de travail et de leur gestion - Autorisation n ° AU-008 ; empreintes digitales exclusivement enregistrées dans un dispositif individuel en la possession de la personne concernée pour contrôler l'accès aux lieux de travail - Autorisation n ° AU-007. La CNIL insiste sur le fait que les personnes concernées doivent être préalablement informées de ces contrôles. Doivent être clairement notifiés aux personnes concernées : les conditions d'utilisation, le fait que ces contrôles sont obligatoires ou facultatifs, qui a accès aux données, comment s'y opposer et les droits d'accès et de rectification aux données. En outre, le 19 avril 2005, le tribunal de Paris (TGI) a interdit à une filiale de la SNCF d'utiliser les empreintes digitales pour une machine à pointer. Les juges ont estimé que les empreintes digitales sont des données morphologiques biométriques utilisées pour identifier des caractéristiques physiques spécifiques qui sont uniques et permanentes pour chaque individu et que leur utilisation constitue une atteinte à la vie privée. Ce jugement est basé sur la directive européenne et sur l'article L. 120-2 du code du travail français.
En Espagne, les gestionnaires doivent enregistrer la base de données avec l'accord de la DPA et fournir des informations sur le droit d'accès, de rectification, d'annulation, etc. Ils ont besoin des accords écrits pour transférer des données à d'autres personnes.
Au niveau européen, il n'existe pas de réglementation spécifique pour l'utilisation de la biométrie ; les règles générales pour la protection des données à caractère personnel s'appliquent. Une recommandation a été émise par le groupe 29.

■ Sensibilisation et campagnes

Seul un très faible pourcentage de personnes réagit à ce système (environ 3% de la population concernée dans un cas décrit, et pour la plupart, des personnes âgées). La devise « si vous n'avez rien à cacher, vous n'avez rien à craindre » fonctionne bien et par ailleurs ces cartes biométriques apportent des avantages financiers (remises, etc.). Les jeunes considèrent ces cartes comme des pratiques normales, même si certains se plaignent du marketing (réception d'un trop grand nombre de SMS et d'e-mails par exemple). En général, toute la population est très mal informée et ignore les risques induits par la biométrie dans ces utilisations.
Dans certains domaines, il y a des réactions spécifiques (accès aux cantines scolaires en France par exemple).

■ Conclusions et recommandations

1. La nécessité de ces mesures pour l'accès aux services reste à démontrer : nous nous interrogeons sur le principe de leur nécessité (si, parfois, il peut être justifié pour l'accès à des zones sécurisées, l'argument est plus contestable pour les cantines scolaires) – Il faut travailler à des changements dans la législation au niveau européen afin de limiter les abus ;

2 . Dans la mesure où ce type de contrôle existe et que l'autorisation est donnée, nous demandons la mise en œuvre d'un niveau adéquat de sécurité et l'assurance de la non interopérabilité des bases de données ;

3. La justification par le consentement de l'utilisateur - même éclairé -, ne peut pas être un argument recevable pour autoriser l'utilisation de ces systèmes ;

4. Des campagnes de sensibilisation sont nécessaires sur les dangers et les limites de l'utilisation de la biométrie pour identifier les personnes : les utilisateurs ne sont pas conscients des risques, au contraire, ils semblent être d'accord avec cette utilisation (la fiabilité, la sécurité, la facilité d'utilisation, etc.). Des campagnes doivent aussi dénoncer les intérêts financiers des acteurs industriels couplés à des intérêts politiques pour le contrôle des citoyens.

8. THEME : COMMUNICATIONS INTERPERSONNELLES

PROTECTION DES DONNEES, CONSERVATION ET VENTE

Les problèmes causés par l'utilisation des systèmes de messageries électroniques résultent de la vente ou de la non protection des coordonnées et données de l'utilisateur qui sont utilisées par des entreprises de marketing à des fins commerciales. Les données peuvent être piratées et il existe un risque d'usurpation d'identité. En outre, les communications interpersonnelles sont l'exemple de la plus grande échelle de collecte et de rétention des données (par les opérateurs « télécom » et communications électroniques). En effet l'opportunité a été donnée par la législation européenne aux gouvernements pour augmenter la conservation des données au niveau national, dans le cadre de la lutte contre le terrorisme. En ce qui concerne les téléphones mobiles, il y a le risque supplémentaire de géo localisation à l'insu de l'utilisateur. Presque tous les pays ont présenté des fiches d'étude sur le sujet, pour certains pays, détaillées par outils, d'autres ayant décidé de présenter une fiche unique de « conservation des données ».

