COMMISSION EUROPÉENNE
DIRECTION GÉNÉRALE JUSTICE, LIBERTÉ ET SÉCURITÉ

ÉTUDE COMPARATIVE

SUR LES

DIFFÉRENTES APPROCHES DES NOUVEAUX DÉFIS EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE,

EN PARTICULIER À LA LUMIÈRE DES ÉVOLUTIONS TECHNOLOGIQUES

Contrat N° JLS/2008/C4/011 – 30-CE-0219363/00-28

RAPPORT FINAL

Présenté par :

LRDP KANTOR Ltd (Leader)

En association avec

Centre for Public Reform

Janvier 2010

TABLE DES MATIÈRES

		paras.:	page:
–	**Équipe de recherche**		2
–	**Glossaire et références Internet**		3
I.	**Introduction**	1 – 5	10
II.	**Présentation des défis**	6 – 14	13
III.	**Difficultés rencontrées pour relever ces défis**	15 – 18	17
IV.	**Impératifs fondamentaux**	19 – 25	21
V.	**Constats, conclusions et recommandations**	26 – 149	25
1.	APPROCHE DE BASE	26 – 29	25
2.	CHAMP D'APPLICATION DES RÈGLES DE L'UE EN MATIÈRE DE PROTECTION DES DONNÉES	30 – 35	26
3.	DROIT APPLICABLE	36 – 44	29
4.	HARMONISATION DU DROIT SUBSTANTIEL	45 – 98	32
A.	(NON-) HARMONISATION AU SEIN DE L'UE/EEE	47 – 79	33
B.	PAYS NON MEMBRES DE L'UE/EEE	80 – 89	44
C.	COMMENT PARVENIR À UNE PLUS GRANDE HARMONISATION	90 – 98	47
5.	COOPÉRATION AVEC LES PAYS NON MEMBRES DE L'UE/EEE (Y COMPRIS LES CONSTATATIONS DU CARACTÈRE «ADÉQUAT»)	99 – 103	50
6.	SUPERVISION ET EXÉUTION	104 – 108	52
7.	DROITS INDIVIDUELS ET RECOURS	109 – 113	53
8.	MESURES SUPPLÉMENTAIRES ET ALTERNATIVES	114 – 151	55
–	**Liste des annexes**		69

ÉQUIPE DE RECHERCHE:

	Titre/fonction:	**Institution(s):**	**Nationalité:**
Experts permanents:			
Douwe Korff	Professeur de droit international	London Metropolitan University, Londres, Royaume-Uni	NL
Ian Brown	Chargé de recherches	Oxford Internet Institute, Université d'Oxford, Royaume-Uni	UK
Experts spéciaux:			
Peter Blume	Professeur d'informatique juridique	Faculté de droit, Université de Copenhague, Copenhague, Danemark	DK
Graham Greenleaf	Professeur de droit	Université de Nouvelle-Galles du Sud, Sydney, Australie	AUS
Chris Hoofnagle	Maître de recherche	Berkeley Center for Law and Technology, Université de Californie, Berkeley, CA, États-Unis	USA
Lilian Mitrou	Professeur assistant	Département d'ingénierie des systèmes d'information et de communication, Université de l'Égée, Mytilene, Grèce	GR
Filip Pospíšil, Helena Svatošová, Marek Tichy	Chercheurs	ONG *Iuridicum Remedium*, Prague, République tchèque	CZ
Conseillers :			
Ross Anderson	Professeur d'ingénierie de sécurité	Université de Cambridge, Royaume-Uni	UK
Caspar Bowden	Conseiller principal pour la protection de la vie privée, Microsoft EME&A	Microsoft Corporation	UK
Katrin Nyman-Metcalf	Professeur de droit international et de droit comparé	Tallinn Law School, Université de technologie de Tallinn, Tallinn, Estonie	EST
Paul Whitehouse	Ancien commissaire de police (chef de la police)	Police du Sussex (retraité) aujourd'hui président de la Gangmasters Licensing Authority	UK

GLOSSAIRE ET RÉFÉRENCES INTERNET :

ADN : Acide désoxyribonucléique, un acide nucléique qui contient le code de l'information génétique. Il est de plus en plus utilisé pour les identifications, notamment dans le cadre d'autopsies, ainsi que dans les traitements thérapeutiques.

Adresse IP : Étiquette numérique, basée sur le «Protocole Internet» utilisé pour les communications entre dispositifs reliés à l'Internet, qui identifie le dispositif (généralement un ordinateur personnel ou PC) utilisé pour la communication.

ANASE : Association des nations de l'Asie du Sud-Est.
Voir: http://www.aseansec.org/

APPA : Asia Pacific Privacy Agencies.
Voir: http://www.privacy.gov.au/aboutus/international/appa

BBB : Better Business Bureau OnLine Privacy Seal. Label américain de protection des données personnelles. Voir: http://www.bbbonline.org/privacy/

BCR : Règles d'entreprise contraignantes. Règles d'autoréglementation visant à garantir le respect de la protection des données au sein des multinationales, prônées par le *WP 29**. Voir documents WP 29, WP 153, 154 et 155:
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_fr.htm

CCTV : Télévision en circuit fermé

CE : Communauté européenne, partie originelle de ce qui est aujourd'hui devenu l'*UE** et qui, jusqu'au *Traité de Lisbonne** (qui l'a abolie), constituait le «*Premier pilier*»* de l'UE.

CEDH : Convention européenne des Droits de l'Homme. Le principal instrument européen de protection des droits de l'Homme, mis en application par la Cour européenne des droits de l'Homme (*EctHR**) (voir à cette adresse pour suivre le lien)

CEDH(EctHR) : Cour européenne des Droits de l'Homme, chargée de faire respecter la Convention européenne des Droits de l'Homme (*CEDH**). Voir: http://www.echr.coe.int/ECHR/homepage_fr

CEPD : Contrôleur européen de la protection des données, chargé de veiller à ce que les institutions de l'UE respectent la protection des données et de donner des conseils sur les textes législatifs et les politiques relatifs à la protection des données. Voir: http://www.edps.europa.eu/EDPSWEB/

CEAP : Coopération économique Asie-Pacifique. Voir: http://www.apec.org/

Charte des droits fondamentaux : Charte des droits fondamentaux de l'Union européenne proclamée à Nice en 2000 et qui est devenue un instrument juridique contraignant depuis le *Traité de Lisbonne**. Contrairement à la Convention européenne des Droits de l'Homme (*CEDH**), la Charte contient en son article 8 une disposition spécifique garantissant la protection des données. Voir : http://www.europarl.europa.eu/charter/default_fr.htm

CJE : Cour de justice européenne. Nom complet: Cour de justice de l'Union européenne (*UE**). Voir: http://curia.europa.eu/jcms/jcms/Jo2_6999/

CJ-PD (COE) : Groupe de projet sur la protection des données (du Conseil de l'Europe), qui opère sous l'égide du Comité européen de coopération juridique (CDCJ) du *COE**. Voir: http://www.coe.int/T/E/Legal_Affairs/Legal_co-operation/Steering_Committees/cdcj/

COE : Conseil de l'Europe. La plus ancienne et la plus grande organisation européenne, qui est à l'origine de la Convention européenne des Droits de l'Homme (*CEDH**) et de la *Convention 108** (parmi de nombreux autres traités).

Convention 108 du COE : Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, série des traités du Conseil de l'Europe (STCE) N° 108, adoptée le 28 janvier 1981 (entrée en vigueur le 1er octobre 1985). Premier traité international sur la protection des données. Un Protocole additionnel à la Convention (STCE No. 181, adopté en 2001 et entré en vigueur en 2004) contient des clauses supplémentaires concernant les autorités de contrôle (*DPA**) et les flux de données transfrontaliers.

Dataveillance : Surveillance des individus par le biais des «traces de données» qu'ils laissent derrière eux dans la société électronique/de l'information, par exemple sur l'Internet, ou en payant par carte de crédit ou de débit.

DPA : Autorité chargée de la protection des données (aussi appelée [Bureau du] Commissaire à l'information ou Commissaire à la protection de la vie privée, etc.).

EEE : Espace économique européen. Groupe de pays liés à l'*UE** mais non membres de celle-ci. Depuis l'adhésion à l'UE de l'Autriche, de la Finlande et de la Suède, l'EEE ne concerne plus que trois pays: l'Islande, le Liechtenstein et la Norvège. Les pays de l'EEE sont tenus de mettre en œuvre l'*acquis* communautaire, notamment les directives relatives à la protection des données, au même titre que les États membres de l'UE. D'où les références aux «pays UE/EEE» dans le texte.

EPR : Dossier électronique du patient (aussi appelé Dossier médical électronique).

EuroPriSe : European Privacy Seal. Label européen de protection des données personnelles, créé avec le soutien de la Commission de l'UE. Voir: https://www.european-privacy-seal.eu/

FRA : Agence des droits fondamentaux de l'Union européenne. Voir: http://fra.europa.eu/fraWebsite/home/home_en.htm

Informatique dématérialisée : Type d'informatique dans lequel les données de l'utilisateur ainsi que les applications qu'il utilise ne sont plus installées sur l'ordinateur personnel (PC) de l'utilisateur mais hébergées sur des serveurs et mises à sa disposition via des navigateurs sur l'Internet.

MMS : Service de messagerie multimédia, utilisé pour envoyer un contenu multimédia contenant des messages courts («textes»), généralement via un téléphone portable (voir aussi *SMS**).

OCDE : Organisation de coopération et de développement économiques. Voir : http://www.oecd.org/

OMC : Organisation mondiale du commerce. Voir: http://www.wto.org/

ONG : Organisation non gouvernementale (par opposition à une organisation gouvernementale ou intergouvernementale [OIG])

P3P : Platform for Privacy Preferences (Plate-forme de préférences relatives à la protection de la vie privée). Technologie renforçant la protection de la vie privée (*PET*)* conçue pour permettre aux utilisateurs de connaître les pratiques des sites Internet en matière de protection de la vie privée et de définir les paramètres de leur choix. Voir: http://www.w3.org/P3P/

PBD : Privacy By Design (prise en compte du respect de la vie privée dès la conception). Approche de la conception des systèmes informatiques élaborée par le Commissaire à la protection de la vie privée de l'Ontario mais aussi prônée (par exemple) par le Commissaire à l'information du Royaume-Uni, qui préconise la fabrication et l'utilisation de systèmes respectueux de la vie privée, voir: http://www.privacybydesign.ca/ et: http://www.ico.gov.uk/about_us/news_and_views/current_topics/privacy_by_design.aspx

PET : Privacy Enhancing Technologies (technologies renforçant la protection de la vie privée).

PIA : Privacy Impact Assessment (évaluation des facteurs relatifs à la vie privée). Évaluation des produits, services, politiques ou systèmes réalisée

avant la mise en œuvre de ceux-ci afin de s'assurer qu'ils respectent la vie privée, obligatoire dans plusieurs territoires.

PNR : Passenger Name Record (dossier passager). Liste d'informations relatives aux passagers des vols internationaux, dont la collecte et la divulgation obligatoires aux États-Unis ont suscité une vive controverse sur la protection des données. Voir l'Avis 2/2004 du «groupe de travail Article 29» (*WP29**) du 29 janvier 2004 (WP87): http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp87_fr.pdf (Cf. également les avis et décisions du Conseil et de la Commission à ce sujet: http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_fr.htm

Premier pilier : Autre nom donné à la Communauté européenne (*CE**), la partie originelle de ce qui constitue aujourd'hui l'*UE**. Il existait également un deuxième pilier, qui recouvrait la politique étrangère et de sécurité commune de l'UE, ainsi qu'un *troisième pilier** qui couvrait la coopération policière et judiciaire en matière pénale. Ces piliers ont été abolis par le *Traité de Lisbonne**.

Qui tam : Abréviation de l'expression latine «*qui tam pro Domino rege quam pro sic ipso in hoc parte sequitur*», qui signifie «celui qui, aussi bien pour le Roi que pour lui-même, engage des poursuites à cet égard». Cette expression est couramment utilisée pour renvoyer à une disposition spéciale de la loi fédérale américaine Civil False Claims Act, qui permet aux particuliers d'intenter un procès pour fraude au nom du Gouvernement américain à l'encontre de fournisseurs de l'État et d'autres fournisseurs qui reçoivent ou utilisent des fonds publics. S'il gagne son procès, le citoyen en question reçoit un pourcentage des sommes recouvrées.

RFID : Radio Frequency Identification (identification par radiofréquence). Petit dispositif de localisation qui peut être placé sur des vêtements, des passeports, etc. Voir la Recommandation de la Commission de l'UE C (2900) 3200 (final) du 12.5.2009 *sur la mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence* (en anglais): http://ec.europa.eu/information_society/policy/rfid/documents/recommandationonrfid2009.pdf

SMS : Short Messaging Service (service de messagerie texte), aussi appelé message textuel (ou «texte»), généralement envoyé via un téléphone portable (voir aussi *MMS**)

SNS : Social Networking Sites. Réseaux sociaux numériques, tels que FaceBook.

Solange : Mot allemand signifiant «à condition que». Le «problème *solange*» est le problème qui se pose lorsque des tribunaux (constitutionnels) nationaux

refusent d'accepter la primauté du droit européen s'ils estiment que ce droit n'est pas conforme aux dispositions relatives aux droits de l'Homme fondamentaux de la Constitution nationale concernée. Ce problème s'est principalement posé en Allemagne mais il existe également dans d'autres pays où les droits de l'Homme sont solidement protégés par la Constitution, notamment l'Italie.

Sphère de sécurité : Arrangement conclu entre l'UE et les États-Unis, en vertu duquel les entreprises américaines peuvent déclarer se conformer aux principes européens de protection des données, et sont ensuite surveillées par la Commission fédérale américaine du commerce (Federal Trade Commission - FTA), voir: http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/adequacy-faq1_fr.htm

SWIFT : Society for Worldwide Interbank Financial Telecommunication (Société de télécommunications interbancaires mondiales). Organisme interbancaire qui facilite les transferts bancaires internationaux et qui a fait l'objet d'une vive controverse au sujet de la protection des données. Voir l'Avis 10/2006 du «groupe de travail Article 29» (*WP29**) du 22 novembre 2006 (WP128): http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_fr.pdf

TFUE : Traité sur le fonctionnement de l'Union européenne. Nouveau nom donné au Traité instituant la Communauté européenne. Le TFUE a été modifié (mais pas remplacé) par le *Traité de Lisbonne**.

Traité de Lisbonne : Signé à Lisbonne le 13 décembre 2007, JO 2007/C 306/01. Le Traité de Lisbonne a modifié (mais pas remplacé) le Traité sur l'Union européenne (TUE) et le Traité instituant la Communauté européenne (TCE, renommé depuis lors Traité sur le fonctionnement de l'Union européenne ou *TFUE**). Le Traité de Lisbonne a rationalisé les processus décisionnels au sein de l'UE et aboli les trois «piliers» de l'UE qui existaient autrefois (voir *Premier pilier** et *Troisième pilier**).

Traité de Prüm : Accord international de coopération dans le domaine policier signé le 27 mai 2005 par l'Allemagne, l'Autriche, la Belgique, l'Espagne, la France, le Luxembourg et les Pays-Bas et qui, depuis l'entrée en vigueur du *Traité de Lisbonne**, fait partie intégrante du cadre législatif général de l'Union européenne et sera mis en œuvre dans tous les États membres. Voir: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/803

Troisième pilier : Partie de l'*UE** qui, autrefois, couvrait la coopération policière et judiciaire en matière pénale. Il existait également un premier pilier, qui recouvrait la *CE**, et un deuxième pilier, qui recouvrait la politique étrangère et de sécurité commune de l'UE. Les trois piliers ont été abolis par le *Traité de Lisbonne**.

TRUST-e : Label américain de protection de la vie privée. Voir (en anglais): http://www.truste.com/

TrustGuard : Label américain qui vise à garantir à la fois le respect de la vie privée des consommateurs, la sécurité de leurs données personnelles et la protection de l'identité des entreprises: Voir (en anglais): http://www.trust-guard.com/

UE : Union européenne. Voir: http://europa.eu/

ULD : Centre indépendant pour la protection des données (*Unabhängiges Landes-zentrum für Datenschutz*) du *Land* allemand de Schleswig-Holstein, qui administre également le système du label européen de protection des données personnelles (*EuroPriSe**).

VRM : Vendor Relationship Management. Système de gestion des données centré sur le client (et respectueux de la vie privée) (par opposition aux systèmes de gestion des relations client centrés sur l'entreprise, généralement moins respectueux de la vie privée)

WP29 : «Groupe de travail Article 29» (ou *Groupe de Travail*) créé en vertu de la principale directive *CE** relative à la protection des données (directive 95/46/CE), qui fournit des avis et conseils importants sur l'application et l'interprétation de cette directive ainsi que des autres directives relatives à la protection des données.
Voir: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_fr.htm

Pour la définition des principaux concepts utilisés dans la directive relative à la protection des données, voir l'article 2 de la directive. Celui-ci définit les notions ci-après:

- «Données à caractère personnel» (Article 2(a))
- «Traitement [des données à caractère personnel» (Article 2(b))
- «Fichier de données à caractère personnel»/«fichier» (Article 2(c))
- «Responsable du traitement» (Article 2(d))
- «Sous-traitant» (Article 2(e))
- «Tiers» (Article 2(f))
- «Destinataire» (Article 2(g))
- «Consentement de la personne concernée» (Article 2(h))

Le rapport fait également référence à différents projets ou programmes européens, à propos desquels vous trouverez de plus amples informations sur les sites Internet ci-après:

EuroPriSe	:	https://www.european-privacy-seal.eu/
PRIME	:	https://www.prime-project.eu/
PRISE	:	http://www.prise.oeaw.ac.at/

Pour les différentes applications Internet mentionnées dans le texte, consulter les sites Internet pertinents:

Amazon	:	http://www.amazon.com/ et les sites nationaux tels que: http://www.amazon.co.uk/
Boing Boing	:	http://boingboing.net/
Facebook	:	http://www.facebook.com/
Flickr	:	http://www.flickr.com/
Google	:	http://www.google.com/, et les sites nationaux tels que: http://www.google.co.uk/
MySpace	:	http://www.myspace.com/
YouTube	:	http://www.youtube.com/

- o – O – o -

I. Introduction

1. Le présent document est le rapport final d'une étude commandée par la Direction générale Justice, liberté et sécurité de la Commission européenne et menée sous la direction de l'Unité Protection des données entre octobre 2008 et août 2009. Il s'inscrit dans le prolongement du rapport initial présenté en décembre 2008, du rapport intermédiaire présenté en mars 2009 (révisé à la lumière des commentaires de la Commission) et du projet de rapport final présenté en août 2009. Il prend en compte les derniers commentaires de la Commission.

2. L'étude a été menée par le Prof. Douwe Korff de la London Metropolitan University et le Dr. Ian Brown de l'Oxford Internet Institute de l'Université d'Oxford, assistés des experts européens et non européens suivants: Prof. Peter Blume (Danemark), Prof. Graham Greenleaf (Australie), Prof. Chris Hoofnagle (E-U), Prof. Lilian Mitrou (Grèce), Filip Pospíšil, Helena Svatošová, Marek Tichy (République tchèque) ; et conseillés par: Prof. Ross Anderson (R-U), Caspar Bowden (R-U/France), Paul Whitehouse (R-U) et Prof. Katrin Nyman-Metcalf (Estonie). (Pour des informations plus détaillées à ce sujet, voir la page 2 ci-dessus).

3. Cette étude avait pour objectifs d'identifier les défis que posent les phénomènes sociaux et techniques actuels du point de vue de la protection des données à caractère personnel, parmi lesquels:

   - ✓ *l'Internet;*
   - ✓ *la mondialisation;*
   - ✓ *l'omniprésence croissante des données à caractère personnel et de leur collecte;*
   - ✓ *la puissance et les capacités croissantes des ordinateurs et autres dispositifs de traitement des données;*
   - ✓ *les nouvelles technologies spéciales telles que la RFID, la biométrie, les reconnaissances faciale et autres, etc.;*
   - ✓ *la surveillance accrue (et «dataveillance»); et*
   - ✓ *l'utilisation accrue des données à caractère personnel à des fins autres que celles auxquelles elles ont été collectées, en particulier dans le cadre de la sécurité nationale et de la lutte contre le crime organisé et le terrorisme* -

   et d'élaborer un rapport qui dresse une analyse comparative des solutions à ces défis proposées par les différents systèmes réglementaires et non réglementaires (au sein et en dehors de l'UE) et qui tente de déterminer si le cadre juridique de la principale directive CE relative à la protection des données (directive 95/46/CE) offre toujours une protection appropriée ou s'il y a lieu d'envisager de le modifier à la lumière des solutions identifiées comme étant les plus efficaces. Voici ce rapport.