■ La législation sur la conservation des données

- **Roumanie :** la directive sur la rétention des données électroniques est transposée. Les opérateurs de télécommunications sont tenus de conserver les données de trafic pendant 6 mois sur leurs propres serveurs, et de répondre aux demandes des autorités (puis de les supprimer ou les rendre anonymes). Il n'existe aucun projet pour une base de données centralisée. La loi pourrait être révisée, car elle est considérée comme difficile à appliquer, le gouvernement roumain a annoncé qu'il suspendra la loi, mais rien n'est officiel. Mais la loi est mise en œuvre même si les règles d'application ne sont pas données : par exemple, les conditions d'accès aux données stockées auraient du être précisées par une loi d'application qui n'est pas encore promulguée. Les risques pour la sécurité des données et d'utilisation abusive par les sociétés commerciales sont élevés.
- **Allemagne :** la directive sur la rétention des données électroniques est transposée. Les opérateurs télécommunications sont tenus de conserver les données de trafic pendant 6 mois, sur leurs propres serveurs, et de répondre aux demandes des autorités. La conformité de la législation est actuellement contestée devant la Cour constitutionnelle, le tribunal administratif de Wiesbaden a considèré l'enregistrement « disproportionné » et que « la rétention des données viole le droit fondamental à la vie privée ». Pourtant la Cour de justice de la Communauté européenne a considéré que la directive sur la rétention de données a été adoptée correctement. L'Irlande a demandé à la CJCE d'annuler la directive. (Recours en annulation - Directive 2006/24/CE - Conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques). Le résultat a été : la directive sur la conservation des données repose sur un fondement juridique approprié, c'est à bon droit que la directive a été adoptée sur le fondement du traité CE, celle-ci concernant de façon prépondérante le fonctionnement du marché intérieur.
- **Royaume-Uni :** la directive sur la rétention des données électroniques est transposée. Les opérateurs télécom sont tenus de conserver les données de trafic pendant 12 mois, sur leurs propres serveurs, et répondre aux demandes des autorités. L'idée d'une gestion centralisée d'une base de données a été proposée en 2008. De mauvais échos dans la presse ont conduit à l'annulation. La tendance montre une augmentation des demandes par les pouvoirs publics : 351 243 en 2005, 504 073 en 2008. Les motifs d'accès et les listes des organismes agréés sont très larges (cf. rapport national). L'aggravation est directement liée à la directive de l'UE.
- **Pays-Bas :** la loi de rétention des données néerlandaise n'est pas encore appliquée, un arrêté royal est attendu en raison de la directive européenne. La loi générale sur les télécommunications s'applique (1998). La durée de conservation des données est de 12 mois pour les données de télécommunication et 6 mois pour les données Internet (le gouvernement voulait 18 mois).
- **Finlande :** la directive sur la rétention des données électroniques n'est pas encore transposée dans le droit national, c'est en préparation. La période de rétention minimale est de 3 mois à des fins de facturation, les opérateurs de Télécom et les fournisseurs d'accès Internet peuvent conserver les enregistrements pendant une période maximale de 3 ans pour des tâches annexes de gestion commerciale ou liées à la sécurité des données. La proposition de loi actuelle annonce 12 mois. La loi Nokia est en application.
- **La République tchèque :** la directive sur la rétention des données électroniques est transposée. Les opérateurs Télécom sont tenus de conserver les données de trafic pendant 6 mois. Certaines données doivent être stockées par les fournisseurs pour 12 mois. Les données qui doivent être conservées sont supérieures à la demande de la directive. Les données sont transférées à la demande du service habilité de la police sous forme électronique. Elles sont utilisées même dans les enquêtes sur des infractions mineures. Le traitement des données n'est probablement pas conforme aux normes européennes. L'étendue des bases de données créées depuis 2006 n'est pas connue.

- **Espagne :** LOPD, LSSI, LGT contrôlent les communications interpersonnelles.
- **France :** la directive sur la rétention des données électroniques est transposée, la durée de rétention est d'un an. La loi n ° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme, stipule l'obligation pour les opérateurs de communications électroniques de conserver certaines données relatives au trafic des abonnés. L'article L 34-1 II du Code des postes et télécommunications détermine, selon la CNIL, les catégories de données relatives au trafic des abonnés et la durée de leur rétention. Le décret d'application (N ° 2006-358) a été adopté le 24 mars 2006.

■ Campagnes de sensibilisation

- En Roumanie, une prise de conscience limitée, mais aussi des malentendus sur le contenu des données stockées : les gens pensaient que cela concernait le contenu des communications. Ainsi, ce fut l'un des principaux sujets concernant la vie privée aux yeux du public au début de 2009.
- En Allemagne, la directive rétention des données électroniques et sa mise en œuvre ont été l'un des principaux sujets liés à la protection de la vie privée. La société civile a été très active pour limiter la mise en œuvre. Ainsi, la Cour constitutionnelle examinera en quoi la nouvelle loi correspond à la jurisprudence constitutionnelle allemande.
- Au Royaume-Uni la sensibilisation est faible, la tendance est à une diminution de la mobilisation, même si il y a quelques informations à ce sujet (la presse, les ONG, les membres du parlement).
- Aux Pays-Bas, le débat au niveau politique, notamment la critique du Sénat (durée de conservation, mais aussi quelles sont les données conservées, par exemple) a sensibilisé la population, maintenant quelque peu au courant de l'enjeu. Des campagnes ont été menées avec une pétition (F.A.I. et des membres d'EDRi). Le coût de la rétention des données est également en débat.
- En République tchèque la sensibilisation est probablement faible, malgré les activités des ONG (articles, débats publics et pages web). En mars 2010, 51 parlementaires ont déposé des plaintes établies par IuRe auprès de la Cour constitutionnelle.
- En France, pas de campagnes spécifiques hormis une pétition contre la rétention des données lancée par IRIS en 2004 qui a eu peu de succès. Cependant il y a une certaine sensibilisation sur la question de la vente ou de l'utilisation des les données personnelles à des fins de marketing en ligne.

■ Recommandations et conclusions

1. Les droits conférés par la directive « Vie privée » sont pertinents et suffisants, même s'ils doivent être complétés par des recommandations émises par le Groupe 29 concernant la localisation des enfants (consentement), bien qu'étant mineurs, et la localisation des salariés (ne sont pas en mesure de donner un consentement libre tel que stipulé dans la directive). La question est plus sur les moyens prévus pour faire respecter cette directive au niveau européen. Ainsi, nous demandons une évaluation de la directive afin de déterminer si une révision doit être entreprise.

2. La directive de conservation des données : l'obligation générale de conserver le trafic et l'emplacement des données est une violation grave du droit à la vie privée, elle transforme tous les citoyens en suspects potentiels. Une obligation générale de conservation ne devrait pas être obligatoire.

3. Dans le contexte actuel une surveillance stricte par les DPA doit être obligatoire, aussi sur l'utilisation de ces bases de données par les autorités (des garanties nécessaires doivent être fournies).

4. Des règles doivent être établies pour les fournisseurs afin que les utilisateurs sachent quel niveau de protection des données personnelles est mis en œuvre (informations en bas d'écran par exemple).

5. Des campagnes de sensibilisation.

Des campagnes doivent être menées au niveau européen contre la directive sur la rétention de données. Et, en fonction des équipements :

- **Encourager les utilisateurs à lire les conditions générales d'utilisation, et demander que ces conditions soient accessibles à tous (compréhensibles par tous) ;**
- **Faire pression (au niveau national et européen), sur les gouvernements et les autorités de protection des données (DPA) pour que le droit européen s'applique pleinement à Google, Facebook, Yahoo, etc. du fait que les équipements (ordinateurs des utilisateurs) sont situés dans l'UE pour la collecte de données à partir du territoire européen ;**
- **Campagne sur l'idée qui devient de plus en plus fausse de la distinction entre les données de communication et leur contenu.**

Des campagnes doivent être lancées pour faire adopter des bonnes pratiques de protection des données personnelles :

- **Utiliser un anti-virus et un outil anti-spam ;**
- **Ne publier aucune adresse e-mail sur Internet ;**
- **Utiliser une adresse e-mail spécifique pour les services en ligne et une autre pour communiquer avec les amis et la famille ;**
- **Changer l'« adresse e-mail de service» si elle reçoit trop de spam ;**
- **Ne jamais répondre aux « pourriels », même pour protester : cela ne ferait que confirmer la validité de l'adresse.**

9. THEME : LES RÉSEAUX SOCIAUX

Le principal problème identifié est la violation de la vie privée. Elle résulte bien souvent d'un manque de prise de connaissance des possibilités de paramétrages qui permettent aux utilisateurs de protéger leurs données à caractère personnel, rendant public seulement une partie des données personnelles, partageant d'autres données avec un nombre limité de contacts. Néanmoins les mesures de sécurité mises en œuvre par les fournisseurs de services sont souvent insuffisantes. Souvent, ces derniers n'ont pas adopté une politique d'information transparente sur la façon dont les données des utilisateurs sont traitées ou partagées.
La large couverture médiatique des problèmes rencontrés par certains membres de réseaux sociaux ou de blogueurs a permis de sensibiliser les utilisateurs qui exigent désormais de plus en plus le droit de supprimer les données les concernant.
Deux types de réseaux sociaux : ceux qui peuvent être considérés comme des réseaux sociaux « nationaux » et les réseaux « internationaux ». Toutes les fiches ont souligné que si les réseaux sociaux « nationaux » sont soumis à la législation nationale, les réseaux « internationaux », principalement basés aux Etats-Unis, affirment obstinément dépendre de la législation américaine. Selon les pays, les réseaux sociaux « nationaux » peuvent être les plus populaires (Finlande, Pays-Bas par exemple), mais presque partout le développement de réseaux sociaux internationaux est la principale question.