4. Comme le souhaitait la Commission, l'équipe a procédé à un examen approfondi de tous les principaux aspects de la mise en œuvre de la directive dans les systèmes juridiques de plusieurs États membres prédéfinis de l'UE (tant du point de vue des normes de fond que du point de vue des procédures formelles et de la supervision), et s'est intéressée à la question du chevauchement des compétences (conflit des lois) au sein de l'UE. Nous avons également étudié le système réglementaire dans ce domaine aux États-Unis, aux niveaux fédéral et fédéré, dans deux états représentatifs; dans deux

autres pays tiers membres de l'OCDE, et dans deux pays qui n'appartiennent pas à l'Espace économique européen et qui ne sont pas membres de l'OCDE. Notre étude a ainsi couvert plus d'une douzaine de systèmes juridiques extrêmement différents.

Ces travaux ont débouché sur l'élaboration d'une série de rapports par pays, présentés en annexe au présent projet de rapport final, concernant les pays et territoires ci-après :

PAYS ET CIRCONSCRIPTIONS ÉTUDIÉS:

A. Pays européens :

- Allemagne
- Danemark
- France
- Grèce
- République tchèque
- Royaume-Uni

B. Pays et territoires non européens :

- Australie
- États-Unis :
  - Niveau fédéral
  - Californie
  - New Jersey
- Hong-Kong
- Inde
- Japon

5. Conformément au contrat et aux souhaits de la Commission, le présent rapport (final), en tant que tel, se veut bref et se concentre essentiellement sur les principaux sujets de l'étude. De plus amples informations ainsi que des analyses plus approfondies sont fournies dans des rapports et documents distincts, présentés en annexe au présent rapport final (voir liste des annexes en fin de rapport). La plupart de ces documents ont déjà été présentés précédemment dans le cadre du rapport intermédiaire mais ils ont été complétés à la lumière des commentaires de la Commission, en particulier:

- La **Section II** du présent Projet de rapport final présente les défis que nous avons identifiés comme découlant des phénomènes énumérés au paragraphe 3 ci-dessus.

  Pour en savoir plus, voir : Document de travail n°1 : The challenges to European data protection laws and principles - An overview of the global social and technical developments and of the challenges they pose to protection des données.

- La **Section III** présente notre synthèse et notre évaluation globale du régime européen actuellement en vigueur en matière de protection des données ainsi que des difficultés que l'UE rencontre pour relever les défis susmentionnés, par comparaison à des problèmes similaires (ou différents) dans des pays et territoires non membres de l'UE, comme nous le verrons plus en détail à la Section V (voir l'alinéa de cette section, ci-dessous, pour les références).

– La **Section IV** aborde de façon très succincte quelques questions fondamentales plus larges qu'il convient de prendre en compte dans toutes les études sur le régime de protection des données dans l'UE.

Pour en savoir plus, voir : Document de travail n°1 (déjà mentionné); Douwe Korff, *Paper No. 4: The Legal Framework*, dans Ian Brown & Douwe Korff, Privacy & Law Enforcement, étude pour le Commissaire à l'information du Royaume-Uni, 2004, (inclus dans les documents fournis en annexe au présent rapport); et les Rapports par pays (en particulier le rapport concernant l'Allemagne).

– La **Section V** présente nos conclusions et recommandations plus spécifiques. Celles-ci s'appuient sur l'évaluation globale exposée à la Section III, et tiennent compte des questions fondamentales posées à la section IV. Cette section tente d'identifier, à partir des nombreuses informations comparatives recueillies dans le cadre de l'étude, les réponses les plus appropriées et les plus efficaces aux différents défis, y compris les meilleures approches et les meilleures pratiques juridiques, ainsi que des solutions innovantes alternatives à ces défis (en particulier des solutions qui n'ont pas encore été entièrement testées en Europe), et des suggestions sur la meilleure façon de les utiliser en vue de préserver et de renforcer le régime européen de protection des données.

Pour en savoir plus (en particulier concernant les analyses de fond), voir: Document de travail n°2 : Protection des données laws in the EU - The difficulties in meeting the challenges posed by global social and technical developments, ainsi que les Rapports par pays.

– Enfin, ce rapport est assorti d'un **glossaire** de termes techniques (ci-dessus, en p. 3), d'un **tableau comparatif** (en annexe) et d'une **note de synthèse**. Cette synthèse fait l'objet d'un document distinct afin d'en faciliter la diffusion.

- o – O – o -

II. Présentation des défis[1]

6. De manière générale, les défis dont il est question dans cette étude sont divisés en deux catégories (qui s'entremêlent). La première catégorie comprend les défis liés aux évolutions techniques; la deuxième recouvre les défis liés à des changements et à des choix sociaux et politiques. Elles s'entremêlent dans le sens où de nombreuses nouvelles technologies, d'une part rendent l'application effective de la protection des données plus difficile (bien que certaines d'entre elles peuvent la faciliter) et, d'autre part, appellent la mise en place de nouvelles politiques, plus intrusives, ou sont volontiers utilisées pour les renforcer.

7. Nous avons observé des changements technologiques spectaculaires depuis la première directive sur la protection des données proposée par la Commission européenne en 1990. L'Internet a dépassé le cadre des laboratoires universitaires et s'est immiscé dans 56 % des foyers européens et dans 95 % des entreprises de l'OCDE. La puissance du traitement informatique des données a continué d'évoluer suivant la loi de Moore, et la densité des transistors a doublé tous les 18-24 mois – ce qui signifie qu'elle s'est multipliée par mille au cours des vingt dernières années. La capacité de stockage des ordinateurs et le débit des communications ont tous deux connu une accélération encore plus frénétique puisqu'ils ont doublé tous les 12 mois, et se sont donc multipliés par mille tous les dix ans. Ces augmentations exponentielles ont considérablement renforcé la capacité des organisations de collecter, stocker et traiter les données à caractère personnel. L'environnement physique est désormais saturé de capteurs tels que caméras de télévision en circuit fermé et téléphones portables, et d'identifiants biométriques et électroniques utilisés pour relier les données aux individus. Dans le monde numérique, presque toutes les communications et accès à des pages Web laissent derrière elles des empreintes détaillées. L'Internet et les appareils informationnels portables permettent le transfert de grandes quantités de données entre territoires, et ce de façon très banalisée. Les outils d'extraction de données tentent d'identifier des modèles dans de vastes ensembles de données personnelles, à la fois pour identifier les personnes «présentant un intérêt» et pour tenter de prévoir leurs intérêts et leurs préférences. De nouvelles multinationales se sont créées autour de ces technologies afin de proposer leurs services à une clientèle mondiale, les petites entreprises sous-traitant le traitement des données de leurs employés et clients à des entreprises des pays en développement.

8. De plus en plus, les gouvernements analysent et échangent des informations sur leurs citoyens en réaction aux craintes liées aux attaques terroristes. Les individus utilisent des réseaux sociaux numériques pour partager des informations concernant leur famille et eux-mêmes, leurs amis et leurs collègues. Compte tenu de l'ubiquité des données à caractère personnel et de la collecte de données, la position par défaut des organismes publics et privés consiste non plus à devoir décider de collecter des données mais plutôt à faire un effort pour ne pas collecter des données (de plus en plus sensibles).[2]

---

[1] Pour obtenir des informations détaillées et des références complètes, voir Document de travail n° 1: The challenges to European data protection laws and principles - An overview of the global social and technical developments and of the challenges they pose to protection des données. Cette section consiste essentiellement en un résumé des questions traitées plus en détail dans ce document.

[2] Nous utilisons ici le terme «position par défaut» pour décrire une attitude socio-organisationnelle et non

9. Cette évolution technique alimente les grandes tendances sociales et politiques actuelles. Nous sommes tous préoccupés par le terrorisme, la pornographie enfantine et le crime organisé international grave. L'État s'inquiète aussi de l'explosion des budgets des soins de santé, de l'éducation et de la protection sociale. Les gouvernements veulent encourager les «bons» comportements et dissuader les «mauvais» comportements (qu'il convient ici d'entendre dans un sens beaucoup plus large que «non-criminel» par opposition à «criminel»). Dans certains pays (dans l'UE, en particulier au Royaume-Uni), les autorités sont convaincues que plus leurs responsables collectent et partagent des informations, plus elles seront aptes à combattre les différents maux de la société, qu'il s'agisse de la grossesse chez les adolescentes, de l'obésité ou de l'«extrémisme», qui peut conduire au terrorisme. Les systèmes d'administration en ligne contiennent généralement de grandes quantités de données sensibles à caractère personnel concernant des populations entières, lesquelles sont partagées entre les services gouvernementaux via des «passerelles» spécifiques prévues dans la législation. Les applications d'«arrière-guichet» sont axées sur le renforcement de l'efficacité du traitement des données et sur l'utilisation de nouveaux services (notamment la détection et la prévention des fraudes liées au paiement des prestations et aux déclarations fiscales) à l'insu du citoyen. Les «portails» permettent aux citoyens de dialoguer en ligne avec le gouvernement, de communiquer des informations telles que les déclarations fiscales et de demander des services sans qu'aucune conversation téléphonique ou en face à face entre les parties ne soit nécessaire et sans qu'aucun formulaire ne doive être rempli manuellement. Les dossiers électroniques des patients (EPR), qui sont la version électronique des dossiers médicaux, sont envisagés au niveau national dans certains pays comme la France, les États-Unis, le Canada, l'Allemagne et le Royaume-Uni. La plupart de ces projets s'articulent autour de normes d'interopérabilité permettant aux différents fournisseurs de soins de santé (publics et privés) d'échanger des informations médicales lorsque les patients sont traités en plusieurs endroits différents. Le séquençage du génome des patients devrait devenir une procédure de routine en raison de la chute de son coût. Le vieillissement de la génération des «baby-boomers» en Amérique du Nord et en Europe entraînera probablement de fortes pressions sur les coûts du traitement ambulatoire des maladies chroniques chez les personnes âgées, et nous devrions donc avoir des informations beaucoup plus détaillées sur les indicateurs physiologiques ainsi que des données plus générales sur le mode de vie des personnes âgées et des personnes en mauvaise santé. Les organismes chargés de l'application des lois et les agences de renseignements cherchent depuis longtemps à avoir accès à toute une série d'informations personnelles générées par les systèmes d'information et créées à des fins diverses. Cette tendance s'est intensifiée depuis 2001 sous le couvert de la «sécurité nationale» et de la lutte contre le terrorisme (notamment la surveillance des transactions financières afin d'enrayer le blanchiment d'argent). De nombreux gouvernements se sont arrogé le droit d'exiger des fournisseurs d'accès à Internet que leurs réseaux puissent être mis sur écoute et qu'ils conservent les données relatives aux communications des clients afin que les responsables puissent ensuite y avoir accès. La protection des données est considérée comme un obstacle aux politiques publiques de ce type.

---

un réglage technique. La question des réglages par défaut des applications (y compris les applications sur Internet) est abordée à la Section V, sous-section V.8, ci-dessous. Voir aussi la section V, sous-section V.2(ii), para. 35.

10. Les détaillants exerçant désormais leurs activités en ligne et de nouvelles sociétés en ligne telles qu'Amazon s'étant accaparé une importante part des marchés mondiaux, ils ont tiré parti de la capacité des serveurs de compiler un historique détaillé des transactions de leurs clients. Les magasins en ligne peuvent non seulement étudier le comportement d'achat de leurs clients mais aussi les différents produits que le client examine, et pendant combien de temps il hésite avant de décider ou non de l'acheter. Les réseaux publicitaires peuvent retracer les activités de navigation des individus à travers des milliers de sites. Les fournisseurs de services tels que les moteurs de recherche peuvent stocker toutes les informations communiquées par un utilisateur, notamment les termes recherchés. Le groupe de travail «Article 29» a dû faire pression sur les sociétés telles que Google afin qu'elles limitent la durée de stockage des informations mais de nombreux modèles commerciaux en ligne dépendent des revenus publicitaires, et ces sociétés seront de plus en plus incitées à cibler plus efficacement les publicités en utilisant des informations relatives aux intérêts des utilisateurs. Il est difficile, voire presque impossible, pour le consommateur moyen d'empêcher cette surveillance.

11. Les technologies «Web 2.0» permettent aux utilisateurs de créer et de partager des textes ainsi que des contenus audio et vidéo sur des blogs et sur des sites de photos et de vidéos tels que Flickr et YouTube, sans oublier les réseaux sociaux désormais omniprésents, tels que MySpace et Facebook. Ces nouvelles possibilités, ajoutées aux appareils photo et caméras dont sont équipés la plupart des téléphones portables, permettent aux individus de partager des informations sur eux-mêmes et sur leur entourage dans une mesure sans précédent. Les réseaux sociaux comptent désormais des centaines de millions de membres à travers le monde, tandis que les blogs célèbres tels que BoingBoing ont un lectorat qui rivalise avec celui des journaux nationaux.

12. Par ailleurs, les politiques technologiques et les politiques publiques ont tendance à mondialiser la collecte et la diffusion des données, et à disperser le stockage des données. Le citoyen moyen ainsi que les criminels et les terroristes se déplacent et exercent leurs activités dans de nombreux pays. Conformément aux normes relatives aux passeports établies récemment par l'Organisation de l'aviation civile internationale, la puce fixée sur les nouveaux «passeports électroniques» doit contenir les empreintes digitales ainsi que l'image faciale. Aujourd'hui, l'UE à son tour exige que ces données figurent dans les passeports des États appartenant à l'espace Schengen, en partie en réaction aux menaces des États-Unis qui, en cas de refus d'obtempérer, supprimeraient l'exemption de visa pour les ressortissants européens. Des tests à grande échelle ont mis en évidence des difficultés substantielles lors de l'enregistrement et de la vérification des empreintes digitales et des scanners de l'iris, en particulier pour les personnes handicapées. Les données à caractère personnel voyagent beaucoup plus, non seulement sur l'Internet via les sites des réseaux sociaux et les magasins en ligne mais aussi dans le cadre de la coopération internationale entre les autorités publiques, destinée à permettre d'identifier les hooligans, les migrants illégaux ou ceux qui font l'objet d'un trafic, les éléments subversifs, les terroristes et les pédophiles. L'attribution de l'une de ces étiquettes par une autorité, ou même sur un site social, dans n'importe quel pays, peut rapidement conduire à la généralisation de cette stigmatisation sans qu'il ne soit possible de demander des explications à l'organisme qui a posé cette étiquette (ou même d'identifier celui-ci). La Cour européenne des Droits de l'Homme a estimé récemment que le caractère systématique de l'utilisation des bases de données d'ADN au Royaume-Uni constituait une atteinte au droit à la vie privée consacré par la

Convention européenne (et pourtant, en vertu du «principe de disponibilité» de La Haye et du Traité de Prüm, nous constatons une augmentation du partage de ces données par les organismes chargés de l'application de la loi) et que les données n'étaient pas protégées de façon «pleinement satisfaisante», d'après le Contrôleur européen de la protection des données.

13. Enfin, il convient de prendre en compte les contraintes technologiques. Un grand nombre de ces technologies se heurtent à d'importantes limites, souvent inhérentes aux technologies elles-mêmes. La reconnaissance faciale et la reconnaissance de la démarche sont loin d'être parfaites. Les données biométriques ne sont pas aussi probantes que ce que l'on croit. Le «profilage» est confronté à ses propres limites. Le US National Research Council a publié récemment un rapport sur les technologies de lutte contre le terrorisme, qui conclut: «*il n'existe pas de consensus au sein de la communauté scientifique, ni au sein du comité, quant à savoir si les techniques de surveillance du comportement ou de contrôle physiologique sont prêtes à être utilisées dans le cadre de la lutte contre le terrorisme dans l'état actuel de la science*». Il s'agit là d'un obstacle majeur dû au nombre extrêmement élevé de faux positifs obtenus lors de la recherche de terroristes potentiels et à la facilité avec laquelle les terroristes adaptent leur comportement afin de dissimuler leurs intentions. Certains craignent également que l'extraction de données ne conduise à une discrimination systématique, par laquelle les individus seraient traités de façon inéquitable sur la base de simples suppositions sur leur comportement découlant de données transactionnelles antérieures.

14. Il convient de tenir dûment compte de ces contraintes dans toute analyse des évolutions technologiques. Une confiance excessive dans les technologies, aussi merveilleuses qu'elles puissent paraissent, peut entraîner des injustices graves et une mauvaise gouvernance. Une protection efficace des données permet non seulement le respect de la vie privée au sens strict du terme mais aussi une protection contre ce type de tendances et d'impacts.

- o – O – o -

III. Difficultés rencontrées pour relever ces défis: résumé et aperçu[3]

15. Les principes, règles et critères fondamentaux de la protection des données, tels qu'ils ont été définis en Europe par le COE et l'UE et tels qu'ils ont été approuvés au niveau mondial, en particulier par l'OCDE, ont résisté au passage du temps, même si certains aspects mériteraient d'être consolidés. Le fait qu'ils soient de plus en plus souvent adoptés comme fondement des textes législatifs dans de nombreuses régions du monde, y compris en Asie et en Afrique[4], atteste qu'ils sont largement approuvés.

En revanche, leur impact sur les lois de protection de la vie privée aux États-Unis a été moins grand: certaines lois américaines en la matière reprennent quelques-uns des principes de base de la protection des données mais le champ d'application de ces lois est très limité. La collecte d'une grande quantité d'informations tombe donc sous le coup d'autres règles, notamment des règles relatives aux pratiques commerciales déloyales ou de nature à induire en erreur.[5] Toutefois, cela a au moins servi à mettre en évidence la faiblesse du modèle américain (dans la mesure où l'on peut parler d'un seul modèle dans ce cas précis). Les principes européens de base doivent donc être réaffirmés et de préférence renforcés; de même, l'Europe doit poursuivre ses efforts pour encourager leur adoption dans le monde entier.

Ce point est traité plus en détail (en particulier en référence au document de travail N°2) à la Section V, sous-section V.1.

---

[3] Pour un examen plus détaillé des sujets abordés dans cette section, voir la Section V ci-dessous. Pour des informations plus détaillées (en particulier concernant les analyses sous-jacentes) et des références complètes, voir le Document du Groupe de travail n°2: Data Protection laws in the EU - The difficulties in meeting the challenges posed by global social and technical developments, présenté en annexe au présent rapport. Veuillez noter qu'il s'agit d'une nouvelle version étendue du même document que celui qui a été présenté dans le cadre du Rapport intermédiaire.

[4] La Convention du COE sur la protection des données (STCE N°108) et la directive de la CE (directive 95/46/CE) sont indubitablement la principale source d'inspiration de toutes les lois européennes en matière de protection des données, y compris des lois des États candidats à l'adhésion et d'autres pays tels que la Russie. Pour ce qui concerne la région Asie-Pacifique, voir l'étude comparative de Graham Greenleaf, Twenty-one years of Asia-Pacific data protection, Privacy Laws & Business International, numéro 101, octobre 2009, et plus particulièrement le passage suivant: «*Les influences sur les principes de protection des données [dans la région Asie-Pacifique] sont essentiellement les lignes directrices de l'OCDE et la directive de la CE mais le cadre du CEAP concernant le respect de la vie privée n'a pas encore eu d'influence directe. L'influence de la directive de l'UE semble plutôt se renforcer au fil du temps*». (Conclusions, p. 11). La loi de la Région administrative spéciale de Macao en particulier est élaborée sur le modèle de la directive (via la législation portugaise), le projet de loi à l'étude en Chine en 2006-7 était, lui aussi, fortement influencé par l'UE, tout comme la législation sud-coréenne. Des progrès modestes sont également réalisés concernant l'introduction de la protection des données en Afrique, notamment avec l'aide de l'autorité française de protection des données, la CNIL. Grâce à cette aide, les nouvelles lois créées sur ce continent s'inspirent, elles aussi, clairement des instruments européens. Pour en savoir plus sur un nouveau projet de loi sud-africaine élaboré en conformité avec la directive, voir l'article de Iain Currie dans Privacy Laws & Business International, numéro 101, octobre 2009. Il convient également de mentionner les travaux entrepris récemment par la Conférence internationale des Commissaires à la protection des données et de la vie privée en vue de la mise en place de normes mondiales fondées sur les normes européennes dans le cadre de l'«Initiative de Barcelone» ainsi que l'engagement pris par une large coalition d'organisations de la société civile en faveur de cette initiative au travers de leur «Déclaration de Madrid», lancée le 3 novembre 2009.

[5] Voir le *Rapport concernant les États-Unis*, sections 2 et 4.

16. Toutefois, leur application et leur mise en œuvre spécifiques ont été beaucoup moins efficaces, et les nouvelles avancées technologiques (l'omniprésence et le caractère plus intrusif de l'informatique ainsi que de la collecte et de l'utilisation des données à caractère personnel; le «profilage»; l'internationalisation omniprésente du traitement de ces données; les contenus Web produits par l'utilisateur; etc.) risquent de rendre plus difficile encore l'application des principes, même sur papier (bien que certaines nouvelles technologies puissent faciliter leur application).

17. Nous présentons ci-après les principaux domaines qui représentent un défi pour la loi européenne de protection des données. Ils seront examinés plus en détail à la Section V (comme indiqué):

- ✓ Certaines affaires ne relèvent pas de la directive ni des lois nationales qui l'appliquent, et ces exclusions seront encore plus problématiques dans le nouvel environnement «Web 2.0».