■ Interrogations

En règle générale presque tous les réseaux sociaux sont critiqués pour les questions de protection des données personnelles :

- Les conditions d'utilisation ne sont pas facilement accessibles ou claires, généralement non connues ;
- La difficulté d'établir un véritable contrôle sur les données publiées afin de déterminer précisément à quel public elles sont rendues accessibles. La connaissance de la possibilité de limiter l'accès aux données à un groupe défini d'utilisateurs est souvent faible ;
- Le risque que les données publiées sur les sites de réseaux sociaux soient accessibles sans autorisation ou sans que la personne qui publie ne le sache ;
- Le profilage à des fins commerciales (publicité ciblée par exemple) ;
- La conservation des données, parfois de façon permanente (les fournisseurs de réseaux sociaux affirment qu'elles sont leur propriété), sans véritable information de l'utilisateur ;
- Les difficultés à être en mesure de se désinscrire réellement et complètement.

■ Le cadre législatif

- En Allemagne, les DPA sont actives pour l'information du public sur les réseaux sociaux et leur utilisation, et visent en particulier les adolescents. Des guides ont été publiés. Un appel public demande aux fournisseurs allemands de respecter le cadre de protection des données et rappelle les dispositions légales applicables. Les principaux sites de réseaux sociaux allemands ont adopté (en 2009) un code de conduite volontaire pour les enfants, les consommateurs et la protection des données (un bouton facilement accessible est mis à disposition pour supprimer complètement le profil de l'utilisateur, etc.).
- En République tchèque, aucune législation spécifique ne s'applique, les directives EU sur la protection des données s'appliquent, mais il y a un manque de respect de ces directives dans le cas des réseaux sociaux.
- En France, la CNIL a demandé que les entreprises étrangères de réseaux sociaux soient soumises à la législation européenne.

■ Sensibilisation et campagnes

- Généralement les utilisateurs ne sont pas suffisamment conscients des conséquences de leurs actes et des dangers du partage des données personnelles à une trop grand échelle, ainsi la plupart des

campagnes ciblent les utilisateurs, en particulier les enfants (par exemple, en République tchèque et en Roumanie).

Certaines bonnes pratiques peuvent être soulignées :

- En Finlande les employeurs ne peuvent pas utiliser les informations (sur leurs salariés) obtenues par moteur de recherche, Galleria IRC essaye d'éduquer par des vidéos pédagogiques, les images inappropriées sont détruites, une plate-forme de travail des jeunes a été réalisée sur internet, une unité de police est accessible en cas de problèmes.
- En Allemagne les organisations de consommateurs ont été leader des actions les plus importantes contre les réseaux sociaux pour les cas de violation de la vie privée : par exemple, une action en justice contre StudiVZ qui n'a pas respecté toutes les exigences. L'affaire est toujours en suspend, bien que certaines exigences aient été appliquées après la mise en œuvre du Code de conduite. Des actions ont été lancées également contre d'autres réseaux sociaux pour le changement des conditions d'utilisation afin d'être sûr que les données des abonnés ne soient utilisées que s'ils y consentent.
- En République tchèque, des campagnes s'adressent essentiellement aux enfants.
- Au Royaume-Uni un important débat a impliqué la société britannique sur les changements des conditions d'utilisation de Facebook au début de 2009 : les documents ont été lourdement critiqués, le processus pour revoir les conditions d'utilisation a été appelé « démocratie-théâtre ».

■ Recommandations et conclusions

1. Une disposition de l'Union européenne dans une directive protection des données devrait cibler spécifiquement ce sujet afin que les prestataires fournissent des choix de protection des données personnelles par défaut (la configuration d'un profil doit être vraiment facile et possible ; la fermeture permanente d'un compte doit être possible, y compris la suppression de toutes les données personnelles partagées ; les profils utilisateurs doivent être par défaut inaccessibles aux moteurs de recherche). Des campagnes doivent être menées visant les autorités publiques nationales et européennes et les autorités de protection des données pour que tous les réseaux sociaux soient soumis à la législation européenne.