  Ce point est traité plus en détail (en particulier par référence au document de travail N°2) à la Section V, sous-section V.2.

- ✓ De graves conflits de lois subsistent, même au sein de l'UE/EEE, mais surtout par rapport aux responsables du traitement dans les pays non membres de l'UE/EEE; et ces conflits vont s'intensifier.

  Ce point est traité plus en détail, toujours par référence au document de travail N°2 à la Section V, sous-section V.3.

- ✓ Il existe toujours d'énormes différences au niveau de l'application et de l'interprétation des concepts et règles de base en matière de protection des données, même au sein de l'UE/EEE, et ces différences sont encore plus grandes entre les pays de l'UE/EEE et les autres pays; compte tenu de l'internationalisation du traitement des données, ces différences poseront de plus en plus problème.

  Ces différences sont imputables, d'une part, à la mise en œuvre inadéquate ou lacunaire de la directive par les États membres et, d'autre parte, aux différences au niveau de l'interprétation et de l'application de la directive. Les mécanismes mis en place pour assurer une mise en œuvre complète et plus harmonisée de la directive n'ont pas encore été pleinement exploités. De notre point de vue:

  - La Commission européenne n'a pas suffisamment, ni avec suffisamment de fermeté, poursuivi les États membres qui n'ont pas mis en œuvre la directive de façon adéquate; et

  - Les mécanismes de la directive destinés à accroître l'harmonisation n'ont pas été suffisamment exploités. Dans une certaine mesure, ces procédures sont elles-mêmes insuffisantes et doivent être remaniées.

  Ce point est traité plus en détail, par référence au document de travail N°2 et à une autre étude de la Commission sur le groupe de travail «Article 29»; à la Section V, sous-section V.4.

- ✓ La Commission européenne n'a eu recours à la procédure de publication de «constatations du caractère adéquat de la protection des données» que dans un nombre limité de pays. Au niveau mondial, la procédure a donc eu un impact plus limité que ce que l'on était en droit d'espérer; et l'élaboration de lois strictes en matière de protection des données dans les pays non membres de l'UE/EEE a donc été moins encouragée qu'elle n'aurait pu l'être.

  Ce point est traité plus en détail à la Section V, sous-section V.5.

- ✓ Même dans l'UE/EEE, la mise en application par les autorités nationales chargées de la protection des données (DPA) est souvent insuffisante. À quelques exceptions près (en particulier la Nouvelle-Zélande et, dans une certaine mesure, pour le secteur privé, la Corée du Sud), l'application dans les pays non européens, notamment les États-Unis, est encore moins stricte. Or, elle deviendra encore plus importante et difficile dans le nouvel environnement mondial-technique (bien que, une fois encore, la technologie puisse être utile dans certains cas).

  Ce point est traité plus en détail à la Section V, sous-section V.6, en référence, pour ce qui concerne les pratiques des DPA de l'UE/EEE, à une étude commandée par l'Agence des droits fondamentaux de l'UE et, pour ce qui concerne la mise en application en dehors de l'UE/EEE, aux rapports sur les pays non membres de l'UE/EEE.

- ✓ L'exercice des droits des personnes concernées, soit individuellement soit avec l'aide d'ONG, est souvent difficile et entravé par plusieurs facteurs, en Europe et dans d'autres régions. Toutefois, certains pays non européens, et en particulier les États-Unis, bien qu'ils protègent moins bien les données, permettent des recours spéciaux qui pourraient être utilisés comme exemples pour renforcer le pouvoir des individus de protéger les données qui les concernent dans l'UE/EEE.

  Ce point est traité plus en détail à la Section V, sous-section V.7.

- ✓ Les autres moyens de renforcer la protection des données, et notamment les moyens techniques tels que le cryptage, l'anonymisation, les outils de gestion des identités et autres technologies renforçant (soi-disant) la protection de la vie privée (PET), sont encore très peu développés, souvent peu mis en application et peu efficaces, et trop souvent appliqués d'une façon inappropriée qui les rend inefficaces. Certains d'entre eux ne sont rien de plus que des cache-misère. D'autres (comme l'anonymisation) sont de plus en plus contournées par les avancées technologiques. Et souvent, ils ne résolvent pas les problèmes au bon moment, en particulier au moment de la conception, ou ne sont pas conviviaux. Dans le nouvel environnement technique, nous devrons accorder davantage d'attention à ces mesures et poser sur elles un regard plus critique. Certaines solutions à caractère relativement peu technologique, comme par exemple le fait d'exiger que les paramètres par défaut pour diverses applications offrent une protection efficace de la vie privée ou la délivrance de labels de protection de la vie privée, peuvent contribuer à une protection adéquate.

  Ce point est traité plus en détail à la Section V, sous-section V.8.

18. Toute analyse sérieuse du régime européen de protection des données devra prendre en compte les problèmes susmentionnés, qui sont exacerbés du fait des changements sociaux et techniques qui se profilent à l'horizon (ou auxquels nous sommes déjà confrontés). Les défis se multiplient. Toutefois, comme nous l'avons fait remarquer, ceux-ci concernent essentiellement l'application, l'interprétation et l'efficacité de la mise en application/l'exercice des droits: les principes de base de la protection des données ne sont pas remis en question mais ils doivent être réaffirmés et appliqués de façon plus complète dans la pratique.

- o – O – o -

IV. Impératifs fondamentaux

19. Certaines questions sont à ce point fondamentales qu'elles doivent être prises en compte dans toute révision du régime de protection des données dans l'UE: elles ne peuvent pas être laissées de côté (ou banalisées car «trop légalistes») sans mettre en péril les valeurs constitutionnelles fondamentales de l'Europe. Elles sont donc présentées brièvement ici et prises en compte dans nos conclusions et recommandations spécifiques.

Impératifs sociopolitiques:

20. L'évolution des technologies de l'information et de la communication offre de nombreux avantages mais crée également de nouvelles menaces pour l'individu et pour sa relation avec des organismes puissants (publics et privés). Il ne s'agit pas seulement de menaces pour la vie privée au sens traditionnel du terme (liberté de ne pas faire l'objet d'intrusions et de surveillance) mais aussi de nouvelles menaces pour l'autonomie et les libertés individuelles, notamment les libertés politiques, et pour la société dans son ensemble.

21. Nous nous contenterons de citer la décision de la Cour constitutionnelle allemande, dans son célèbre arrêt de 1983 relatif au recensement:[6]

> Un ordre social et juridique dans lequel le citoyen ne sait plus qui sait quoi et quand à son sujet, ni dans quelle situation, est incompatible avec le droit à l'autodétermination informationnelle. Une personne qui ne sait pas si tous ses comportements inhabituels sont consignés et enregistrés de façon permanente, utilisés ou diffusés, essaiera de ne pas attirer l'attention en adoptant ce type de comportement. Une personne qui suppose, par exemple, que sa participation à une réunion ou à une initiative citoyenne est officiellement enregistrée et qu'elle est donc susceptible de lui occasionner des problèmes, peut décider de renoncer à l'exercice de ses droits fondamentaux ([tels que garantis dans les] articles 8 et 9 de la Constitution). Cela limiterait non seulement les possibilités d'épanouissement personnel de l'individu, mais aussi le bien commun dans la mesure où l'autodétermination est une condition essentielle à l'existence d'une société libre et démocratique qui repose sur les capacités et la solidarité de ses citoyens.

La société que les avancées technologiques mentionnées dans le Document de travail n°1 risquent inconsciemment de faire naître n'est plus la «société libre et démocratique» à laquelle fait allusion cet extrait.

22. Mais les nouvelles technologies entraînent dans leur sillage de nouvelles menaces: face à la multiplication des analyses de plus en plus automatisées de données toujours plus nombreuses et accessibles, les individus risquent d'être réduits à de simples objets, qui seront traités (ou qui pourront même faire l'objet de discrimination) sur la base de «profils» informatiques, de probabilités et de prévisions, sans possibilité de s'opposer aux algorithmes sous-jacents. À défaut de maintenir une protection des données très stricte, les décisions qui ont un «impact significatif» (par exemple, la décision de vous refuser un poste ou de ne pas même vous accorder un entretien d'embauche; d'être arrêté à une frontière et éventuellement de se voir refuser l'entrée dans un pays; d'être soumis à une surveillance intrusive, et éventuellement d'être arrêté, etc.) seront de plus

6 *Volkszählungsurteil*, BVerfGE Bd. 65, S. 1 ff.

en plus souvent motivées «par le fait que l'ordinateur a dit non» (même si les responsables ou le personnel prenant la décision ne peuvent la justifier complètement). Les nouvelles technologies, par nature, ont tendance à modifier l'équilibre du pouvoir, qui n'est plus du côté de l'individu mais bien du côté des personnes qui détiennent les données le concernant: les termes «personne concernée» et «responsable du traitement» prennent une dimension nouvelle, plus grave et plus menaçante. Certaines technologies peuvent être utilisées pour contrer en partie cette tendance mais elles sont beaucoup plus faibles et sont souvent, *par nature*, moins efficaces que ce que l'on veut bien dire ou croire. Si nous ne réussissons pas à maîtriser les nouvelles technologies, leur libre utilisation ébranlera le fondement même de la société démocratique. Et l'outil qui peut nous permettre d'apprivoiser la machine est la protection des données.

Référence: Pour en savoir plus à ce sujet, voir Document de travail n°1 (résumé au point I ci-dessus ainsi qu'à la Section V, sous-section V.8 ci-dessous).

Impératifs constitutionnels-juridiques européens :

23. La protection des données est de plus en plus reconnue dans la jurisprudence de la Cour européenne des Droits de l'Homme, en vertu de l'article 8 de la Convention des Droits de l'Homme, ainsi que dans le droit européen (dans ce dernier cas en particulier, au travers des «principes généraux du droit communautaire», la Charte des droits fondamentaux, et la jurisprudence de la Cour de justice européenne). Les principes et règles de base de la protection des données ont donc désormais bel et bien acquis un statut constitutionnel. Il s'agira de s'en souvenir lors de toute révision des directives européennes relatives à la protection des données. Si une directive révisée devait ne pas respecter ces obligations fondamentales, sa constitutionnalité pourrait être remise en cause et elle pourrait être rejetée à Luxembourg (pour ce qui concerne sa mise en œuvre dans et par les États membres) et à Strasbourg. Toute révision devrait donc avoir pour objectif premier non pas seulement d'éviter ces infractions mais bien de s'assurer que tout nouveau régime européen de protection des données (dans ce qui reste les trois «piliers» de l'UE) satisfait pleinement aux critères européens fondamentaux en matière de Droit de l'Homme.

Référence: Pour en savoir plus à ce sujet, voir Douwe Korff, *Paper No. 4: The Legal Framework*, in: Ian Brown & Douwe Korff, Privacy & Law Enforcement, étude réalisée pour le Commissaire à l'information du Royaume-Uni, 2004 (qui figure parmi les documents accompagnant ce rapport).

24. Dans plusieurs États membres de l'UE, parmi lesquels l'Allemagne, le Danemark et la Grèce, la protection des données est solidement ancrée dans la Constitution. Tout manquement du régime européen de protection des données aux obligations constitutionnelles-légales de ces États membres risque d'entraîner de graves conflits entre ces législations nationales et le droit CE/UE, comme en atteste l'approche *solange* adoptée par la Cour constitutionnelle allemande, réaffirmée récemment par rapport au Traité de Lisbonne. Les extraits ci-après illustrent ces conflits:

Extraits :

Arrêt Stauder de la CJE :
(Affaire 29/69, *Stauder v. Ulm*, [1969], Rec. 419, paras. 3-4)

Le recours aux règles ou concepts juridiques du droit national pour juger de la validité des mesures adoptées par les institutions communautaires serait préjudiciable à l'uniformité et à l'efficacité du droit communautaire. La validité de ces mesures ne peut être jugée qu'au regard du droit communautaire. En réalité, le droit découlant du Traité, qui est une source de droit indépendante, ne peut, par nature, être annulé par des règles du droit national, quelle que soit leur formulation, sans être vidé de son caractère de droit communautaire et sans que ne soit remis en question le fondement juridique de la Communauté elle-même. Par conséquent, **la validité d'une mesure communautaire ou son effet au sein d'un État membre ne peut être affecté par des allégations selon lesquelles elle serait contraire soit aux droits fondamentaux tels que formulés par la Constitution dudit État, soit aux principes d'une structure constitutionnelle nationale.**

Suite au verso

Cf., par contraste :

Décision de la Cour constitutionnelle allemande concernant la constitutionnalité du Traité de Lisbonne :
(Décision de la Cour constitutionnelle allemande [BVerGE], 2BvE 2/08, du 30 juin 2009, para. 240)

Lorsque la protection juridique n'est pas garantie au niveau de l'Union [européenne], la Cour constitutionnelle juge [c'est-à-dire réaffirme pour elle-même le droit de juger - DK] si les actes juridiques des organes et institutions européens restent dans les limites des pouvoirs souverains qui leur ont été conférés ...

Un arrêt important rendu en Roumanie au moment de la préparation du présent rapport montre que les conflits évoqués ci-dessus ne concernent pas uniquement les «anciens» États membres: le 8 octobre 2009, la Cour constitutionnelle roumaine a jugé anticonstitutionnelle une loi qui aurait imposé aux opérateurs de téléphonie mobile et aux fournisseurs d'accès à Internet de stocker les données relatives aux communications pendant six mois.[7] Ladite loi était destinée à la mise en œuvre de la directive européenne relative à la conservation des données (directive 2006/24/CE), et la décision de la Cour indique que les dispositions de cette directive sont contraires aux prescriptions légales nationales-constitutionnelles du pays.

L'exemple décrit ci-dessus montre que, au sein de l'UE, la protection des données est un terrain éminemment favorable à la résurgence du problème *solange*. Il est dès lors impératif que tout régime européen de protection des données révisé (en particulier s'il doit s'appliquer dans tous les domaines actuellement couverts par les trois «piliers») respecte les prescriptions de la CEDH et des Constitutions des États membres (notamment mais pas seulement les prescriptions de la Constitution allemande à cet égard, telle qu'elles ont été édictées par la Cour constitutionnelle de ce pays).

Références: Pour en savoir plus à ce sujet, voir plus particulièrement le *Rapport concernant l'Allemagne*, ainsi que l'analyse comparative dans le Document de travail n°2. Voir aussi para. 43 ci-dessous.

25. De la même manière, dans certains des pays non membres de l'UE/EEE que nous avons étudiés, le fondement constitutionnel de la protection des données est très important.

[7] Voir: http://sofiaecho.com/2009/10/09/797385_romanian-constitutional-court-data-retention-law-unconstitutional.

Cela est particulièrement vrai dans le cas du Japon et à Hong Kong. Toutefois, dans ces pays, la protection des données ne s'est pas encore pleinement développée au sein d'une protection plus générale de la vie privée. En Australie, il n'existe pour ainsi dire pas de fondement constitutionnel pour la protection des données. Dans d'autres pays d'Asie et du Pacifique, la situation est tout aussi mitigée. Dans la région Asie-Pacifique, il n'existe donc pas, à ce stade, d'élément d'harmonisation comparable aux normes européennes en matière de Droits de l'Homme. Aux États-Unis, la protection offerte par la Constitution fédérale se limite essentiellement à restreindre l'accès du Gouvernement aux informations à caractère personnel, et l'utilisation de celles-ci (même dans ce cas, uniquement pour ce qui concerne les citoyens américains), et cette protection était régulièrement balayée par le Premier amendement (mais voir para. 34 ci-dessous pour connaître les derniers développements à ce sujet). Bien que certains États (tels que le New Jersey) aient élargi la protection accordée par leur Constitution, celle-ci reste très éloignée de la situation dans des pays européens tels que l'Allemagne.

Références: Pour en savoir plus à ce sujet, voir les *Rapports par pays* concernant les pays non membres de l'UE susmentionnés.

V. Conclusions et recommandations

1. APPROCHE DE BASE [développement des sections précédentes]

26. Toute révision du régime européen de protection des données doit commencer par la reconnaissance explicite de la nécessité de respecter les prescriptions de la CEDH et de la Charte des droits fondamentaux, ainsi que des Constitutions des États membres.[8] Le respect des impératifs sociopolitiques et juridico-constitutionnels à cet égard (dans tous les domaines couverts par les trois anciens piliers) sera plus crucial encore dans le nouvel environnement sociopolitique et technique mondial.

27. La législation européenne en matière de protection des données (dans tous les domaines couverts par les trois anciens piliers) peut et doit continuer de s'appuyer sur les principes de base de la protection des données - ainsi que sur les critères définis dans la directive 95/46/CE. L'application de ces normes générales doit être clarifiée (comme expliqué ci-dessous, en particulier à la sous-section V.4) mais les normes en elles-mêmes ne nécessitent pas de révision majeure pour faire face aux nouveaux défis. Au contraire, elles reflètent des normes européennes et nationales en matière de droits constitutionnels/de l'Homme du type que nous venons d'évoquer, qui doivent être réaffirmées avec force.

28. Toute révision visant à permettre de relever les nouveaux défis doit être axée sur les questions ci-après (étroitement liées entre elles), qui sont examinées dans les sous-sections indiquées:

- les exclusions problématiques de certains domaines du champ de la directive (V.2);
- la question délicate du «droit applicable» (V.3);
- la nécessité d'une harmonisation beaucoup plus grande (à haut niveau) au sein de l'UE/EEE, par différents moyens y compris le renforcement des mesures de mise en application par la Commission (V.4);
- la nécessité d'un renforcement de la coopération avec les pays non membres de l'UE, et une plus grande reconnaissance des efforts «adéquats» de ces pays (V.5);
- la nécessité d'assurer une plus grande conformité avec la législation existante et une application beaucoup plus stricte de celle-ci par les DPA au niveau national (V.6);
- la nécessité de renforcer les droits et les possibilités de recours pour les particuliers (éventuellement en collaboration avec ou par le biais des ONG compétentes) (V.7); et
- la nécessité de développer les mesures supplémentaires et les mesures alternatives (tout en étant conscients des limites intrinsèques et des restrictions pratiques de ces mesures) (V.8).

[8] Depuis l'entrée en vigueur du Traité de Lisbonne, le 1er décembre 2009, la Charte est devenue juridiquement contraignante. L'article 8 reconnaît un droit autonome à la protection des données à caractère personnel, et l'article 16 du Traité sur le fonctionnement de l'UE prévoit l'adoption, par l'Union et ses États membres, d'un cadre juridique homogène mettant en œuvre ce droit fondamental dans toutes les activités de l'Union. Par ailleurs, le Traité a aboli les trois «piliers» autrefois distincts.

29. Les deuxième et troisième questions en particulier sont étroitement liées dans la mesure où la question cruciale du «droit applicable» (c'est-à-dire faire en sorte qu'un seul droit national facilement identifiable s'applique à toute opération de traitement des données dans l'UE/EEE, et à ce qu'il n'arrive jamais qu'aucun droit ne s'applique) ne peut être réglée que si l'on renforce l'harmonisation au niveau de l'application de la directive. De manière générale, bien entendu, il n'y a guère d'intérêt à mettre en place des règles strictes en matière de protection des données si celles-ci ne s'appliquent pas aux activités importantes ou si elles ne sont pas respectées et appliquées de façon appropriée ou dans leur totalité.

Nos conclusions et recommandations à ce sujet sont présentées ci-dessous.

2. CHAMP D'APPLICATION DES RÈGLES EUROPÉENNES EN MATIÈRE DE PROTECTION DES DONNÉES

(i) Domaines couverts par les anciens premier et troisième piliers:

30. **Constat/conclusion:** Les activités qui, avant l'entrée en vigueur du Traité de Lisbonne, étaient couvertes par les premier et troisième «piliers» de l'UE[9] se confondent de plus en plus, au point qu'il en devient impossible de les distinguer (cf., par exemple, les controverses SWIFT et PNR); en cela, l'abolition des différents piliers est une bonne chose. Par ailleurs, le principe de «propriété permanente» des données de l'ancien troisième pilier est inexploitable en ce sens qu'il suppose qu'un pays d'origine peut réellement garder le contrôle des données transmises à des autorités dans un autre pays. Il est également incompatible avec l'obligation de «disponibilité» (consacrée dans le Traité de Prüm), qui va totalement à l'encontre des principes de protection des données.

31. Nous pensons que le renforcement de la coopération en matière de police et de sécurité doit aller de pair avec la garantie de la protection des données, tant au sein des États membres que dans les institutions européennes dans ce domaine, au plus haut niveau prescrit par la Constitution de n'importe quel État membre, et par la législation européenne en matière de Droits de l'Homme. Si la protection des données n'est pas garantie (comme dans l'ancien premier pilier) au moins à ce niveau, la coopération au sein de l'UE dans les domaines couverts par l'ancien troisième pilier est gravement menacée. L'harmonisation de la protection des données dans le domaine policier doit être fondée sur la recommandation R(87)15 du COE, qui est régulièrement invoquée dans les instruments de l'UE (et du COE) en matière de coopération policière tels que les traités Schengen et Europol (mais sans que l'on ne tienne pleinement compte de ses répercussions, ou que l'on n'adhère à ses principes dans la pratique).

Remarque: Certains pourraient faire valoir que, au-delà de la question du caractère approprié de l'application de la législation européenne dans le droit national, le degré de protection des données offert au niveau national ne relève pas de la législation de la CE ou de l'UE. Toutefois, comme nous l'expliquons aux sous-sections V.3 et V.4, cet argument a déjà montré ses faiblesses dans l'ancien premier pilier en raison du lien étroit qui existe entre l'harmonisation et la question du droit applicable. Si la directive était étendue à l'ancien troisième pilier, ou si des règles similaires aux règles de «droit applicable» actuellement prescrites par la directive étaient appliquées à ce domaine, le

[9] Voir note précédente.

niveau de protection des données policières dans tous les pays de l'UE/EEE deviendrait un problème urgent pour les pays dont la Constitution offre un niveau élevé de protection des données à cet égard. Ceux-ci ne pourraient accepter, dans un contexte aussi sensible, que des lois étrangères non conformes à leur Constitution nationale soient appliquées à leurs citoyens: voir paragraphe 24 ci-dessus. En réalité, le principe de «disponibilité» suscite déjà les mêmes craintes, bien qu'il n'ait pas encore été porté devant les tribunaux.

32. Tout ceci nécessite des règles juridiques strictes qui soient conformes aux obligations européennes en termes de «qualité» de la «législation» telles qu'elles sont définies par la Cour européenne des Droits de l'Homme; des limites à la «disponibilité» et à la conservation des données (y compris les données relatives aux communications et à l'ADN); et des limites strictes à l'utilisation des «profils»; ainsi qu'une protection procédurale stricte, et le libre accès aux tribunaux nationaux et européens pour les personnes affectées par les mesures en question, ainsi qu'une habilitation totale de ces instances à examiner sur le fond toutes les questions liées à chaque affaire.

Référence: Document de travail n°2, section 2, sous-section 2.1.

33. **Recommandation**: Les principes, règles et critères de base en matière de protection des données consacrés dans la directive doivent s'appliquer «de façon uniforme» aux activités appartenant à tous les domaines autrefois couverts par les différents piliers. Cela comprend l'application des exceptions (limitées) pour les activités du troisième pilier énumérées à l'article 13 de la directive. Si nous voulons pouvoir relever les défis, nous devons renforcer l'harmonisation, ou tout au moins le rapprochement, des règles de protection des données qui régissent ces activités dans l'UE, sur la base de la recommandation R(87)15 du COE. Il est également primordial de garantir une protection judiciaire totale dans les tribunaux nationaux, et par le biais de la CEJ, et de reconnaître pleinement le statut des personnes concernées (avec comme garantie la Cour européenne des Droits de l'Homme).

(ii) Exceptions concernant le traitement des données à des fins exclusivement personnelles et la liberté d'expression, en particulier pour ce qui concerne les sites de réseaux sociaux et le «blogage» sur le «Web 2.0»:

34. **Constat/conclusion:** Le contenu généré par les utilisateurs (User-generated content - UCG) va se développer massivement dans le nouvel environnement électronique, en particulier via les réseaux sociaux numériques, le «blogage», le «microblogage» et autres phénomènes similaires: une déferlante d'informations qui ne sont pas encore numérisées va s'abattre sur le nouveau «Web 2.0». Celle-ci pourrait bien être dominée par le contenu généré par les utilisateurs, ou du moins ce contenu sera-t-il aussi important que le contenu généré par les institutions. Les exemptions spéciales de la directive concernant le «traitement à des fins personnelles exclusivement» et la «liberté d'expression» seront très difficiles à appliquer à ce phénomène. Il existe un risque, d'une part, d'exonérer de la loi des activités qui ont un impact direct sur la protection de la vie privée et des données et, d'autre part, d'appliquer des règles «lourdes», conçues pour réglementer (vraisemblablement) des institutions bien organisées, à des actes simples posés par des particuliers dans le cadre de leurs activités quotidiennes. C'est là l'une des critiques formulées par la CJE dans son arrêt Linqvist, qui a appliqué pleinement les dispositions de la directive principale au petit site Internet d'une paroisse locale en Suède.

Il convient de faire remarquer que, dans les pays non membres de l'UE/EEE dont la Constitution protège des droits concurrents tels que la vie privée et la liberté d'expression, les problèmes sont très similaires: la question de l'équilibre entre ces droits est inévitable mais, dans la plupart des pays, elle n'a pas encore été examinée de façon exhaustive. Aux États-Unis, beaucoup avaient le sentiment que le Premier amendement à la Constitution (qui protège la liberté d'expression) l'emportait généralement sur la vie privée, et plusieurs délits civils tels que la diffamation et la «divulgation publique de faits de la vie privée» (délictueuse) ont effectivement été fortement circonscrits au nom du Premier amendement. Toutefois, dernièrement, des lois analogues aux lois relatives à la protection de la vie privée, telles que celles sur la notification des crédits financiers et sur les services financiers, ont survécu au test du Premier amendement: voir le Rapport concernant les États-Unis, sections 1.5 et 1.6. Bien qu'il soit encore trop tôt pour parler d'une convergence entre les approches américaine et européenne, ces faits attestent que les différences commencent à s'estomper.

Références: Document de travail n° 1, section relative aux *Réseaux sociaux et au contenu généré par les utilisateurs* (pp. 11-12); Document de travail n° 2, section 2, sous-section 2.2. Rapport sur les États-Unis, sections 1.5 et 1.6.

35. **Recommandation**: Il devrait être possible d'appliquer les règles de protection des données de façon plus souple aux activités relativement insignifiantes sur l'Internet. Le fait de vouloir soumettre les particuliers qui utilisent normalement l'Internet au plein effet de toutes les règles qui s'appliquent aux «contrôleurs» pose problème. Et nous pensons que la meilleure façon de résoudre ce problème consiste à réglementer les services qu'utilisent ces particuliers: les sites de réseaux sociaux, les sites hébergeant des «blogs», etc. Ces hôtes devraient être obligés à doter leurs sites et leurs services de paramètres par défaut et d'outils respectueux de la vie privée. Les utilisateurs ordinaires qui utilisent ces sites sans modifier les paramètres par défaut devraient pouvoir être sûrs qu'ils n'enfreignent aucune loi sur la protection des données; si les paramètres par défaut ne protègent pas la vie privée et les données à caractère personnel, le site qui a défini ces paramètres doit en assumer la responsabilité principale. Cela laisserait la possibilité d'adopter un régime (ou, s'il existe déjà, de le conserver) de délits et quasi-délits [quasi-délit ou *faute*] en vertu duquel les individus peuvent être tenus pour responsables de divulgation publique abusive ou injustifiée d'informations à caractère privé ou d'«intrusion», sur l'Internet ou via d'autres systèmes de communication omniprésents tels que les SMS ou les MMS. Ces systèmes fonctionnent relativement bien aux États-Unis (sous réserve de l'invocation du Premier amendement, comme expliqué ci-dessus) et sont récemment apparus dans le droit jurisprudentiel en Nouvelle Zélande; en Australie et à Hong Kong, ils sont recommandés par les commissions de réforme du droit. Ces systèmes pourraient être renforcés par la possibilité d'obtenir des injonctions provisoires délivrées par les tribunaux ou des ordonnances délivrées par les autorités chargées de la protection des données, exigeant le retrait des UGC que la personne concernée ou l'autorité en question estime contraires à la loi, décisions qui pourraient être contestées par la personne qui a communiqué ces informations au motif que cette communication ne constitue pas une infraction à la loi. Nous sommes convaincus que, dans de nombreux États membres de l'UE, des solutions de ce type sont déjà possibles (en se fondant en partie sur le droit civil et en partie – en particulier pour ce qui concerne les paramètres par défaut des sites de réseaux sociaux – sur la législation relative à la protection des données).

Références: Rapports concernant l'Australie et Hong Kong, sections 1.7 dans chacun des rapports, et concernant les États-Unis, sections 1.5 et 1.6.

3. DROIT APPLICABLE

36. **Constat/conclusion:** Tous les traitements de données, en ce compris le traitement des données à caractère personnel, s'internationalisent. Ce phénomène est inhérent à l'utilisation de l'Internet, et ne fera que s'amplifier à l'ère de l'«informatique dématérialisée». Par ailleurs, les acteurs de ces traitements se diversifient et sont de plus en plus éparpillés à travers les différents pays, et il est souvent difficile de distinguer leurs tâches et leurs responsabilités. Les conflits de droit vont donc se multiplier, notamment au sein de l'UE/EEE, en raison de l'ambiguïté des règles de «droit applicable» de la directive et des différences au niveau de leur mise en œuvre.

37. De façon plus spécifique, en vertu de la directive principale, les États membres doivent, au sein de l'UE/EEE, appliquer leur législation nationale de protection des données à une opération de traitement de données si «*le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'État membre»;* mais «*si un même responsable du traitement est établi sur le territoire de plusieurs États membres, il doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable»*. (Article 4(1)(a) de la directive principale). En d'autres termes, le choix du droit qui s'applique à une opération spécifique dépend tout d'abord : (i) de l'identité du «responsable du traitement» (qui est souvent difficile à déterminer, et qui le sera plus encore dans le nouvel environnement technique mondial décrit dans le Document de travail n° 1); (ii) du lieu où le responsable est «établi» (et, de manière générale, il est difficile de répondre à la question de l'«établissement» en vertu du droit communautaire); (iii) du «contexte» dans lequel a lieu le traitement; et (iv) du type d'«établissement» du responsable du traitement concerné (qu'il est souvent difficile de définir avec précision) – sans oublier que nous devons encore tenir compte de la deuxième sous-clause concernant les responsables «*établis sur le territoire de plusieurs États membres»*. Les règles de l'article 4(1)(a) sont tout simplement confuses et impossibles à appliquer dans le nouvel environnement technique mondial. Sans surprise, les règles sont appliquées différemment dans les États membres, ce qui donne lieu à des conflits de lois (qui ne sont pas trop graves dans la pratique car, souvent, les lois qui sont en concurrence et en conflit sur papier ne sont pas mises en œuvre dans la pratique).
Référence: D Korff, EC Study on Implementation of Data Protection Directive 95/46/EC, 2002, section 4, «droit applicable», qui conclut (sur la base d'une analyse plus détaillée dans le rapport sur cette étude) que:

> L'on constate (...) de graves problèmes liés à la mise en œuvre de la première disposition principale de la directive, qui stipule que «*Chaque État membre applique [sa législation nationale] aux traitements de données à caractère personnel lorsque (…) le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'État membre»*. Cette disposition n'est pas appliquée pleinement ou de façon appropriée (et surtout, pas de façon cohérente) dans tous les États membres, ce qui donne lieu au type de conflit [de lois] que l'article 4 de la directive prétend précisément empêcher. Cela est en partie imputable à la transposition lacunaire dudit article 4 mais aussi à la complexité excessive de la disposition elle-même».

38. Il est également nécessaire d'examiner de façon plus approfondie l'application de ces règles aux organismes publics, et en particulier aux organismes semi-publics qui sont de plus en plus impliqués dans le traitement de données à caractère personnel dans les États membres, y compris dans des domaines sensibles tels que la santé et la justice pénale.

39. Par ailleurs, les dispositions de la directive relatives au droit applicable sont effectivement impossibles à appliquer aux entreprises et aux organisations de pays tiers qui exercent leurs activités en Europe (en particulier si elles sont actives sur l'Internet – comme elles le sont, ou le seront, certainement presque toutes). À première vue, elles obligent souvent ces entreprises et organisations à se conformer simultanément à toutes les lois relatives à la protection des données, dans les 27 États membres - ce qui est évidemment impossible compte tenu des différences majeures qui subsistent entre les lois et de la difficulté à définir les obligations de chacune d'entre elles concernant le traitement des données sur l'Internet par des entreprises établies en dehors de l'UE/EEE.

40. Les règles relatives au «droit applicable» concernant les pays qui ne sont pas membres de l'UE/EEE et qui offrent une protection des données «adéquate» ne sont pas claires non plus.[10] La directive ne précise pas si, aux fins du «droit applicable», ils doivent être traités de la même façon que les pays membres de l'UE/EEE, ou comme des pays non membres de l'UE/EEE.

41. Dans les pays tiers étudiés (qui sont tous «*in*adéquats» en termes européens), la question du «droit applicable» est considérée comme relevant du champ d'application extraterritorial de la législation nationale relative à la protection des données. Cette question n'a pas encore trouvé de réponse dans certains territoires mais elle fait l'objet d'une disposition spécifique dans la législation australienne, bien que le champ d'application de cette disposition soit également ouvert à diverses interprétations.

Référence: Rapport concernant l'Australie, section 2.5

42. Tous ces problèmes sont graves et constituent un obstacle pour les entreprises et les organisations actives au niveau international en ce sens qu'il est de plus en plus difficile pour elles de se conformer aux règles et principes relatifs à la protection des données. Ces problèmes sont décuplés dans le nouvel environnement sociotechnique internationalisé, et surtout (mais pas seulement) pour ce qui concerne l'Internet.

Référence: Document de travail n° 2, section 3.

43. Une autre question cruciale est celle du lien entre les règles de «droit applicable» et l'harmonisation, à la lumière des dispositions nationales-constitutionnelles de plusieurs États membres (comme mentionné au paragraphe 24 ci-dessus). Il est évident que, en vertu des règles de «droit applicable», il arrivera que le traitement dans un État membre, concernant des personnes se trouvant dans cet État membre, soit déjà soumis (et cela se produira souvent dans le nouvel environnement sociotechnique mondial) à la législation d'un autre État membre en matière de protection des données. Toutefois, si la législation «étrangère» applicable ne satisfait pas aux dispositions constitutionnelles de l'État dans lequel se trouvent ces personnes, cela soulèvera d'autres problèmes du type *solange*: il y a fort à parier que la Cour constitutionnelle de l'État en question refuse d'appliquer la

[10] La question du recours aux constatations du caractère «adéquat» en tant que telles est examinée à la sous-section V.8 ci-dessous.

législation étrangère dans la mesure où elle n'est pas conforme aux dispositions de l'État en question, même si cela revient, en réalité, à refuser d'appliquer les règles européennes du «droit applicable». En d'autres termes, dans un domaine aussi sensible d'un point de vue constitutionnel que le traitement des données à caractère personnel, les règles de «droit applicable» qui contournent les lois d'un État dont les citoyens font l'objet du traitement ne sont acceptables que si elles sont assorties de règles garantissant que toutes les règles nationales, dans tous les États membres, sont conformes aux dispositions les plus strictes de la Constitution nationale de tout État membre.

44. **Recommandation:** Il est absolument indispensable d'améliorer, de clarifier et de préciser les règles relatives au droit applicable. Nous proposons quelques pistes à suivre pour améliorer ces règles:

– Au sein de l'UE/EEE, les règles devraient, à notre avis, être simplement fondées sur le principe du «pays d'origine», comme cela devait être initialement le cas. Cela ne permettra peut-être pas de résoudre tous les problèmes, et nous sommes également conscients que les questions telles que celle de l'«établissement» sont complexes dans le cadre d'une CE élargie. Mais cela permettrait au moins de limiter les problèmes et de les synchroniser dans différents contextes du droit communautaire. Toutefois, comme nous l'expliquons au paragraphe 43 ci-dessus, pour ce faire, il est essentiel d'assurer une plus grande harmonisation, ou du moins un rapprochement à haut niveau, entre les législations des États membres. À l'heure actuelle, cette harmonisation est encore inexistante dans de nombreux aspects cruciaux: voir sous-section V.4 ci-dessous, au point A. Les outils de base dont nous avons besoin pour renforcer (ou du moins encourager) l'harmonisation (notamment le groupe de travail «Article 29») existent mais ils ne sont pas utilisés de façon efficace et doivent être consolidés (voir sous-section V.4 ci-dessous, au point B).

– Les entreprises qui n'appartiennent pas à l'UE/EEE, etc. et qui sont présentes (c'est-à-dire qui sont «établies») dans l'UE/EEE devraient pouvoir se conformer uniquement à la législation du pays UE/EEE où se situe leur principal établissement (leur QG européen) et, sinon, devraient être traitées comme des entreprises UE/EEE (à condition qu'elles se conforment également aux règles de l'UE/EEE relatives au transfert de données vers des pays tiers n'offrant pas de protection adéquate, et qu'elles traitent donc les données à caractère personnel transmises à leur QG [international] dans le pays tiers en conformité avec la législation de l'UE/EEE relative à la protection des données).

Remarque: Ceci est conforme aux dispositions générales du droit communautaire, en vertu desquelles les entreprises non européennes qui sont établies dans l'UE sont traitées comme des entreprises européennes.

– Les règles relatives au «droit applicable» concernant les entreprises qui n'appartiennent pas à l'UE/EEE, etc. et qui ne sont pas présentes dans l'UE/EEE mais qui utilisent des «moyens» dans l'UE/EEE (généralement des entreprises qui n'appartiennent pas à l'UE/EEE et qui offrent leurs produits ou services sur l'Internet à des citoyens et entreprises appartenant à l'UE/EEE, sans avoir d'établissement dans l'UE/EEE) devraient être simplifiées de manière à ce qu'elles puissent, elles aussi, ne se conformer qu'à la loi d'un seul pays membre (pertinent) de l'UE/EEE. Il pourrait être envisagé de rendre ce choix de législation possible dans le cadre des règles d'entreprise contraignantes; le caractère approprié du choix de législation serait l'un des éléments à

prendre en compte pour juger du caractère adéquat et approprié des règles d'entreprise contraignantes.

– Sous réserve de la première remarque, ci-dessous, les entreprises qui n'appartiennent pas à l'UE/EEE, etc. et qui sont soumises à une législation offrant une protection «adéquate» dans leur pays (selon ce qui aura été déterminé par la Commission) devraient être traitées de la même façon que les entreprises qui appartiennent à l'UE/EEE, c'est-à-dire qu'elles devraient pouvoir ne se conformer qu'à leur propre législation («adéquate») – à condition que les États concernés se conforment également aux mesures prises dans l'UE/EEE pour garantir une application harmonisée/comparable de la législation (encore une fois, comme nous le verrons plus en détail à la sous-section V.4 ci-dessous).

Remarques:

(1) Pour cette dernière suggestion, il sera peut-être nécessaire de laisser s'exprimer les pays tiers concernés, par exemple en leur accordant l'adhésion complète ou partielle au WP29 ou le statut d'observateur de ce groupe, et de procéder régulièrement à des évaluations afin de s'assurer qu'ils continuent d'offrir une protection «adéquate».

(2) Par ailleurs, n'oublions pas qu'il est possible que des pays non membres de l'UE/EEE deviennent parties à la Convention n°108 du Conseil de l'Europe et à son protocole additionnel. Cela serait particulièrement intéressant s'il pouvait être décidé que les États qui sont parties à cette Convention et à son Protocole seront considérés *ipso facto* comme offrant une protection «adéquate». Il reste toutefois des problèmes à résoudre à cet égard.

(3) Dans la dernière suggestion, il est également supposé que les lois «adéquates» s'appliquent de façon extraterritoriale aux entreprises concernées qui n'appartiennent pas à l'UE/EEE, en particulier pour ce qui concerne leurs opérations dans l'UE/EEE. Or, ce n'est pas toujours une réalité, si le cas de l'Australie (l'effet extraterritorial est limité aux données concernant les ressortissants australiens) est courant. En revanche, l'exemple du Japon (l'effet extraterritorial s'applique à toute entreprise présente au Japon) répondra à ce critère. Bien entendu, cela sert uniquement à mettre en évidence des problèmes complexes dans ce domaine. C'est certainement une question dont la Commission (et le WP29) devra tenir compte lorsqu'elle examinera les législations des pays non membres de l'UE/EEE.

Références: Rapports concernant l'Australie et le Japon, section 2.5 dans chaque document.

Nous sommes conscients que ces questions sont éminemment complexes, et nos suggestions sont simplement destinées à susciter le débat. Nous sommes toutefois convaincus que c'est là un problème crucial: il est impossible de comprendre ou d'appliquer totalement les règles de «droit applicable» actuelles. Dans ce contexte de mondialisation effrénée, où l'informatique est désormais dématérialisée, il est indispensable et urgent de clarifier (et de simplifier) ces règles.

4. HARMONISATION DU DROIT SUBSTANTIEL

45. Dans cette sous-section, nous commencerons par présenter brièvement, au point A (paragraphes 47 à 78), nos constatations et conclusions concernant les principaux domaines dans lesquels l'harmonisation demeure déficiente, même au sein de l'UE/EEE. Nous expliquerons ensuite brièvement, au point B (paragraphe 79 à 88) que la situation n'est pas beaucoup plus claire dans les pays non membres de l'UE/EEE. Enfin, au point C (paragraphes 89 à 96), nous formulerons des recommandations sur les

différentes façons de parvenir à cette harmonisation dans tous ces domaines (ainsi que dans d'autres). Nous tenons à rappeler que les résumés ne se veulent en aucun cas exhaustifs et qu'ils visent avant tout à montrer que des divergences majeures subsistent, tant au sein de l'UE/EEE qu'entre les pays membres de l'UE/EEE et les pays tiers, divergences qui doivent être résolues si nous voulons garantir une protection des données appropriée dans le nouvel environnement technique mondial.