2. Le « citoyen / consommateur » devrait avoir le droit de choisir sa législation nationale, et les normes les plus favorables pour la protection du « citoyen / consommateur » devraient s'appliquer.

3. Des campagnes de sensibilisation : les utilisateurs ne sont pas toujours suffisamment conscients des conséquences de leurs actes et des dangers du partage des données à caractère personnel à une trop grande échelle. Les jeunes doivent connaître les risques liés à la publication d'images et de textes sur Internet sans consentement ou de publier un contenu diffamatoire.

10. CONCLUSIONS ET RECOMMANDATIONS

Quelques remarques d'ordre général

Nous devons souligner que les informations concernant ces sujets sont éparses et difficiles à réunir : établir une base de données sur le sujet est un véritable défi et une nécessité pour la connaissance des droits, les comparaisons, l'évaluation, les interventions sur les tendances et les processus en cours, et la diffusion des bonnes pratiques. Il présente un réel intérêt au niveau européen. C'est la seule façon de savoir s'il existe des bonnes pratiques dans d'autres pays afin de permettre des progrès et argumenter sur des bases concrètes.
Les jeunes adultes représentent la majorité de la population concernée ou sont les principaux utilisateurs des outils identifiés en particulier des systèmes de communication multiples (mobiles, SMS, réseau social). De ce fait ils sont la population la plus exposée aux risques liés à l'utilisation de ces outils. Les bases de données nationales concernent d'abord les jeunes (bases de données à l'école à l'université dans plusieurs pays). De plus, ils obtiennent souvent avant les adultes une carte d'identité biométrique.
Mais notre travail pourrait concerner l'ensemble de la population. Toutes les données recueillies ne sont pas seulement valides pour notre public spécifique, mais aussi pour tous les publics.
Pour tous les sujets étudiés, l'utilisation, le développement et une large diffusion de toutes les nouvelles technologies entraînent de plus en plus d'intrusions dans la vie privée, ce qui est lié à la tendance « société de surveillance » dont les buts et le leitmotiv sont « sécurité » et « lutte contre la criminalité et le terrorisme ».
La raison en est le développement :

- des bases de données qui contiennent des informations sensibles ;
- de la conservation des données ;
- de l'interconnexion des bases de données (données demandées pour des utilisations commerciales et administratives) ;
- de l'utilisation des techniques biométriques et biologiques pour identifier et contrôler les individus

mais aussi l'utilisation croissante des nouvelles technologies pour délivrer librement des données à caractère personnel sur les réseaux ou par l'intermédiaire de communications interpersonnelles, sans prise de conscience des utilisations possibles de ces données.
Deux risques majeurs sont à prendre en considération : l'émergence d'une société de surveillance intrusive, la (ré)-utilisation de données personnelles (par exemple à des fins marketing et commerciales), sans le consentement ou la connaissance.

Les tendances

Les gouvernements mettent l'accent sur ces questions de sécurité et communiquent abondamment à ce sujet (démagogie et populisme) tandis que la communication sur les droits à la vie privée et aux libertés est quasi inexistante. Les tendances pour les législations nationales sont désormais données par le niveau européen et les modifications et développements juridiques nationaux sont souvent liés à la mise en œuvre des directives européennes ou dits comme tels. Mais cela n'efface pas toutes les caractéristiques nationales.
Les comparaisons montrent des différences entre chacun des pays pour la législation, l'application des législations et pour les fonctions effectivement traitées par les DPA, par exemple :

- L'Allemagne est particulièrement sensibilisée aux questions de la protection des données personnelles, et est par conséquent particulièrement attentive à la mise en œuvre d'une législation qui tienne compte du droit à la vie privée.
- Au Royaume-Uni, les garanties de protection de la vie privée sont plutôt faibles, en particulier pour les bases de données gouvernementales. C'est d'ailleurs le pays dans lequel la « société de surveillance » est la plus avancée, en dépit de nombreux rapports d'experts, de membres du parlement et d'ONG.
- La Roumanie commence seulement à réfléchir à la protection des données personnelles, avec une législation mise en œuvre dans le cadre d'un processus d'intégration à l'union européenne, avec une population peu consciente de ces questions.

Les tendances dans de nombreux pays montrent la pression croissante des Etats pour développer de plus en plus de bases de données centralisées contenant des informations sensibles, avec le risque d'avoir

ou de développer des interconnexions de fichiers, et de développer des systèmes de surveillance directe (vidéosurveillance en particulier).