Remarque: Cette sous-section doit nécessairement être brève et ne peut donc rendre compte des complexités du sujet. C'est pourquoi nous vous renvoyons aux parties plus détaillées de la section 4 du Document de travail n° 2. Pour obtenir des informations plus complètes, voir la Comparative Summary of National Laws, rédigée en 2002 pour la Commission par Douwe Korff et publiée par la Commission en 2003.[11] Voir aussi le tableau comparatif annexé au présent rapport.

46. Avant d'aborder les différents sujets, il convient de faire remarquer que, dans une certaine mesure, il pourrait être avancé qu'un régime de «droit applicable» simple pourrait aussi contribuer à réduire les nombreuses et importantes divergences: il permettrait aux pays de faire ce qu'ils veulent, jusqu'à un certain point. Toutefois, comme nous l'expliquons à la Section IV, paragraphe 24, et ci-dessus, au paragraphe 43, cela ne tarderait pas, du moins dans l'UE/EEE, à entraîner des conflits entre les dispositions nationales-constitutionnelles et la législation européenne, faisant ainsi resurgir les problèmes *solange*. En outre, ni l'UE ni les États membres ne pourraient considérer comme «adéquates» des législations non européennes très divergentes. Nous pensons donc qu'il est indispensable de «rapprocher» les législations nationales, à un niveau qui respecterait au moins les prescriptions des Constitutions les plus exigeantes (y compris, mais pas seulement, l'Allemagne) et de la CEDH. Nous sommes convaincus que, à défaut de pareil rapprochement, des problèmes majeurs se poseront au niveau des législations nationales et européenne en matière de Droits de l'Homme, ainsi que du point de vue de la validité et de la suprématie du droit de la CE/l'UE. L'harmonisation, du moins au sein de l'UE/EEE, est primordiale si nous voulons pouvoir faire face aux nouveaux défis. Nos conclusions concernant le manque d'harmonisation sont donc très sérieuses: ce problème devra être traité en priorité dans toute révision du régime de protection des données de l'UE/EEE.

A. (NON-) HARMONISATION AU SEIN DE L'UE/EEE

(i) Concepts et définitions de base (Article 2 de la directive)

47. **Constat/conclusion:** Les définitions de nombreux concepts de base mentionnés dans la directive laissent sans réponse de nombreuses questions cruciales.[12] Ainsi, par

[11] Douwe Korff, Study on Implementation of Data Protection Directive 95/46/CE - Comparative Summary of National Laws, 2003, consultable à l'adresse http://ec.europa.eu/justice_home/fsj/privacy/studies/index_en.htm. À certains égards, le résumé de 2003 est aujourd'hui quelque peu dépassé. Nous avons, le cas échéant, mis à jour certaines parties du Document de travail n° 2 à la lumière des informations communiquées par les experts participant à cette étude. Dans ce Document de travail, nous nous sommes également penchés sur une question spécifique, qui touche à de nombreux aspects de la protection des données, qui est essentielle pour le nouvel environnement mais qui n'est pas examinée en détail ici: le «profilage».

[12] Outre les concepts mentionnés dans le texte, il convient également de faire remarquer que les types de fichiers manuels «non structurés» que recouvre et ne recouvre pas le concept de «fichiers de données à caractère personnel» ne sont pas clairement définis. Toutefois, sauf dans des cas très spécifiques, cela revêt une moindre importance à l'ère numérique. La question de ce qui constitue un consentement (valable) est examinée au

exemple, pour ce qui concerne les concepts de «données à caractère personnel» et de «personne concernée», d'importantes questions subsistent quant à l'anonymisation et la pseudonymisation, la ré-identifiabilité, les données concernant des «choses» qui sont liées à des personnes (comme les adresses IP et les données relatives au trafic et à la localisation), et le «profilage». Les législations et pratiques nationales répondent toujours très différemment à ces questions. Bien que le WP29, dans son Avis sur le concept des données à caractère personnel[13], donne de précieuses indications à ce sujet, nous craignons que ces questions ne soient toujours pas traitées de façon appropriée aux niveaux européen et national, et qu'elles ne tiennent aucun compte des problèmes graves liés à la ré-identification, qui sont bien connus (du moins des experts informatiques) depuis plusieurs années.[14] Les problèmes résultant de la quasi-impossibilité de rendre les données à caractère personnel totalement anonymes dans le nouvel environnement sociotechnique constituent l'un des plus grands défis en matière de protection des données, et doivent être au cœur de tout débat sur une révision du régime européen de protection des données.

48. En outre, à certains égards, les définitions mêmes des termes «responsable du traitement» et «sous-traitant» (et donc de «tiers» et de «destinataire») dans la directive principale prêtent à confusion et, dans la pratique, il est souvent difficile de distinguer clairement le responsable du traitement du sous-traitant (ou un tiers ou un destinataire non tiers), en particulier dans les organisations internationales complexes telles que les entreprises ou groupes d'entreprises multinationaux. En outre, les législations des États membres divergent aussi sur ces points. Ce problème prendra, lui aussi, une dimension nouvelle dans le nouvel environnement technique mondial très complexe; il a d'importantes répercussions, en particulier en termes de «droit applicable» (et pourtant, dans ce domaine, les directives sont beaucoup moins claires et la confusion demeure[15]).

Référence: Document de travail n° 2, section 4.1.

(ii) Les principes de la protection des données (article 6 de la directive)

49. **Constat/conclusion:** Les principes de la protection des données sont spécifiés dans les législations de tous les États membres, dans des termes identiques à, ou proches de ceux utilisés dans la directive, à quelques rares exceptions près. Toutefois, certaines législations utilisent des termes quelque peu différents. Ainsi, l'une d'entre elles définit les critères de protection des données (examinés ci-dessous, au point iii) au milieu des principes; une autre ajoute d'autres principes. En outre, certains pays précisent ou mettent en évidence les principes, parfois de manière à les renforcer mais parfois dans le sens contraire.

---

paragraphe iii ci-dessous.

[13] Avis 4/2007 sur le concept de données à caractère personnel du 20 juin 2007 (WP136), examiné en détail dans le Document de travail n° 2, section 4.1.

[14] Voir, en particulier, le document majeur (destiné aux profanes en informatique) de Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, Colorado Law, Legal Studies Research Paper Series, Working Paper Number 09-12, 13 août 2009, consultable en ligne à l'adresse: http://ssrn.com/abstract=1450006. Des commentaires sur ce document ont été ajoutés au Document de travail n° 2.

[15] Les problèmes liés à l'identification, dans certains cas complexes, du responsable du traitement et du sous-traitant, ont été soulevés à la conférence des autorités chargées de la protection des données qui s'est tenue à Barcelone en janvier 2009. Il a été proposé d'accepter que, dans certains cas, leurs rôles et responsabilités respectifs soient amalgamés ou partagés. Toutefois, il n'a pas été tenu compte des répercussions ni des complications qu'une telle approche entraînerait pour la question du «droit applicable».

50. Dans la législation de la plupart des États membres, le principe de spécification et de limitation de la finalité est défini dans des termes identiques ou très semblables à ceux utilisés dans la directive. Toutefois, en dépit de la similitude au niveau de la formulation, l'imprécision du principe laisse la place à des divergences sur le plan de l'application, et les États membres appliquent différents tests à cet égard, qu'il s'agisse des «attentes raisonnables» de la personne concernée, de l'«impartialité» ou encore de tests d'«équilibre». Dans quelques pays, le principe est assorti d'un nombre considérable d'exemptions, en particulier pour les responsables du traitement appartenant au secteur public. Dans d'autres, les finalités sont parfois définies dans des termes beaucoup trop généraux, nuisant ainsi au principe en lui-même. Par exemple, la législation britannique parle de «finalités policières» de façon globale (et autorise donc l'utilisation des données obtenues à une fin policière pour toute autre fin policière), tandis que la législation allemande établit une distinction très nette entre «réaction à des menaces immédiates», «prévention générale et spécifique», et «investigation et poursuite des infractions pénales [présumées]».[16] La législation britannique relative à la protection des données, enfreignant plus ouvertement encore la directive, ajoute la «recherche médicale» à la liste des finalités médicales définies à l'article 8(3) de la directive, contournant ainsi la limitation des finalités à cet égard (à l'encontre des directives du WP29, très claires à ce sujet).[17]

51. Des différences considérables sont également observées dans les règles relatives au traitement secondaire des données à caractère personnel non sensibles à des fins de recherche sans le consentement des personnes concernées. Certains États membres ne prévoient aucune mesure de protection (enfreignant ainsi la directive de façon manifeste); d'autres prévoient des garanties minimales (c'est-à-dire insuffisantes) (par exemple, ils décrètent que les données ne peuvent pas être utilisées pour prendre des décisions au sujet des personnes concernées, ou qu'elles ne peuvent être utilisées que pour la recherche en question); d'autres encore prévoient des tests d'«équilibre» plutôt abstraits ou se contentent de stipuler que la recherche doit être fondée sur un «plan de recherche approprié». D'autre part, la législation de certains États membres contient des dispositions détaillées qui limitent les données et leur traitement, et qui stipulent que la recherche doit être approuvée par un «comité d'éthique» universitaire, ou exigent que les chercheurs demandent une autorisation spéciale à l'autorité chargée de la protection des données, qui définira les différentes conditions (il est également possible que ces conditions complémentaires soient déjà définies dans la législation).

Référence: Document de travail n° 2, section 4.2.

(iii) Les critères de protection des données (article 7 de la directive)

Traitement en vertu d'une autorisation légale[18]

[16] Voir Douwe Korff, The feasibility of a seamless system of protection des données rules for the European Union, étude réalisée pour la Commission européenne (1996 – 97, publiée en 1999).

[17] Voir le «Document de travail sur le traitement des données à caractère personnel, relatives à la santé, contenues dans les dossiers médicaux électroniques (DME)» du WP29, WP131 du 15 février 2007. Remarque: les conséquences de la définition lacunaire des finalités dans les règles juridiques et de la demande du «consentement» pour le traitement de données à des fins mal définies, sont examinées au point iv. Les nombreux aspects liés à la nécessité d'une définition stricte des finalités suffisent à démontrer l'importance de la clarification et de l'harmonisation à cet égard.

[18] Dans ce cas précis, cette expression recouvre les deux critères mentionnés aux paras. (c) et (e) de l'article 7 de la directive, à savoir: «le traitement [qui] est nécessaire au respect d'une obligation légale à laquelle le

52. **Constat/conclusion:** De nombreuses législations nationales reprennent les critères relatifs aux obligations, aux missions et aux pouvoirs légaux dans des termes identiques ou très semblables à ceux utilisés dans la directive. Il convient ici de faire deux remarques générales fondamentales. Tout d'abord, ces critères se rapportent généralement au traitement en vertu de l'une ou l'autre forme d'autorisation légale:[19] Selon les termes de la CEDH, ils se rapportent au traitement des données à caractère personnel (ce qui, aux termes de la Convention, constitue *ipso facto* une «ingérence» dans la vie privée) qui est prévu par la «loi». Deuxièmement, les critères contiennent l'autre mot clé utilisé à l'article 8 de la CEDH, le terme «nécessaire». Cela signifie que les règles juridiques sur lesquelles est fondé le traitement doivent satisfaire aux conditions de «loi» et de «nécessité» (en ce compris la spécificité et la proportionnalité) expliquées en détail par la Cour européenne des Droits de l'Homme dans sa longue jurisprudence.[20] Ces dernières années, la Cour européenne des Droits de l'Homme a, à plusieurs occasions, estimé que les législations nationales autorisant le traitement des données à caractère personnel ne respectaient pas ces obligations de qualité. Ces affaires ont également soulevé des doutes quant à la précision des termes utilisés pour définir la(les) finalité(s) pour laquelle(lesquelles) les données à caractère personnel sont traitées.[21]

53. Il est évident que, dans plusieurs États membres, les règles juridiques invoquées pour autoriser le traitement (et le partage, ainsi que l'«extraction de données») des données à

---

responsable du traitement est soumis» et le «traitement [qui] est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées». Plus particulièrement, nous remarquons que les «obligations légales» auxquelles fait référence l'article 7(c) ne sont pas celles qui résultent d'une situation contractuelle ou précontractuelle puisque celles-ci sont couvertes par l'article 7(b); et que les «missions» et l'«autorité» auxquelles il est fait référence à l'article 7(e) seront des missions et des pouvoirs conférés par la loi.

19 Voir la note précédente.

20 Pour en savoir plus à ce sujet, voir Douwe Korff, *Paper No. 4: The Legal Framework*, in: Ian Brown & Douwe Korff, Privacy & Law Enforcement, étude réalisée pour le Commissaire à l'information, 2004, consultable sur le site UK ICO: http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/legal_framework.pdf. Pour connaître les prescriptions de la CEDH concernant la «loi», le «but légitime» (finalité), la «nécessité», etc., voir pp. 9 à 15. Le document donne ensuite un résumé détaillé de plusieurs affaires portées devant la Cour européenne des Droits de l'Homme, à savoir Amann c. Suisse (arrêt du 16 février 2000) et Rotaru c. Roumanie (arrêt du 4 mai 2000), et un résumé plus concis d'affaires antérieures, à savoir Leander c. Suède (26 mars 1987), Gaskin c. Royaume-Uni (arrêt du 7 juillet 1989), Peck c. Royaume-Uni (28 janvier 2003), et d'autres affaires (pp. 16 à 33); ainsi que d'affaires portées devant la Cour de justice européenne, à savoir Österreichischer Rundfunk c. Autriche (affaires jointes C-465/00 (Rechnungshof c. ÖRF et al.), C-138/01 et C-139/01 (respectivement, Christa Neukomm et Lauermann c. ÖRF) (respectivement les demandes de décision préjudicielle du Verfassungsgerichtshof et de l'Oberster Gerichtshof autrichiens), conclusions de l'Avocat général Tizzano du 14 novembre 2002; l'arrêt du 20 mai 2003) et l'affaire Lindqvist c. Suède (affaire C-101/01 Bodil Lindqvist c. Åklagarkammaren i Jönköping (demande de décision préjudicielle du Göta Hovrätt), Conclusions de l'Avocat général Tizzano du 19 septembre 2002; arrêt du 6 novembre 2003) (pp. 33 à 44). Pour un aperçu plus concis, voir Douwe Korff, The need to apply UK data protection law in accordance with European law, Data Protection Law & Practice, mai 2008. La note suivante renvoie à d'autres affaires, plus récentes, de la Cour européenne des Droits de l'Homme. Elles confirment l'approche adoptée par la Cour de Strasbourg dans les affaires susmentionnées, et renforcent davantage encore la jurisprudence. Un autre arrêt majeur, rendu après l'étude de l'ICO de 2004, est l'arrêt I. c. Finlande (arrêt du 17 juillet 2008): cette affaire a eu d'importantes répercussions sur le traitement des données relatives à la santé dans les dossiers électroniques des patients en Europe.

21 Voir, par exemple, Copland c. Royaume-Uni, arrêt de la Cour européenne des Droits de l'Homme du 3 avril 2007; S. & Marper c. Royaume-Uni, arrêt de la Cour européenne des Droits de l'Homme du 4 décembre 2008 (qui confirment toutes deux la jurisprudence antérieure).

caractère personnel, en particulier dans les secteurs public et quasi-public, ne sont pas conformes à ces normes. Des problèmes surgiront immanquablement au niveau strictement national mais aussi (ce qui nous intéresse davantage dans la présente étude) par rapport aux autres États et par rapport à la CE/UE, si ces lois déficientes viennent à être appliquées au niveau extraterritorial en raison des règles de «droit applicable». Il ne fait aucun de doute que ces situations seront beaucoup plus fréquentes dans le nouvel environnement internationalisé, dans lequel le traitement des données sera de plus en plus régi par les législations nationales d'autres pays plutôt que par celle du pays où réside la personne concernée (ou de l'endroit où celle-ci se trouve au moment de la communication des données).

Référence: Document de travail n° 2, section 4.3 (sous ce titre).

Traitement fondé sur le consentement

54. **Constat/conclusion:** Du point de vue de l'«autodétermination informationnelle», le traitement fondé sur le consentement revêt clairement une importance cruciale mais *à condition* que (comme stipulé à l'article 7(a) de la directive) ce consentement soit «libre, spécifique et éclairé». Toutefois, bien que cette question soit cruciale, elle n'est pas traitée de façon uniforme dans les États membres. Ainsi, plusieurs législations mettent en avant la nécessité que le consentement soit *manifestement* libre, spécifique et éclairé, etc., en incluant le terme «non équivoque» dans la définition même du consentement (Espagne, Portugal, Suède); la législation luxembourgeoise va même jusqu'à inclure dans sa définition les termes «sans équivoque» et «explicite». En Allemagne et en Italie, la législation stipule que le consentement doit (en principe) être donné par écrit (bien qu'elle permette que le consentement soit donné sur l'Internet par un simple «clic de souris»). En revanche, selon les directives de l'autorité britannique chargée de la protection des données concernant la législation, le consentement pour le traitement de données non sensibles peut souvent être implicite.

55. En Allemagne, une demande de consentement pour une finalité autre que la finalité première doit être spécifiquement notifiée par écrit, etc. – mais la législation de ce pays (ainsi que d'autres) n'établit pas clairement si le consentement d'une personne à ce traitement secondaire, qui n'est pas nécessaire pour la finalité première d'un accord, peut être posé comme condition à la conclusion du premier accord: ceci était légal dans la loi britannique précédente, sauf en cas d'abus, mais l'autorité irlandaise chargée de la protection des données est plus stricte à cet égard.

56. Ces divergences seront encore plus problématiques dans le nouvel environnement internationalisé, et notamment sur l'Internet. Le «consentement» obtenu en vertu de la législation d'un pays (le «droit applicable» au moment où les données sont collectées) et valable en vertu de cette législation, pourrait être considéré comme insuffisant et non valable dans le cadre d'un traitement ultérieur dans un autre pays (même s'il s'agit d'un autre État membre de l'UE/EEE), par exemple parce que (de l'avis du deuxième pays) le consentement initial n'était pas suffisamment spécifique ou a été obtenu sous ce que le deuxième pays considère comme une contrainte, etc.

57. Tout cela sans même tenir compte des questions fondamentales, plus générales, de la validité du consentement obtenu par le biais de déclarations de confidentialité en ligne, écrites en petits caractères et que personne ne lit (à l'exception des militants en faveur de la protection de la vie privée ou des avocats). Nous nous contenterons de faire

remarquer tout d'abord que, une fois encore, les États membres n'ont pas tous la même approche de ce type de «consentement» et que, jusqu'à présent, le WP29 n'a donné aucune directive claire à ce sujet; par ailleurs, cette question touche souvent à des questions juridiques plus larges, telles que la protection des consommateurs, l'impossibilité d'appliquer certaines conditions de vente standard, la concurrence déloyale, etc.

Référence: Document de travail n° 2, section 4.3 (sous ce titre). Ce document contient également des références concernant l'obtention du consentement de mineurs, et concernant les directives du WP29 sur le consentement dans le cadre des flux transfrontières de données, de l'emploi, des écoles et des soins médicaux.

Traitement fondé sur le critère d'«équilibre»

58. **Constat/conclusion:** Le critère d'«équilibre» (article 7(f) de la directive) est, par nature, le critère le plus flou et le plus ouvert, et probablement celui qui a le plus grand besoin d'être clarifié quant à la façon dont il peut et doit être appliqué dans des contextes spécifiques. Ce critère est reconnu dans la législation de plusieurs pays (Belgique, Irlande, Royaume-Uni), qui envisagent de mettre en place de nouvelles règles sur l'application du critère d'«équilibre» dans des contextes spécifiques. Toutefois, fait étonnant, aucun d'entre eux n'a effectivement mis en place de dispositions plus précises.

59. Dans l'ensemble, il existe également des différences non négligeables dans la façon dont ce critère est appréhendé dans les États membres. Au Royaume-Uni, la décision de traiter ou non les données non sensibles sur cette base revient essentiellement aux responsables du traitement. En Allemagne, un test d'«équilibre» dans des termes généraux analogues à ceux utilisés dans la directive est appliqué, uniquement dans le secteur privé. Des tests relativement similaires, mais formulés avec plus de précision, sont appliqués dans le secteur public mais ceux-ci, en réalité, s'apparentent davantage à des tests de «nécessité». Les autres pays appliquent généralement un test plus strict ou imposent des formes substantielles strictes au traitement effectué sur la base de ce critère. Ainsi, en Grèce, la législation fait fortement pencher la balance en faveur de la personne concernée en autorisant le traitement uniquement si celui-ci «est *absolument* nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées et à condition que ledit intérêt légitime prévale *manifestement* sur les droits et intérêts des [personnes concernées] et que leurs libertés fondamentales n'en soient pas affectées».