L'autre tendance générale (transports publics, contrôle d'accès privés) est de mobiliser des informations sensibles au travers de l'utilisation de puces et de lecteurs RFID et de créer des bases de données sans réelle nécessité, souvent sans toutes les garanties nécessaires pour la sécurité et aussi avec la possibilité d'une éventuelle utilisation commerciale sans le consentement ou la connaissance de l'utilisateur.

Un des points principaux est que même si la législation existe, elle n'est pas toujours mise en œuvre ou respectée ni par les entreprises privées ni par l'Etat. Et l'application de la loi n'est pas suffisamment contrôlée avec des sanctions contraignantes au niveau national ou européen.

Pour conclure, une autre tendance très importante est la façon dont les systèmes de communications et les réseaux sociaux sont de plus en plus utilisés pour donner librement des informations personnelles (exposition de soi), alors que les risques et les possiblités de détournement de ces informations ne sont pas pris en compte.

Par conséquent, nos recommandations ciblent la législation et les politiques européennes ainsi que les législations nationales, mais visent également la sensibilisation de la population , dans la mesure où la protection de notre vie privée est aussi de la responsabilité de chacun.

1 - Nos propositions sont fondées sur les principes de protection des données édictés par l'UE (directive 95 notamment) qui doivent être réaffirmés

- **Le principe de nécessité. Pourquoi est-il nécessaire de créer des fichiers, par exemple : pour les enquêtes criminelles, l'optimisation des systèmes de transport public, les soins de santé d'urgence ?**
- **Le principe de finalité et sa dérogation ciblée « nécessaire dans une société démocratique », par exemple les transferts financiers entre les banques exigent la mise en place de fichiers et le transfert des données qui ne peuvent pas être détournées à d'autres fins, sauf par la police dans des cas ponctuels, ciblés et dans le respect du principe de proportionnalité ; idem à l'égard des dossiers commerciaux (cartes de fidélité commerciales).**
- **Le principe de proportionnalité. L'utilisation d'un fichier en dehors de son objectif principal doit être proportionnel au problème qui la nécessite et sur la base du consentement et, ou dans des cas exceptionnels, par exemple lutte contre la grande criminalité, elle doit toujours être centrée sur l'affaire et ne pas utiliser la totalité du fichier.**
- **La durée de rétention des données doit être strictement limitée à leur objet et par conséquent à leur utilisation et leur destruction doit pouvoir être surveillée.**
- **Le principe de sécurité.**
- **Toutes les personnes doivent avoir le droit d'être informées de l'utilisation de leurs données, de s'opposer au traitement de celles-ci sur la base de raisons légitimes, d'accéder à leurs données, de les faire rectifier et effacer si nécessaire.**
- **Une autorité indépendante doit être en mesure d'exercer un contrôle obligatoire avant que les fichiers soient mis en place, dans tous les cas où existe un risque particulier pour les droits de l'Homme, en particulier pour tous les traitements de données qui dérogent aux principes de base de la protection des données, pendant et après le traitement. Cette autorité de contrôle doit être complétée par des contrôles internes opérés par une personne spécifique nommé en interne par l'organisation exploitant le traitement des données et dont le travail est de vérifier la conformité du fichier avec la législation (prévu seulement comme facultatif pour les Etats membres dans la directive 95/46, mais déjà mis en œuvre dans plusieurs Etats membres et dans des institutions de l'Union européenne et quelques institutions de l'Union européenne comme Eurojust).**
- **Principe de la protection adéquate dans les pays tiers où les données doivent être transférées.**
- **Nécessité d'une norme internationale dont la référence pourrait être au minimum la Convention 108 du Conseil de l'Europe et son protocole additionnel.**
- **Les accords sur les échanges de données avec les pays tiers ne devraient être conclus qu'en conformité avec les normes européennes sur la protection des données et inclure la possibilité de recours juridiques, y compris dans les pays où les personnes concernées ne sont pas résidentes et / ou n'en possèdent pas la nationalité.**

2 - Vue d'ensemble de nos recommandations

L'Union européenne doit se mettre en conformité avec sa propre législation sur la protection des données à caractère personnel, avec la Charte des droits fondamentaux, avec la Convention européenne des droits de l'Homme, d'autant plus que la prolifération des fichiers de données personnelles, leur juxtaposition, les risques d'interopérabilité constituent une atteinte à l'intégrité des personnes concernées.

Si les droits de l'Homme peuvent être soumis à des limitations, celles-ci ne peuvent ne pas être de nature à les vider de leur substance. Les institutions européennes doivent restreindre les décisions fondées sur des dérogations aux principes de la protection des données pour des questions de sécurité. Les fichiers doivent être en conformité avec les droits de l'Homme, en particulier pour le respect de la vie privée et des libertés fondamentales. Dans tous les cas, ils doivent rester strictement dans le cadre de l'avis formulé par une autorité européenne indépendante, et chaque personne concernée doit être en mesure d'avoir accès à ses données personnelles et exercer un recours administratif et judiciaire.

L'entrée en vigueur du traité de Lisbonne donne à penser que l'Union européenne doit redéfinir une politique ambitieuse digne de celle qu'elle a initiée, qui réponde aux enjeux actuels, en s'appuyant sur les pouvoirs accrus du Parlement et sur l'article 8 de la Charte européenne des droits de l'Homme qui consacre le droit à la protection des données et la responsabilité de fait qu'a l'Europe, à l'échelle mondiale, dans ce domaine :

- Une (re)-évaluation de tous les instruments mis en œuvre sous la pression des questions de sécurité, qui devraient néanmoins respecter les principes de protection des données. En particulier, la directive sur la rétention des données, l'accord PNR, le passeport électronique européen devraient être remis en cause et pas seulement modifiés dans leur mise en œuvre (voir les conclusions et recommandations dans les chapitres sur ces sujets).

- Un regroupement (premier et troisième « piliers ») et un renforcement du cadre législatif de la loi fondamentale Données personnelles et de son cadre institutionnel au niveau national et européen (avec le maintien au niveau européen du Contrôleur européen (CEDP) et du « groupe de travail article 29 », en lui intégrant toutes les autorités spécifiques pour Europol, SIS, etc. et en le repositionnant institutionnellement, avec un mandat qui devra être revu en conséquence).

  Ce cadre législatif devra inclure en particulier certains points essentiels. De solides garanties en application du principe de proportionnalité pour les fichiers ADN de la police doivent être mises en place avec une nouvelle législation restrictive traitant spécifiquement des bases de données ADN. Les abus des contrôles biométriques doivent être strictement interdits. Les contrôles biométriques doivent être confrontés en particulier au principe de nécessité (exemple : le passeport biométrique). Des procédures de certification doivent être établies pour les réseaux sociaux, et ils doivent être soumis à la législation européenne et /ou nationale. La fiabilité de la protection des données à caractère personnel doit être vérifiée pour toutes les cartes de transport. Les utilisations de puces RFID doivent être soumises à des procédures de certification obligatoires d'autant plus que la sécurité des puces vis à vis des lecteurs peut être minime pour des préoccupations de rentabilité. De plus, l'option de cartes anonymes devra être obligatoire (nécessaire à la liberté de circulation), et l'interopérabilité avec d'autres fichiers interdite. Pour cela, toutes les fonctions relatives à différentes utilisations doivent être strictement définies et non contenues dans un même support (cartes bancaires, cartes de transport, cartes d'achat, cartes d'identité ou passeports électroniques).

  Le cadre institutionnel devra renforcer les autorités de protection des données avec des pouvoirs réels, y compris dans le domaine du suivi et des sanctions, en inscrivant leur statut dans la constitution. Leur indépendance doit aussi être rendue effective en leur donnant les moyens (ressources humaines et financières) pour jouer complètement leur rôle y compris celui d'information et de sensibilisation. Leurs fonctions doivent être renforcées et il faut veiller à ce que leurs avis et leurs conseils aux gouvernements soient rendus publics. Leurs activités doivent être menées de façon transparente avec une vaste consultation sur les projets d'avis, recommandations et réglementations.

  Le cadre institutionnel devra également renforcer la fonction du groupe 29 en le plaçant dans le cadre de la Commission et non pas en relation avec une DG spécifique, puisque son domaine de compétences est en interaction avec tous les domaines d'intervention de l'Union européenne, et lui allouer un budget significatif. Le dialogue avec la société civile devra être effectivement assuré aussi bien qu'avec les industriels et les Etats.

En outre, étant donné le nombre croissant de lois et de règlements visant à contrôler les citoyens dans le cadre de la lutte contre le terrorisme et pour le renforcement de la sécurité, ces « paquets », adoptés au niveau des Etats membres depuis la fin des années 90 pour certains ou depuis le 11 septembre 2001 pour les autres, devront être évalués du point de vue des lois fondamentales de protection des données personnelles.