60. En Italie, le test d'«équilibre» ne s'applique que dans les cas spécifiés par l'autorité chargée de la protection des données tandis que, dans la législation finlandaise, les responsables du traitement doivent obtenir une autorisation de l'autorité s'ils souhaitent recourir à ce test (mais la législation contient également quatre dispositions spéciales qui autorisent le traitement dans certains cas, par exemple dans le cadre d'une relation clientèle, qui peuvent être considérés comme des exemples spécifiques de l'application de ce test).

61. Encore une fois, ces divergences peuvent poser problème dans le nouvel environnement internationalisé si les données sont obtenues sur la base de ce critère dans un État membre, puis transférées vers un autre dans lequel le critère est appliqué de façon plus restrictive - ou si un responsable se trouvant dans un pays qui applique ce critère de

façon relativement laxiste tente d'obtenir des données directement auprès des personnes concernées (par exemple, sur l'Internet ou par téléphone) sur cette base, en vertu de la législation nationale du pays où il se trouve (qui serait normalement le «droit applicable») alors que les personnes concernées se trouvent en réalité dans un autre État membre dont la législation est plus stricte à cet égard.

Référence: Document de travail n° 2 (version étendue), section 4.3 (sous ce titre).

(iv) Traitement de données sensibles

62. **Remarque préliminaire:** Le traitement des données sensibles est appelé à se généraliser, et il sera encore plus difficile à maîtriser dans le nouvel environnement technique mondial: les images et les clips vidéo téléchargés sur les sites des réseaux sociaux ainsi que les commentaires postés sur les «blogs» et sur les «plates-formes de microblogage», «révèlent» tous, en toute banalité, des informations sensibles telles que l'appartenance à une ethnie, une orientation sexuelle ou des convictions religieuses (voire même des affaires criminelles). Et toutes ces informations sont beaucoup trop facilement diffusées à un grand nombre de personnes, même au-delà des frontières nationales. Comme nous l'avons déjà fait remarquer, la seule détermination du «droit applicable» dans ce type de traitement relève du défi. Les conflits de lois sont donc particulièrement problématiques à cet égard.

63. **Constat/conclusion:** Certains États membres étendent les conditions spéciales (techniquement, dans la directive et dans les législations des États membres, les exceptions à une interdiction de principe du traitement de ces données) à certaines données qui ne sont pas visées par la directive. Cela concerne les données relatives aux créances, à la situation financière et au paiement des prestations de sécurité sociale en particulier. Certains États inscrivent également dans la liste générale des données sensibles les données relatives aux condamnations pénales, etc. - ce qui signifie que ces données peuvent être traitées sur la base des mêmes exceptions (critères spéciaux) que les autres données sensibles (et notamment aussi sur la base du consentement, qui n'est pas mentionné à l'article 8(5) de la directive).

64. À part cela, nous nous contenterons d'exposer les règles relatives au traitement des données sensibles dans certains contextes spécifiques:

Emploi: Bien que plusieurs États membres aient incorporé dans leur législation des dispositions générales relatives au traitement des données sensibles afin de se conformer à la législation du travail, en accord avec la directive, celles-ci ne sont pas très détaillées. Certains envisagent d'adopter des règles spéciales (ou une loi spéciale) mais, dans la plupart d'entre eux, cela n'a pas encore été fait. Dans l'ensemble, de nombreux États ont mis en place des dispositions séparées (très divergentes) dans d'autres législations que celle relative à la protection des données mettant en œuvre la directive, et la législation relative à la protection des données, ou les règles plus spécifiques élaborées dans le cadre de cette législation, ne donnent pas beaucoup d'indications à cet égard.[22]

[22] Ceci est également corroboré par une récente étude commandée par l'Agence des droits fondamentaux de l'UE: voir la synthèse du projet final de Comparative Legal Study on assessment of protection des données measures and relevant institutions, rapport commandé par l'Agence des droits fondamentaux (FRA) de l'Union européenne (2009), para. 8.

65. Le WP29 a publié un avis général sur le traitement des données à caractère personnel dans le contexte professionnel; une recommandation concernant les données d'évaluation des employés; et un document de travail concernant la surveillance des communications électroniques sur le lieu de travail. Son avis sur les services de vérification du contenu des courriers électroniques est également intéressant.[23] Toutefois, à ce jour, ces documents n'ont pas débouché sur une grande convergence (et encore moins sur une harmonisation) dans ce domaine.

66. Intérêt public important: Les législations de plusieurs États membres prévoient la promulgation de décrets ou d'autres règles subsidiaires concernant le traitement des données sensibles pour les intérêts publics importants - en réalité, cela n'a été fait que dans quelques rares États membres (en particulier, le Royaume-Uni et la France) et, dans les règles en question, du moins au Royaume-Uni, les normes sont quelque peu ambiguës.

67. Plusieurs lois autorisent de la même manière l'autorité nationale chargée de la protection des données à délivrer des autorisations *ad hoc* - mais, pour autant que nous sachions, la Commission n'a reçu aucune notification dans ce sens (comme cela aurait dû être le cas en vertu de l'article 8(6) de la directive). Un État membre (la Belgique) prévoit la délivrance de permis aux organisations de défense des Droits de l'Homme les autorisant à traiter les données sensibles sans consentement (voir article 6 § 2(k) de la *Loi belge de protection des données*), mais cette disposition en soi est sujette à controverse et pourrait bien enfreindre la Convention européenne des Droits de l'Homme; à notre connaissance, aucun permis de ce genre n'a été demandé, du moins pas par les organisations internationales de défense des Droits de l'Homme.

68. Il convient toutefois de faire remarquer, dans ce contexte, que les lois relatives à la protection des données de plusieurs États membres s'en remettent de façon générale aux autres lois (ou règles) nationales, et un grand nombre de ces lois autorisent le traitement des données sensibles. Quant à savoir si ces autres lois prévoient des «garanties appropriées» à cet égard comme l'exige l'article 8(4) de la directive, la question est discutable. Ces autres lois ou dispositions auraient dû être notifiées à la Commission, mais il semble que cela n'ait pas été souvent le cas. Ce domaine demeure donc relativement obscur mais il est évident que, dans de nombreux pays et à de nombreux égards, de sérieux doutes doivent être émis quant à la conformité de ces règles avec la directive. De surcroît, ces questions étant manifestement régies par de nombreuses lois différentes (dont la plupart n'ont pas du tout été conçues en vue de la protection des données), des différences majeures subsistent entre les États membres.

69. Une fois encore, si ces lois devaient être appliquées dans les cas où le droit national pertinent est le «droit applicable» dans un contexte transnational, cela aurait des conséquences graves. Il y a peu de temps encore, ce problème ne présentait aucune urgence puisque de nombreuses affaires d'«intérêt public important» étaient traitées intégralement dans le cadre de la législation nationale et concernaient uniquement les ressortissants et résidents de l'État en question. Toutefois, compte tenu du renforcement

[23] Il s'agit, respectivement, des documents suivants: Avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel (WP48 du 13 septembre 2001); Recommandation 1/2001 concernant les données d'évaluation des employés (WP42 du 22 mars 2001); Document de travail concernant la surveillance des communications électroniques sur le lieu de travail (WP55 du 29 mai 2002); et Avis 2/2006 sur les problèmes de protection de la vie privée liés à la fourniture de services de vérification du contenu des courriers électroniques (WP118 du 21 février 2006).

de la coopération au sein de l'UE, notamment dans les domaines de la santé, de la protection sociale, de l'immigration, etc., un plus grand nombre d'arrangements transnationaux (au niveau européen), et de flux de données correspondants, tomberont sous le coup de la législation relative à la protection des données.

70. Il est donc urgent de préciser les choses, en particulier concernant la définition des «garanties appropriées» à cet égard, afin de faciliter le rapprochement (nivellement vers le haut) des garanties en matière de protection des données dans ces domaines.

71. Condamnations pénales: Les législations des États membres adoptent des approches très différentes à l'égard du traitement des données relatives aux condamnations pénales, etc. Certaines intègrent ces données dans la catégorie générale «données sensibles» (ce qui n'est pas sans conséquence, en particulier pour ce qui concerne l'autorisation de ces traitements avec le consentement de la personne concernée), tandis que d'autres étendent les règles spéciales relatives aux condamnations pénales aux données relatives aux autres contentieux juridiques ou aux données relatives à des «problèmes sociaux graves» ou à des «affaires strictement privées». Par ailleurs, les législations appliquent au traitement de ces données des normes très différentes. Certaines autorisent le traitement de ces données s'il est «autorisé par ou en vertu d'une quelconque disposition juridique» ou à toute «fin spécifiée par la loi»; ou autorisent ce traitement sur la base de tests d'«équilibre» vagues et subjectifs; tandis que d'autres prévoient des tests de «nécessité» très stricts et/ou exigent que les responsables du traitement (en particulier dans le secteur privé) se procurent des permis ou autorisations spéciaux. Des différences importantes entre les législations des États membres subsistent donc à cet égard.

72. Numéro national d'identification: Il existe différentes approches de l'utilisation des numéros nationaux d'identification et autres identifiants généraux similaires. Certains États membres autorisent l'échange généralisé de ces numéros entre les administrations publiques si cela peut permettre de faciliter leur travail, tandis que d'autres adoptent une approche plus restrictive, selon laquelle l'utilisation de ces numéros est (doit être) réglementée avec plus de précision. Certains pays autorisent l'utilisation de ces numéros dans le secteur privé avec le consentement des personnes concernées, tandis que d'autres se montrent, une fois encore, plus restrictifs, surtout par crainte que leur utilisation ne permette trop facilement les interconnexions entre bases de données et la divulgation des données sans aucun contrôle.[24]

Référence: Document de travail n° 2 (version étendue), section 4.4

(v) Règles relatives aux flux de données transfrontaliers

73. **Constat/conclusion:** La directive traite de deux types de flux de données transfrontaliers: les flux de données au sein de l'UE/EEE et les transferts de données vers des pays non membres de l'UE/EEE (pays dits «tiers»). S'agissant de ces derniers, elle établit également une distinction entre les pays tiers qui offrent une protection «adéquate» des données et ceux qui n'offrent pas de protection adéquate. Les règles de

[24] Au Royaume-Uni, il n'existe pas (encore) de numéro national d'identification. Cela serait toutefois le cas si le Registre d'identité nationale était créé en vue de la création des cartes d'identité nationales. Cependant, d'autres identifiants largement répandus, tels que le National Insurance Number (numéro d'assurance national), le National Health Service Number (numéro du service national de santé) et le permis de conduire sont souvent utilisés, tant par le secteur privé que par le secteur public, avec de rares restrictions.

base sont (ou du moins étaient) simples: au sein de l'UE/EEE, et au sein de ce qui constituait auparavant le premier pilier, les flux de données doivent s'effectuer librement. Toutefois, ce pilier ayant été aboli, la situation n'est plus aussi simple, comme nous l'expliquons ci-dessous. Les données peuvent aussi être transférées librement vers des pays tiers offrant une protection adéquate (si cette protection est adéquate à certains égards mais pas à d'autres, à condition que les données relèvent du domaine pour lequel la protection est adéquate) (Article 25(1)). Et en principe, les données ne peuvent pas être transférées vers des pays tiers n'offrant pas de protection des données adéquate (ni vers des pays où la protection est adéquate à certains égards mais pas à d'autres, si les données relèvent du domaine pour lequel la protection n'est pas adéquate), à moins qu'il ne soit satisfait à une condition spéciale (Article 26(1)).

74. Toutefois, ici encore, ces règles ne sont pas appliquées de façon uniforme. Tout d'abord, seuls quelques États membres prévoient expressément le libre transfert des données au sein de l'UE/EEE; la plupart d'entre eux l'acceptent de façon implicite (en imposant uniquement des restrictions explicites aux transferts vers des pays tiers) mais ne l'affirment pas clairement. Par ailleurs, parmi les rares États à stipuler cette liberté, seul un (l'Autriche) établit clairement que cette liberté ne s'applique qu'à l'égard des traitements visés par la directive. Cela est bien sûr essentiel puisqu'il n'existe aucune garantie que les traitements ne relevant pas de la directive (en particulier ceux couverts par l'ancien troisième pilier) soient soumis à un régime de protection des données adéquat (cf. article 3(2), premier alinéa, de la directive). L'application sans réserves de la règle de «libre circulation des données» énoncée à l'article 1(2) de la directive, si bien qu'elle n'érige aucun obstacle non plus au transfert des données au sein de ce que l'on appelait troisième pilier au sein de l'UE, est donc très problématique et entraînera immanquablement des violations des normes en matière de protection des données. Bien sûr, officiellement, la structure à trois piliers de l'UE n'existe plus depuis l'entrée en vigueur du Traité de Lisbonne. Il est cependant crucial, et aujourd'hui plus que jamais compte tenu de la nouvelle situation, d'assurer une protection des données complète et appropriée dans tous les domaines autrefois couverts par les différents piliers (comme expliqué ci-dessus, au point 5.02(i)). C'est à cette seule condition qu'il sera possible d'adopter une règle en accord avec l'article 1(2) qui s'appliquera à tous les transferts de données au sein de l'UE/EEE, sans se limiter aux domaines relevant du droit communautaire. Si nous voulons réussir à faire face aux défis du nouvel environnement technique mondial, cela doit se faire sans tarder.

75. S'agissant des transferts de données vers des pays offrant une protection des données «adéquate», la principale différence (mais qui est de taille) concerne la période précédant la constatation officielle du caractère «adéquat» par la Commission. En Autriche, en Espagne, en Grèce, au Luxembourg et au Portugal, la législation dispose clairement que, en l'absence de constatation du caractère «adéquat» par la Commission, seules les autorités nationales sont habilitées à déterminer si un pays tiers spécifique garantit une protection «adéquate». En d'autres termes, à moins que le caractère adéquat de la protection offerte par un «pays tiers» n'ait été constaté au niveau national (ou européen), et jusqu'à ce qu'il soit constaté, les transferts de données à caractère personnel vers ce pays sont soumis à une interdiction de principe. Dans certains pays, comme le Royaume-Uni, l'évaluation dans l'attente d'une «constatation» de la Commission revient aux responsables du traitement, ce qui reflète l'approche généralement laxiste et peu interventionniste adoptée par les autorités de ce pays.[25] Cela

[25] Voir la citation du Commissaire à l'information du Royaume-Uni à la p.180 du Comparative Summary

semble ne pas concorder avec la position du WP29. Le groupe de travail reconnaît que «la directive ne précise pas (...) si une autorité doit être chargée d'évaluer le caractère adéquat de la protection des données dans des pays tiers», mais en conclut qu'il est dès lors au moins «possible que la législation nationale des États membres assigne cette tâche aux autorités nationales chargées de la protection des données, dont l'autorisation peut être nécessaire pour que le transfert de données à caractère personnel puisse s'effectuer». En effet, si l'on en juge par le paragraphe ci-après, le groupe de travail semble estimer que ce sont là les deux seules réelles options:[26]

> Outre la possibilité que les autorités nationales évaluent le caractère adéquat si la législation nationale les y autorise, la directive dispose que les décisions relatives au caractère adéquat à l'échelon européen sont prises par la Commission, renforçant ainsi la certitude et l'uniformité juridiques dans l'ensemble de la Communauté...

76. Le problème est que si l'on associe la règle de base des «transferts libres au sein de l'UE/EEE» à la position laxiste du Royaume-Uni (ainsi que de certains autres pays), les règles strictes en vigueur dans la première catégorie de pays peuvent être facilement contournées: les autorités chargées de la protection des données dans ces pays ne peuvent pas (selon les termes de la directive) empêcher les transferts de données à caractère personnel vers les États membres appliquant des règles moins strictes, et les données peuvent ensuite être transférées de ces autres États membres vers des pays tiers dont le caractère «adéquat» n'a pas été officiellement constaté, que ce soit au niveau européen ou par les autorités du pays d'origine, lorsque le responsable du traitement estime que la protection est néanmoins suffisamment garantie. Il est impossible de déterminer l'ampleur de ce phénomène (notre impression est que, de manière générale, le degré de conformité aux règles juridiques en matière de transfert des données est relativement faible) mais il s'agit clairement d'une faille du système. Qui plus est, dans le nouvel environnement, au sein duquel les données sont transférées continuellement et couramment vers différents territoires, ce problème (l'utilisation de cette faille, consciemment ou inconsciemment) risque de se développer très rapidement.

77. Enfin, des divergences sont constatées au niveau de l'application des conditions spéciales auxquelles des données peuvent être envoyées vers des pays tiers n'offrant pas de protection «adéquate». Nous nous contenterons simplement de faire remarquer que, ici encore, les conditions ne sont pas appliquées de façon homogène: certains États membres ajoutent des tests ou des conditions plus strictes, par exemple en exigeant que la dérogation concernant le transfert pour protéger les intérêts vitaux d'une personne concernée ne s'applique que si ladite personne se trouve dans l'incapacité de donner son consentement au transfert. Un État membre assouplit plus qu'il ne faudrait les règles relatives au transfert des données à des fonctionnaires du fisc se trouvant dans des pays tiers qui n'offrent pas de protection, tandis que plusieurs autres n'appliquent pas la dérogation obligatoire concernant les transferts de données au départ de registres publics. Le WP29 a publié un document de travail à ce sujet dans le but spécifique de:[27]

(note 11, supra).

[26] WP29 «Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995» (note 12, supra), p. 4.

[27] *Idem*, synthèse, p. 2.

> faire part de ses craintes que des interprétations différentes ne soient données aux dispositions de l'article 26(1) dans la pratique, empêchant ainsi l'application uniforme de ces dispositions dans les différents États membres.

Il ajoute ceci:

> Le groupe de travail considère ce document comme un élément essentiel de sa politique en matière de transfert de données vers des pays tiers. Dès lors, il doit être lu à la lumière des autres travaux du groupe de travail dans ce domaine, notamment ses travaux sur les «règles d'entreprise contraignantes», les clauses contractuelles standard et le caractère adéquat dans les pays tiers, y compris la sphère de sécurité.

78. Ce document donne des directives sur l'application des différentes conditions spéciales dans le cadre des transferts de données vers des pays tiers n'offrant pas de protection adéquate, définies à l'article 26(1) de la directive. Toutefois, cela n'a donné lieu à aucun réel changement dans les pratiques des États membres. Les pays «stricts» susmentionnés restent attachés, sur papier, au principe selon lequel les données ne doivent pas être transférées au départ de leur territoire vers des pays dans lesquels ils (ou la Commission) n'ont pas constaté de protection adéquate; de leur côté, les pays «plus laxistes» restent convaincus que l'évaluation peut être effectuée par les responsables du traitement. En effet, à notre connaissance, les pays «stricts» ne constatent jamais le caractère adéquat d'un pays dont le caractère adéquat n'a pas été précédemment constaté par la Commission.

79. De manière générale, dans de nombreux États membres, qu'ils soient stricts ou laxistes sur papier, l'article 26 semble être davantage enfreint que respecté. Il est indispensable et urgent d'assurer une interprétation plus harmonisée de cette disposition importante; cette harmonisation doit aller de pair avec une politique uniforme visant à garantir une conformité effective dans tous les États membres. Comme nous l'expliquons au point C. ci-dessous, nous pensons que le WP29 peut contribuer à cela.

B. LES PAYS NON MEMBRES DE L'UE/EEE

80. Même si la directive et les Lignes directrices de l'OCDE ont influencé la législation de nombreux pays tiers, ces législations ne sont formellement liées à aucun des deux textes. Il n'est donc pas surprenant de constater que, dans ces pays, les questions abordées ci-dessus sont traitées de façons encore plus différentes (et lorsqu'ambiguïté il y a, ce qui est souvent le cas, il est encore plus difficile de les lever). Quelques brefs résumés suffiront à illustrer cela:

81. Définitions: Dans les pays non membres de l'UE/EEE, l'approche de la définition des «informations à caractère personnel» (ou «données à caractère personnel») est globalement la même que celle adoptée dans l'UE, bien qu'elle diffère quelque peu au niveau de la formulation et des définitions connexes. Compte tenu de l'absence d'interprétation judiciaire, il est difficile de déterminer si les différences sont significatives, mais tel ne semble pas être le cas sauf peut-être à Hong Kong, où la notion de «données à caractère personnel» a été interprétée par la Cour d'Appel, qui a estimé qu'il n'existait pas de «données à caractère personnel» lorsque les informations étaient collectées sans intention d'identifier l'individu. Certaines législations sont limitées aux collectes de données systématiques. Pour sa part, la législation indienne n'utilise pas du tout l'expression «données/informations à caractère personnel».

82. Les législations des pays non membres de l'UE/EEE n'utilisent pas invariablement les termes «responsable du traitement» et «sous-traitant». Certaines utilisent les termes «traitement» et «utilisateur des données» (Hong Kong), tandis que d'autres parlent de «traitement» sans définir ce terme (Japon).

Références: Rapport concernant Hong Kong, 2.2; rapport concernant le Japon 2.2; rapport concernant l'Inde 3.2.