- Pour des raisons pratiques, à court terme et dans l'intérêt général, un portail sera ouvert permettant d'accéder à tous les textes, à la fois généraux et ceux qui ont des applications particulières, au suivi de toutes les nouvelles initiatives d'où qu'elles proviennent (consultations, propositions, rapports, évaluations, etc.) et aux comptes-rendus des missions des autorités de contrôle (G29, les autorités de contrôle communes, Schengen, Europol, etc. ainsi que le Contrôleur européen). Un tel portail devrait également être mis en œuvre à chaque niveau national pour la dissémination de l'information émanant des autorités nationales de protection des données.
- Une approche éthique doit être adoptée vis-à-vis des lobbies industriels et de police, d'autant plus que les mesures prises peuvent favoriser les industriels des technologies de surveillance. La vente de données personnelles collectées par un organisme public à des entreprises ou des organisations privées doit être interdite. L'utilisation croissante de fichiers de profilage à des fins commerciales et marketing doit aussi être prise en compte et encadrée.
- Une initiative visant à la promotion du droit à la protection des données dans le monde entier doit être prise, fondée sur la dynamique de la Convention 108 et de son protocole additionnel, et soutenue par des politiques respectueuses des droits et libertés dans le domaine de la recherche, des normes, des partenariats avec des pays tiers et dans le domaine des projets soutenus dans les pays en voie de développement.
- Une politique ambitieuse de sensibilisation à la protection des données personnelles visera les citoyens : nous devons souligner que, globalement, la sensibilisation sur la vie privée et la protection des données personnelles est faible. Compte tenu de l'importance des besoins d'information des jeunes et des citoyens en général, l'Union européenne doit lancer des campagnes d'information et de sensibilisation dans laquelle les autorités de protection des données et la société civile doivent être fortement impliquées.
- Le rôle de la société civile dans le domaine de la vie privée, des libertés et du traitement des données personnelles doit être renforcé. Il est important que les associations de défense des droits tiennent compte de l'importance du sujet. De même, ces campagnes doivent s'appuyer sur les enseignants. De nombreux exemples de campagnes se trouvent dans chacun des chapitres thématiques.

Enfin nous insistons sur le fait que, tant au niveau national qu'européen, pour faire face à toutes ces questions, les décideurs doivent acquérir plus de connaissances sur les nouvelles technologies : ces compétences sont indispensables pour légiférer sur les technologies de l'information et de la communication.

Annexe : fiches d'études par pays

	Mobilité et transports	Identité biologique	Communications interpersonnelles	Réseaux sociaux	Autres
CZ	• Prague opencard • PNR • In Karta	• Fichiers ADN • Registre national de santé • Base de données ADN : génomique • Base de données ADN : fichier Národn9 • dépôt central des ordonnances électroniques	• Rétention des données de communications électroniques	• Lide.cz • Libimseti.cz • Spoluzati.cz • Facebook	• Base de données centralisée des registres des écoles • Base de données de l'Union des étudiants
FR	• Cartes de transport Navigo • PNR • Géo localisation au travail – téléphone portable	• Passeport biométrique • Contrôles d'accès : entreprises / écoles	• Messageries Gmail et SFR • Twitter et téléphonie	• Facebook • Copains d'avant • Myspace • Flikr • Skyrock blog	
ES	• Cartes de transport	• DNIE (document national d'identité électronique) • Passeport électronique • Accès gym	• Messenger (messagerie instantanée) • messages électroniques • Téléphone portable	• Tuenti • Facebook • Common	• C-R d'interviews
FI	• Cartes de transport	• Passeport Européen	• Téléphone portable et services télécom sur ad. IP	• IRC Galeria	
EL	• CCTV (videosurveillance)	• Projet pilote de l'aéroport d'Athènes • Base de données ADN	• Détecteur de mensonges	• Zoo.gr • Hi5.com	
NL	• Carte à puce OV	• Carte de loisirs Alcazar, carte fakkel, puce VIP; VIS2000; reconnaissance faciale lors des grands événements publics	• Services Telecom	• Hyves	
UK	• Plaques immatriculation • Frontières électroniques	• Registre ID • DNA	• Rétention des données	• Réseaux sociaux	• Base contact
D	• Pass véhicule	• Passeport électronique	• Rétention des données	• Réseaux sociaux	
RO	• Passeport électronique	• DNA	• Rétention des données	• Réseaux sociaux	

LDH, Ligue des droits de l'Homme
http://www.ldh-france.org

AEDH, Association européenne pour la défense des droits de l'Homme
http://www.aedh.eu

EDRi, European Digital Rights
http://edri.org

Pangea, Coordinadora Comunicació per a la Cooperació
http://pangea.org

IuRe, Iuridicum Remedium
http://www.iure.org

Cette publication a été éditée avec le soutien financier du programme Droits Fondamentaux & Citoyenneté de la Commission Européenne. Les contenus de cette publication sont de le seule responsabilité de la LDH, EDRi, AEDH, Pangea et IuRe et ne peuvent en aucun cas être pris comme le reflet des positions de la Commission Européenne.