83. Principes de protection des données: Dans la plupart des pays tiers examinés dans le cadre de cette étude, les approches adoptées par les législations à cet égard sont encore plus variées puisque celles-ci ne cherchent pas à se conformer à un autre modèle que les Lignes directrices de l'OCDE, qui sont relativement générales. Toutefois, l'Australie, Hong Kong et le Japon s'efforcent tous trois de mettre en œuvre le principe de finalité (bien que l'Australie et le Japon autorisent des exceptions relativement larges concernant l'utilisation secondaire). L'Inde n'a pas encore mis en place de loi générale sur la protection des données, mais sa loi relative à la notification des crédits financiers applique de façon très stricte le concept de finalité (à l'instar de la loi australienne équivalente, mais dans une plus grande mesure que Hong Kong).

Références: Rapport concernant l'Australie, 2.2; rapport concernant Hong Kong, 2.2; rapport concernant le Japon 2.2; rapport concernant l'Inde 3.2.

84. Critères de protection des données: Dans les territoires de la région Asie-Pacifique couverts par cette étude, le concept de 'traitement légal' n'est pas explicitement au cœur de la législation relative à la protection des données, et il n'y figure sans doute pas de façon implicite non plus. Dans ces territoires, il n'est pas supposé que le traitement est illégal à moins d'être justifié. Au lieu de cela, le traitement (bien que ce terme ne soit pas toujours utilisé) est supposé légal à moins qu'il n'enfreigne l'un des principes de confidentialité des informations (collecte, utilisation, divulgation, sécurité, etc.). Sur le fond, cela n'entraîne peut-être pas souvent de divergences dans la pratique, mais l'approche et l'attitude sont très différentes. Il est donc difficile d'établir des comparaisons directes entre ces législations et les législations européennes examinées dans le reste de cette section.

85. Dans ces territoires, il est donc indispensable d'examiner de façon spécifique, dans un contexte particulier, si le consentement, ou du moins une certaine forme d'avertissement, est nécessaire pour la collecte de données à caractère personnel afin de pas commettre d'infraction, et si le consentement, l'autorisation légale ou l'évaluation de l'«équilibre» de l'intérêt public signifient qu'une utilisation ou une divulgation secondaire ne constituera pas une infraction au principe d'utilisation ou de divulgation. En d'autres termes, il convient de se poser la question de la «légitimité» de la collecte, de l'utilisation ou de la divulgation dans un cas spécifique plutôt que la question, plus générale, de la «légitimité du traitement légitime» au regard d'un «critère» spécifique. Toutefois, la réponse sera souvent la même.

86. Généralement, les États-Unis ne reconnaissent pas le principe de proportionnalité dans la collecte de données. En outre, leur approche sectorielle donne lieu à différentes situations de consentement, de refus, et de neutralité. Le consentement peut être requis dans certains contextes mais pas dans d'autres où les données en cause sont sans doute tout aussi sensibles. Voir le rapport concernant les États-Unis, à la section 7.6. L'approche américaine est davantage axée sur la formalité d'obtention du niveau de consentement spécifié et ne se préoccupe pas suffisamment de savoir si les membres

sont bien informés des conséquences de leur consentement. En outre, de nombreuses entreprises assimilent l'achat d'un produit ou d'un service au consentement à une utilisation secondaire des données; cela se reflète dans un certain nombre de lois qui exonèrent les clients ayant des «relations commerciales bien établies» avec une entreprise de certaines obligations en matière de consentement.

Référence: Rapport concernant les États-Unis, sections 4.3 et 7.6.

87. Traitement des données sensibles: Le cadre américain n'offre pas de protection générale pour les données sur la seule base de leur sensibilité. Toutefois, les vérifications des antécédents préalables à l'embauche sont soumises à une réglementation relativement précise (et sont traitées comme la notification des crédits financiers), qui s'appuie sur les principes de la protection des données. Par ailleurs, les données relatives aux ressources humaines et les autres informations collectées dans le cadre professionnel ne sont pas couvertes par une loi sectorielle sur la vie privée. Les États-Unis traitent les arrestations criminelles et les condamnations pénales comme des archives publiques; en règle générale, les informations peuvent être utilisées à presque n'importe quelle fin.

Référence: Rapport concernant les États-Unis, sections 5.1, 5.5 et 5.7

88. Flux de données transfrontaliers: Dans les pays non membres de l'UE/EEE, les restrictions aux flux de données transfrontaliers sont très diverses. Dans les pays de la région Asie-Pacifique visés par l'étude, la position est la suivante (sans tenir compte des complications liées à la position des mandataires/administrateurs ni des questions liées à l'effet extraterritorial [limité] des législations concernées):

(a) La législation australienne relative au secteur privé contient actuellement une disposition de restriction aux exportations de données (NPP 9), librement inspirée des articles 25 et 26 de la directive, dont elle n'a pas la force; cette restriction n'a jamais fait l'objet d'aucune plainte officielle, et encore moins d'une décision judiciaire;
(b) La Région administrative spéciale de Hong Kong impose une restriction à l'exportation de données dans son Ordonnance (s. 33) mais celle-ci n'a jamais été appliquée; si elle venait à l'être, elle aurait une force au moins comparable à celle des dispositions de la directive;
(c) L'Inde n'impose aucune restriction aux exportations de données;
(d) Le Japon n'impose aucune restriction aux exportations de données autre que les prescriptions habituelles relatives à la 'finalité' concernant l'utilisation et la divulgation, et elles sont aussi faciles à éviter.

89. Dans les autres pays de la région Asie-Pacifique, les seules autres restrictions à l'exportation de données concernent la Région administrative spéciale de Macao (une disposition stricte inspirée de la directive), la Corée du Sud (fondée sur le consentement) et Taiwan (une disposition inconsistante et inutilisée). En Nouvelle Zélande, une disposition minimaliste est actuellement en cours d'adoption.

Références: Rapport concernant l'Australie, 6; rapport concernant Hong Kong, 6; rapport concernant l'Inde, 7; rapport concernant le Japon, 5.

C. COMMENT PARVENIR À UNE PLUS GRANDE HARMONISATION

90. **Recommandation:** Comme nous l'avons fait remarquer précédemment, si nous voulons, dans l'UE/EEE, un régime de protection des données efficace qui nous permette de faire face aux défis que pose le nouvel environnement technique mondial, il est impératif d'assurer une plus grande harmonisation des règles relatives à la protection des données au sein de l'UE. L'une des façons d'y parvenir serait de remplacer la directive principale (et donc probablement les directives accessoires) par un Règlement (directement applicable) (ce qui avait déjà été envisagé lors de l'élaboration de la directive principale), ou par une toute nouvelle directive rédigée en des termes beaucoup plus stricts. Toutefois, cela soulèverait les questions complexes de la subsidiarité et de la compétence juridique et déboucherait sur des règles plus rigides. Nous nous sommes donc intéressés à la solution alternative: trouver des moyens de renforcer l'harmonisation dans le cadre de la directive principale telle quelle. Cela peut se faire de différentes manières, qui ne sont pas toutes incompatibles les unes avec les autres:

91. Tout d'abord, concernant les États membres de l'UE/EEE, nous pensons que la Commission pourrait se montrer plus ferme dans les mesures prises à l'encontre des États membres qui, à l'évidence, n'appliquent pas les dispositions de la directive de façon appropriée (tant sur papier que dans la pratique); et que la Commission devrait utiliser ses pouvoirs d'exécution de la loi pour renforcer l'harmonisation (comme suggéré au paragraphe 94 ci-dessous).

92. Nous pensons cependant que le rôle le plus crucial à cet égard pourrait revenir au WP29: bien que ses avis, etc. ne soient pas contraignants, il dispose de l'expertise nécessaire et d'un lien direct avec les pratiques nationales, ce qui lui permet de formuler des interprétations et des modes d'application de la directive harmonisés. Il peut toutefois être reproché au WP29 de parfois adopter collectivement, au niveau européen, des points de vue et des interprétations, ainsi que des propositions pour l'application des directives, que ses membres ne peuvent pas (ou ne souhaitent pas) appliquer dans leur pays. Parfois, ce sont les textes des lois nationales qui y font obstacle; parfois encore, les autorités chargées de la protection des données ne disposent tout simplement pas du pouvoir juridique d'imposer au niveau national des interprétations ou des solutions convenues au niveau européen.

93. Nous pensons que, à cet égard, le régime européen de protection des données peut être considérablement renforcé. Le WP29 adopte déjà de nombreux avis, documents de travail et positions sur l'interprétation et l'application de la directive. Abstraction faite de la critique émise ci-dessus, ces positions et avis sont très respectés, en Europe et au-delà, et sont considérés comme faisant autorité et comme reflétant la bonne façon d'interpréter et d'appliquer les normes européennes (et mondiales). La question clé est: comment s'assurer que ces positions et avis ont réellement un impact au niveau national (sans attribuer au WP29 les pouvoirs qui doivent normalement revenir à la Commission et aux tribunaux)?

94. Nous recommandons de demander au WP29, en consultation avec la Commission (qui, de toute façon, lui sert de secrétariat) de multiplier et d'approfondir ses études sur les législations et pratiques nationales afin de définir les «meilleures pratiques» et de proposer des interprétations (ce qu'il fait déjà), tout en demandant aussi aux États

membres d'expliquer dans quelle mesure ils adhèrent (ou estiment qu'ils ne devraient pas être obligés d'adhérer) à ces suggestions. Il appartiendrait ensuite à la Commission, le cas échéant, de vérifier si les directives du WP29 sont celles qui, dans le droit, doivent être suivies par les États membres - en considérant les mesures d'exécution forcée comme une façon normale de vérifier cela si nécessaire (cf. notre précédente recommandation sur le renforcement des mesures d'exécution forcée, au paragraphe 91 ci-dessus). L'idée est que le WP29 formule des recommandations quant à la façon appropriée d'interpréter les directives et de les appliquer au niveau national (comme il le fait déjà); et que si la Commission reconnaît que l'interprétation et l'application proposées sont appropriées mais que ces suggestions ne sont pas suivies par certains États membres, elle prenne des mesures d'exécution forcée à l'encontre de ces États. Les États en question pourraient s'y conformer, auquel cas l'harmonisation pourrait être réalisée. Ils pourraient aussi contester devant la CJE l'interprétation du WP29 approuvée par la Commission, auquel cas une décision définitive faisant autorité serait prononcée, qui aurait également un impact favorable sur l'harmonisation.

95. Nous pensons que cette solution ne nécessiterait aucune modification de la directive. Elle témoignerait néanmoins d'un changement radical dans l'approche de la Commission vis-à-vis de l'harmonisation de la transposition et de la mise en œuvre des directives puisque les avis du WP29 seraient effectivement mis en application, le cas échéant, par la Commission (sous la supervision, bien entendu, de la CJE).

96. Pour faire un premier pas dans cette direction, et afin de permettre au WP29 et à la Commission d'agir, nous recommandons que les positions du WP29 ainsi que les informations relatives à leur transposition dans les législations et pratiques nationales des États membres soient présentées de façon plus structurée et plus complète, et que l'attention des organismes administratifs et judiciaires compétents aux niveaux national et européen soit attirée sur ces informations.

Référence: Une recommandation à cet effet figurait déjà parmi les recommandations d'une autre étude de la Commission européenne présentée cette année, dans le cadre de laquelle il a été procédé à une Évaluation de la contribution du groupe de travail «WP29» aux travaux de la Commission dans le domaine de la protection des données: voir la recommandation 7 de cette étude, qui stipule ce qui suit:

> Nous recommandons que le WP29 étudie la possibilité de créer une base de données ou une ressource électronique similaire dans laquelle seraient stockées de façon structurée les parties pertinentes de tous les avis et documents de travail du WP29, de manière qu'il soit possible de trouver rapidement et de mettre en corrélation les commentaires qui figurent dans n'importe lequel d'entre eux concernant un sujet plus large (par exemple, sur la notion de données à caractère personnel, ou de droit applicable); et de demander aux membres du WP29 de communiquer à cette même ressource des informations similaires sur les législations et pratiques nationales dans leur propre pays. Nous sommes convaincus que cela contribuerait largement à la «valeur ajoutée européenne» déjà fournie par le WP29, et à l'harmonisation (de l'application des) des législations et pratiques nationales.
>
> Nous sommes convaincus que cette ressource contribuerait aux trois points mentionnés par le WP29 dans son dernier programme de travail, sous le titre «Accroître l'efficacité du groupe de travail 'Article 29'»: elle contribuerait à l'élaboration de principes directeurs et de normes directrices, améliorerait l'efficacité du WP29 pour ce qui concerne les pratiques nationales, et faciliterait

l'exécution. Il ne fait aucun doute que cela aiderait aussi le WP29 dans le rôle consultatif qu'il joue auprès de la Commission.

Remarque: Les bases de cette ressource ont déjà été posées dans le cadre d'un programme de la CE baptisé «e-TEN», portant sur la création du label européen de protection de la vie privée «EuroPriSe», qui vient juste d'être clôturé. Afin de faciliter le travail des experts formés dans le cadre de ce projet, une série de critères ont été définis sur la base des directives relatives à la protection des données, et un commentaire a été rédigé, qui formule précisément le même genre de recommandations que celles que nous venons de mentionner concernant les documents du WP29 et les pratiques nationales. Ce commentaire a été très apprécié par la Commission ainsi que par les autorités chargées de la protection des données qui participaient au projet, et est très demandé par les entreprises.[28]

97. En principe, la Convention n° 8 du Conseil de l'Europe (et son protocole additionnel) ainsi que son Comité consultatif et le Groupe de projet sur la protection des données (CJ-PD) peuvent, eux aussi, jouer un rôle très utile, en particulier pour ce qui concerne les pays non membres de l'UE/EEE et du Conseil de l'Europe. Le Comité consultatif et le CJ-PD publient des directives importantes sur l'application des principes de base de la protection des données (qui sont communs à la Convention et à la directive CE) dans des domaines spécifiques tels que la police, l'échange d'informations judiciaires dans des affaires criminelles, etc.[29] Cela n'a toutefois pas conduit à une plus grande harmonisation entre les États parties à la Convention qu'entre les États membres de l'UE/EEE, au contraire: l'harmonisation, même si elle est faible, reste plus grande dans l'UE/EEE que dans l'espace de la Convention du Conseil de l'Europe.

98. Enfin, faisons remarquer que, en dehors de l'UE/EEE et du COE, aucune institution n'a le projet d'encourager l'harmonisation. Le cadre de protection de la vie privée de la CEAP n'a eu aucun effet à cet égard. Les accords sur l'harmonisation des législations relatives au commerce électronique conclus dans le cadre de l'ANASE pourraient contribuer à une relative harmonisation d'ici 2015 dans les pays membres, mais cela reste à démontrer. La réunion des Asia Pacific Privacy Agencies (APPA) n'a pas de base institutionnelle équivalente au WP29, ni d'ailleurs d'expérience ou d'ambition en matière d'harmonisation. Les travaux du WP29 de l'UE n'en sont que plus importants, et ce à l'échelle mondiale.

---

[28] Le catalogue de critères d'EuroPriSe et le Commentaire ont été préparés par le chef d'équipe du présent projet, qui était également conseiller juridique principal pour ce projet, aidé de cinq juristes attachés à l'autorité chargée de la protection des données du *Land* de Schleswig-Holstein, avec la contribution des autorités chargées de la protection des données à Madrid et en France. Une copie de ces documents a été transmise à la Commission (NB: le Commenaire n'est pas publié pour des raisons commerciales). [note figurant dans l'original du rapport d'évaluation du WP29]. Cette recommandation a été complétée par une autre note du chaf d'équipe pour cette évaluation (qui est également le chef d'équipe de la présente étude), à la demande de la Commission. Cette remarque figurait dans le rapport d'évaluation du WP29, à l'Annexe 2.

[29] Ces organismes ont également couvert certains domaines aussi couverts (généralement de façon similaire) par l'UE/EEE, tels que la CCTV et les contrats de transferts de données transfrontaliers. Voir: http://www.coe.int/t/e/legal_affairs/legal_co-peration/data_protection/documents/reports_and_studies_of_data_protection_committees/2Committee%20Studies%20and%20reports.asp#TopOfPage.

5. COOPÉRATION AVEC LES PAYS NON MEMBRES DE L'UE/EEE (Y COMPRIS LES CONSTATATIONS DU CARACTÈRE «ADÉQUAT»)

99. **Constat/conclusion:** Dans le contexte du nouvel environnement sociotechnique, et de la mondialisation en particulier, il est primordial, d'un point de vue européen, d'inciter les autres pays (non européens) à se doter de lois de protection de la vie privée ou de protection des données qui soient «adéquates» de ce point de vue. La directive principale prévoit des procédures spéciales à cette fin, et «récompense» les pays qui adoptent des lois «adéquates» après une évaluation de la Commission (qui tient également compte du point de vue du WP29). Toutefois, jusqu'à présent, cette procédure n'a été utilisée que dans quelques cas, notamment dans trois territoires britanniques en Europe (ainsi que dans le cas spécial de la «sphère de sécurité» américaine et dans le cas encore plus controversé des dossiers passagers demandés par les États-Unis).[30] Depuis l'entrée en vigueur de la directive, il y a une quinzaine d'années, la Commission n'a pas encore pris une seule décision concernant le caractère adéquat des régimes juridiques de territoires appartenant à la région Asie-Pacifique.

100. Nous sommes bien conscients que les constatations du caractère «adéquat» ne peuvent être délivrées officiellement qu'au terme d'un processus rigoureux, et pour les pays qui offrent réellement une protection adéquate, mais l'utilisation limitée de cette procédure n'a peut-être pas envoyé un signal positif aux autres pays, en particulier aux pays non européens. Au départ, les pays de la région Asie-Pacifique étaient particulièrement intéressés par la proposition de se conformer aux normes européennes du caractère adéquat car ils espéraient qu'elle aurait des effets bénéfiques sur le commerce, comme nous l'illustrons au travers des exemples (purement hypothétiques) ci-après:

(i) la constatation du caractère adéquat du régime du secteur privé en Corée du Sud, tandis que celui du Japon n'est pas jugé adéquat en raison d'une application lacunaire;
(ii) la constatation du caractère adéquat du régime de Macao, sur le territoire de la Chine, tandis que celui de Hong Kong n'est pas jugé adéquat en raison de déficiences au niveau de la mise en application et de la non-entrée en vigueur des restrictions aux exportations de données;
(iii) ou la constatation du caractère adéquat de la législation de Hong Kong tandis que celle de Taiwan n'est pas jugée adéquate; ou
(iv) la constatation du caractère adéquat de la législation néo-zélandaise tandis que la législation australienne n'est pas jugée adéquate.

Dans chacun de ces groupes de territoires, de telles décisions concernant le caractère adéquat inciteraient très probablement les territoires jugés «inadéquats» à renforcer leur

[30] Actuellement, les pays dans lesquels la protection des données a été officiellement reconnue «adéquate» sont l'Argentine, le Canada, Guernesey, l'Île de Man, Jersey et la Suisse. Dans certains pays (tels que la Hongrie), la protection avait autrefois été jugée «adéquate» mais ceux-ci ont depuis adhéré à l'UE et la procédure ne s'applique plus à eux: ils sont tenus de se conformer aux directives et de les mettre en œuvre dans leur intégralité. Bien qu'aucune décision formelle n'ait été prise concernant l'Australie, le WP29 a rendu un avis globalement négatif (Avis 3/2001 du 26 janvier 2001, WP40). Il a toutefois été suggéré que certaines des critiques formulées par le WP29 étaient erronées, et certaines d'entre elles ont été depuis prises en compte dans la législation, ainsi qu'il est expliqué en détail dans le rapport des experts sur le caractère adéquat des protections offertes par l'Australie, rédigé par Bygrave et Greenleaf en 2005 et présenté à la Commission. Cela ne signifie pas que la conclusion du WP29 dans son Avis WP40 était inexacte, mais simplement que sa position est plus complexe que ce qu'elle peut paraître ici.

législation en matière de protection des données (et seraient probablement source de mécontentement à l'égard de l'UE au niveau politique) en raison de leur position par rapport à leurs «pairs». Tous les pays de la région Asie-Pacifique seraient probablement amenés à se poser la question suivante: «Aimerions-nous que nos lois soient déclarées 'inadéquates'?».

101. Toutefois, cet argument a perdu de son poids et sonne désormais creux. En 2009, les pays de la région Asie-Pacifique n'accorderaient probablement plus le même crédit à cette proposition qu'il y a dix ans. Le fait d'accorder le caractère adéquat dans le cadre du système de «sphère de sécurité» américain n'a certes pas contribué à la crédibilité de la position européenne de ce point de vue, en particulier en regard de l'absence de constatations concernant certains territoires de la région Asie-Pacifique, que tout observateur impartial considérerait comme beaucoup plus significative que la sphère de sécurité en termes de protection des données. Cependant, la constatation du caractère «adéquat» n'a pas encore perdu tout son attrait, et est toujours invoquée explicitement par le Commissaire à la vie privée de Nouvelle Zélande comme argument pour passer le projet de loi actuel visant à renforcer les dispositions relatives à l'exportation de données.

Remarque: Il convient de distinguer cette question de la question suivante de savoir si les normes définies dans la directive sont considérées comme un modèle pertinent pour les nouvelles lois de protection des données dans les pays d'Asie et du Pacifique. La réponse reste apparemment affirmative puisque la loi la plus récemment promulguée dans la région, celle de Macao, a été élaborée sur le modèle de la directive (via la législation portugaise), et le projet de loi à l'étude en Chine en 2006-2007 a été, lui aussi, fortement influencé par l'UE.

102. Nous reconnaissons que cette conclusion relativement catégorique doit être tempérée par plusieurs autres facteurs, qui compliquent les exemples simples donnés au paragraphe 100: (i) normalement, la Commission attend qu'un pays lui demande d'évaluer le caractère adéquat (bien que cela ne soit pas nécessaire, nous comprenons qu'il puisse être difficile, d'un point de vue politique, d'entamer une telle procédure sans que la demande n'ait été formulée); (ii) les constatations du caractère «adéquat» (et peut-être encore davantage les éventuelles constatations du caractère «*in*adéquat») peuvent avoir des répercussions politiques qui dépassent le cadre de la protection des données, et dont il convient de tenir compte; et (iii) la Commission a à sa disposition d'autres méthodes que les constatations publiques du caractère adéquat pour encourager le renforcement de normes de protection des données dans les pays non membres de l'UE/EEE.

103. **Recommandation:** Nous devons ici nous contenter de constater que le processus de constatation du «caractère adéquat» n'a pas (encore?) eu l'impact qu'il aurait pu avoir. De notre point de vue, le processus ainsi que ses délais d'application doivent être revus. La prise de décisions provisoires est une piste qui pourrait être explorée. Quoi qu'il en soit, il est indispensable de maintenir et de soutenir fermement les autres mesures, moins formelles, telles que l'assistance technique, la collaboration étroite (y compris les «jumelages» de DPA européennes et non européennes) et les autres processus. En attendant, il est important, au niveau politique, de faire en sorte que le processus de l'article 25 de la directive ne perde pas l'impact qu'il pourrait avoir au niveau international.

6. SUPERVISION ET EXÉCUTION: Le rôle des autorités chargées de la protection des données (DPA) et des tribunaux:

104. **Constat/conclusion:** Les DPA ont une excellente connaissance de la législation, et elles donnent des conseils très utiles à ce sujet, mais elles ne sont pas très efficaces en termes d'exécution: le «contrôle» de la conformité aux lois sur la protection des données par les DPA est généralement déficient et inefficace. Selon les conclusions d'un rapport majeur réalisé pour l'Agence des droits fondamentaux de l'UE, rédigé parallèlement au présent rapport:

> Ce rapport comparatif met en évidence les principales failles du système actuel de protection des données à caractère personnel dans les 27 États membres de l'UE. Des lacunes ont été observées en termes de manque d'indépendance, de ressources adéquates et de pouvoir de certaines des autorités chargées de la protection des données. La conformité avec la législation en matière de protection des données dans la pratique de plusieurs États membres pose également question. Par ailleurs, des réformes législatives sont nécessaires dans le domaine des sanctions et des indemnités afin de garantir une meilleure mise en application de la législation pertinente et une plus grande protection des victimes de violations des données à caractère personnel.
>
> Synthèse du projet final du document Comparative Legal Study on assessment of data protection measures and relevant institutions, rapport commandé par l'Agence des droits fondamentaux (FRA) de l'Union européenne (2009), para. 8.

De manière générale, nous adhérons (et nous nous en remettons) à l'étude de la FRA, mais nous tenons à faire remarquer que l'inefficacité de nombreux pays sur le plan de la mise en application avait déjà été relevée dans une précédente étude,[31] et que la situation ne semble pas s'être beaucoup améliorée.

105. Nous nous limiterons ici à quelques observations plus spécifiques. Tout d'abord, nous estimons que, trop souvent, les DPA interviennent trop tard: leur avis est sollicité lorsque les systèmes sont déjà pour ainsi dire «définitifs», en particulier dans le secteur public. Cela est également vrai des *soi-disant* «vérifications préalables», si celles-ci ne sont effectuées que lorsque la conception du système a déjà été finalisée (avec les répercussions majeures que cela implique sur les coûts). Un autre problème est celui du manque de compétences techniques de base de nombreuses DPA: ces autorités comptent toujours un trop grand nombre de juristes et pas suffisamment de spécialistes des systèmes et de l'informatique.

106. Une autre question, plus fondamentale, se pose concernant les rôles (qui, à notre avis, sont incompatibles dans une certaine mesure) des DPA. Ces autorités sont des conseillers et des guides. Ce sont également elles qui interprètent les lois, et jouent parfois presque un rôle de législateur. Elles sont supposées défendre les intérêts des personnes concernées. Et elles sont censées faire appliquer les lois. Nous pensons que toutes ces fonctions sont trop lourdes à porter pour un seul organisme. Le danger est que, en tant qu'autorité de réglementation, elles ne deviennent «prisonnières» de ceux qu'elles contrôlent, en particulier l'industrie et les agences gouvernementales. Ce phénomène est loin de se limiter aux autorités chargées de la protection des données: il

[31] Douwe Korff, étude de la CE intitulée Case-law on compliance, 1998.

a en effet été observé dans de nombreux organismes de réglementation modernes. Mais il fait aussi ressortir les conflits entre les différents rôles de ces autorités.

107. Nous pensons que ces problèmes (ces conflits) doivent être débattus de façon plus approfondie dans le cadre de la révision de la directive. Peut-être faudrait-il envisager de séparer les fonctions «douces» de conseil et d'orientation de ces autorités du rôle plus «dur» de mise en application des lois, et d'assigner ce dernier aux tribunaux (qui interviennent aussi dans les actions intentées par des particuliers: voir section V.7 ci-dessous) et (pour les infractions plus graves ou plus générales) aux autorités chargées des poursuites. Bien sûr, les DPA, en leur qualité d'experts dans ce domaine, pourraient toujours être sollicitées par les tribunaux pour un conseil; elles pourraient également se voir accorder le droit d'émettre un avis *d'office* et le droit de comparaître *d'office* dans les affaires concernant la protection des données. Quoi qu'il en soit, si les questions en rapport avec la protection des données sont placées entre les mains des tribunaux (ou de tribunaux spéciaux, comme c'est le cas au Royaume-Uni), les personnes concernées et les responsables du traitement doivent jouir d'un égal accès à ces instances.

108. **Recommandations:** Nous recommandons une «vérification préalable» de tous les systèmes d'information à l'échelle de la population dans l'État membre, en particulier dans le secteur public - mais (i) avant qu'ils ne soient définitifs (c'est-à-dire dès le début de la phase de planification) et (ii) par un personnel plus qualifié (du point de vue technique). Il est intéressant de constater que le Gouvernement australien a récemment proposé que soit conféré au Commissaire à la vie privée du pays le pouvoir de demander aux agences gouvernementales de préparer des évaluations des facteurs relatifs à la vie privée (rapport concernant l'Australie, 8.2). Dans le secteur privé, les audits en matière de protection de la vie privée ou les labels de protection de la vie privée (réels et efficaces) pourraient jouer un rôle similaire, étant fortement encouragés par des règles relatives aux marchés publics conférant un avantage concurrentiel aux produits et services respectueux de la protection des données (comme cela est déjà le cas en Allemagne, dans le *Land* du Schleswig-Holstein). Nous reviendrons sur cette dernière suggestion à la sous-section V.8 sur les *Mesures supplémentaires et alternatives*. De manière plus générale, nous pensons (sans vouloir préjuger de cela) qu'il pourrait être envisagé de retirer en grande partie le pouvoir de mise en application des mains des DPA pour le placer dans celles des tribunaux et des autorités chargées des poursuites.

7. DROITS INDIVIDUELS ET RECOURS

109. **Constat/conclusion:** L'une des exigences les plus importantes pour tout nouveau régime de protection des données dans l'UE/EEE (et au-delà) est le renforcement des capacités des individus, et en particulier la levée des obstacles aux poursuites, comme les règles relatives aux coûts dans certains pays (notamment en Angleterre), qui rendent presque impossible toute action en justice par un particulier.[32]

[32] À ce sujet, voir la réponse de la Foundation for Information Policy Research (FIPR) à la consultation Civil Litigation Costs Review réalisée par Lord Jackson, juillet 2009, qui stipule que: «*D'après ce que nous avons pu voir, il semble que l'Angleterre soit le pire endroit au monde pour l'exercice des droits numériques par les citoyens*». La proposition prônait la mise en place de règles moins coûteuses pour les particuliers (ou les ONG qui les soutiennent), comme cela existe dans les autres pays tels que l'Allemagne, au moins dans les affaires en rapport avec les droits de l'homme (qui s'étendraient aux questions liées à la protection des données). Pour consulter le document (en anglais): http://www.fipr.org/090730jackson.pdf.

110. **Recommandations:** Les particuliers devraient pouvoir disposer d'une réelle voie de recours et obtenir des injonctions provisoires ou permanentes dans le cadre de procédures rapides, simples et abordables devant des instances compétentes, indépendantes et impartiales. Bien que, en vertu du principe de subsidiarité, les détails de ces recours relèvent de la compétence des États membres, le droit de recours de base doit être formulé de façon plus détaillée qu'il ne l'est actuellement. En particulier, les conditions de base à remplir pour rendre réellement efficace le «recours juridictionnel» prévu à l'article 22, doivent être débattues au sein du WP29, et des directives doivent être formulées à ce sujet - et, conformément à nos recommandations de la sous-section V.4.C (para. 94 en particulier), la Commission ne doit pas hésiter à prendre des mesures d'exécution forcée en cas de non-respect de ces conditions.

111. Par ailleurs, une plus grande attention devrait être accordée au soutien des particuliers à cet égard, en autorisant les groupes non gouvernementaux/de la société civile à contribuer ou à participer officiellement à ces procédures, ou à agir au nom de groupes de personnes concernées, encore une fois sans s'exposer à des frais exorbitants (sous réserve de tests ou de l'autorisation du tribunal afin d'éviter les poursuites abusives, le cas échéant). Bien que des «actions collectives» comme celles qui ont cours aux États-Unis soient rarement prévues dans les systèmes juridiques européens, des procédures analogues sont parfois possibles, et nous pensons qu'elles peuvent davantage aider les particuliers que les aides extrêmement modestes que les DPA offrent actuellement aux personnes concernées. Dans le cadre d'une révision de la directive, il serait utile d'entreprendre une nouvelle étude sur les procédures et les recours auxquels les particuliers et les ONG peuvent et devraient pouvoir avoir accès. Cette étude pourrait également explorer des arrangements moins conventionnels mais peut-être plus efficaces, tels que le système «*qui tam*» (décrit dans le rapport concernant ce pays) utilisé aux États-Unis. Bien sûr, une telle étude devrait reconnaître que les décisions relatives aux modalités de mise en œuvre des directives incombent principalement aux États membres. Il peut néanmoins être utile de connaître avec plus de précision les avantages et les inconvénients, ainsi que l'efficacité ou autre, de ces différentes procédures.

112. Il pourrait également être envisagé de prévoir l'octroi de dommages-intérêts conventionnels par défaut pour la violation de certains droits des personnes concernées. Ces dommages-intérêts doivent être supérieurs au coût de la non-conformité.

113. Par ailleurs, il existe des systèmes gratuits et simples pour défendre les droits des personnes concernées dans des contextes particuliers tels que le démarchage commercial, qui connaissent un grand succès et se révèlent très efficaces. La plupart des États membres de l'UE/EEE ainsi que la Nouvelle Zélande, la Corée du Sud, l'Australie et l'Inde disposent de systèmes de préférences par courrier, par fax et par téléphone. Aux États-Unis, un site Internet très utilisé permet d'accéder gratuitement aux rapports sur les consommateurs. Pour ce qui concerne le démarchage par téléphone, 160 millions de numéros sont actuellement répertoriés dans la liste de «numéros à ne pas appeler» du système. Ces systèmes remportent un franc succès dans le monde entier car ils sont bien connus et faciles à utiliser, et ils constituent une solution efficace à la publicité non sollicitée par courrier, par fax par téléphone ou par SMS (bien que, pour leur utilisation, les données relatives aux personnes concernées doivent obligatoirement être conservées sur les listes oranges de sorte qu'elles ne sont pas une solution au «fichage»).

8. MESURES SUPPLÉMENTAIRES ET ALTERNATIVES

114. Dans cette dernière section, nous portons un regard critique sur diverses mesures dont certains pensent qu'elles pourraient compléter ou remplacer des mesures mises en œuvre actuellement pour tenter de garantir la conformité aux lois et principes en matière de protection des données. Certaines de ces mesures sont bien connues depuis au moins une dizaine d'années; d'autres sont prônées par la directive elle-même. Il semble cependant que, jusqu'à présent, les responsables du traitement des données n'aient pas été suffisamment incités à les utiliser – en dépit de l'obligation de mettre en œuvre «les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel» stipulée dans la directive (Article 17(1)). En outre, il arrive souvent qu'elles ne livrent pas les résultats escomptés. Nous examinerons tour à tour les avantages potentiels et les limites (et les promesses souvent illusoires ou non tenues) des mesures ci-après:

- ✓ **Technologies renforçant la protection de la vie privée (Privacy Enhancing Technologies - PET)**, y compris le cryptage (comme moyen de garantir la conformité au moins avec les obligations en matière de sécurité des données) et une question connexe: la notification des infractions à la sécurité; la désidentification; et d'autres éléments, tels que la P3P et les systèmes d'accès en ligne pour les personnes concernées;

- ✓ **Gestion des identités respectueuse de la vie privée**, y compris les systèmes centralisés (aujourd'hui largement dépassés), les systèmes «centrés sur l'utilisateur» plus récents, les «systèmes de gestion des données centrés sur le client», et l'utilisation des cartes d'identité à des fins diverses;

- ✓ **Prise en compte du respect de la vie privée dès la conception (Privacy by Design)**, y compris l'utilisation des évaluations des facteurs relatifs à la vie privée (Privacy Impact Assessments);

- ✓ **Contrôle de la vie privée par les utilisateurs et paramètres par défaut**;

- ✓ **Autoréglementation et coréglementation sectorielles**; et

- ✓ **Labels de protection de la vie privée.**

(i) Technologies renforçant la vie privée (Privacy Enhancing Technologies - PET):

Cryptage

115. Le cryptage et les mécanismes connexes de sécurisation des informations sont des évolutions technologiques qui peuvent permettre d'améliorer la conformité avec au moins quelques-unes des obligations en matière de protection des données. En 1990, le cryptage était rarement utilisé pour protéger les données en dehors de l'administration et du secteur des services financiers. Aujourd'hui, il est présent dans tous les navigateurs Web et assure la transmission sécurisée de données relatives aux cartes de paiement à des serveurs de commerce en ligne; et la plupart des logiciels de messagerie électronique permettent le cryptage des messages avant leur transmission. Toutefois, les données relatives aux cartes de paiement continuent d'être dérobées à leurs utilisateurs via leurs propres machines au moyen de logiciels malveillants, et ce en raison d'une protection insuffisante au niveau du serveur; et le cryptage du courrier électronique est très rarement utilisé par les particuliers ou par la majorité des entreprises (ceci est en partie dû à un «cercle vicieux»: il ne peut en effet fonctionner que s'il est utilisé à la fois par l'expéditeur et par le destinataire d'un message).

116. Les systèmes d'exploitation traditionnels, et notamment Microsoft Windows, Linux et MacOS d'Apple, permettent le cryptage des données stockées, réduisant ainsi le risque que des voleurs aient accès aux données qui se trouvent sur des machines volées et sur médias amovibles tels que des CD et des clés USB. Cela est particulièrement important pour les appareils et ordinateurs portables, qui se perdent ou se volent facilement, et dont les données seraient facilement accessibles sans cryptage. Il serait possible pour les services Web «dématérialisés» (tels que Google Docs) de stocker et même de traiter des données uniquement sous leur forme cryptée, garantissant ainsi une limitation de l'accès aux propriétaires des données. Il est toutefois indispensable de mener des recherches plus approfondies sur l'«informatique tierce sécurisée» et sur les autres techniques susceptibles d'améliorer la protection des données à caractère personnel stockées dans les services dématérialisés.

117. Bien sûr, le cryptage doit être activé et configuré correctement pour protéger les données contre tout accès et toute modification non autorisés. Les plus grosses violations de données à caractère personnel de ces dernières années ont été possibles parce qu'aucune mesure de sécurité des données n'avait été prise ou que celles-ci avaient été mal configurées (citons, à titre d'exemple, le cas de l'administration britannique, qui a ainsi perdu en 2007 les dossiers d'allocations familiales de 25 millions de personnes, et celui des entreprises TJX, qui a vu les dossiers financiers de plusieurs millions de clients exposés en 2003 et en 2006). Ces infractions étaient également imputables à des déficiences au niveau des pratiques de conception et de gestion globales du système.

118. Le cryptage ne protège pas non plus les données contre l'utilisation des données cryptées à des fins telles que le marketing et le «profilage» par des organisations du secteur privé ou public, ni contre tout abus par des «initiés» qui sont autorisés à accéder aux informations non cryptées. Le Commissaire à l'information du Royaume-Uni a révélé qu'il existait un large marché criminel des données à caractère personnel volées

par le biais de la corruption ou de la fraude de membres du personnel ayant un accès légitime à de vastes bases de données au travail. Le cryptage est loin d'être la panacée en matière de protection de la vie privée.

Question connexe: notification des infractions à la sécurité

119. Nous pensons que la notification des violations des données n'est pas tant une question de recours qu'un renforcement du principe de sécurité dans la mesure où elle s'ajoute aux obligations des responsables des données en cas d'infraction à la sécurité et exige que ceux-ci informent les DPA et les personnes concernées dans certaines circonstances. Le non-respect de cette obligation de notification des violations des données doit être considéré comme une infraction au principe de protection des données, avec toutes les conséquences que cela implique. En d'autres termes, elle ne doit pas être considérée comme un recours, comme cela est parfois suggéré. En revanche, une notification efficace des violations des données contribuerait à renforcer l'efficacité des recours existants.

Désidentification et réidentification

120. En principe, il serait logique de penser que la désidentification ou l'anonymisation des données à caractère personnel par les responsables du traitement peut réduire le risque d'abus. Or dans la pratique, même dans le «vieil» environnement, cela n'était vrai que dans le cadre d'une protection permanente adaptée à la facilité avec laquelle les personnes concernées peuvent être réidentifées. Cela signifie imposer des limites strictes à l'accès à toutes les séries de données; contrôler les requêtes susceptibles de réidentifier collectivement des informations personnelles; et reconnaître le fait que toutes les failles au niveau de l'organisation, les vulnérabilités au niveau de la sécurité et les changements au niveau de la politique publique peuvent entraîner l'annulation des procédures de désidentification. Même alors, la désidentification reste difficile.

121. Dans le nouvel environnement sociotechnique mondial décrit dans le Document de travail n° 1, la disponibilité à grande échelle des données concernant la population, telles que les registres électoraux, les dossiers de crédit et les réseaux sociaux facilitera souvent (généralement) l'identification des personnes associées aux données, même si les informations personnelles évidentes telles que les noms, dates de naissance ou codes postaux ont été supprimées. Les progrès de l'informatique montrent que nous avons déjà dépassé le stade où les données «anonymisées» telles que l'historique des requêtes de recherche, critiques de films ou traitements médicaux pouvaient être mises à la disposition du plus grand nombre sans que cela ne puisse porter atteinte à la vie privée. Selon les termes de Paul Ohm: «l'anonymisation est une promesse non tenue et, dans le nouvel environnement, elle ne suffit pas à protéger la vie privée».[33] Comme nous l'avons déjà fait remarquer à la section IV.A (paragraphe 47), les graves problèmes découlant de la quasi-impossibilité de parvenir à une anonymisation complète des données à caractère personnel dans le nouvel environnement sociotechnique mondial sont l'un des plus grands défis dans le domaine de la protection des données, et devraient être au cœur du débat sur une révision du régime européen de protection des données. L'approche de base devrait consister à réduire au minimum absolu la collecte et même le stockage des données à caractère personnel dès le départ (cf. le principe

[33] Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization (note 14, supra).

allemand – mais aussi européen – de «minimisation des données» et le principe australien d'«anonymat»): une fois les données collectées et stockées, il est presque impossible de les supprimer ou (pour reprendre les termes de Paul Ohm) de véritablement les anonymiser de façon permanente.

Autres PET (P3P, accès en ligne pour la personne concernée, divers)

122. Au-delà du stockage et de la communication sécurisés des données, des technologies renforçant la protection de la vie privée (PET) ont été élaborées, qui permettent une meilleure application technologique de la législation en matière de protection des données. Elles peuvent à la fois accroître la transparence du traitement et minimiser ou éliminer les données à caractère personnel nécessaires pour effectuer des opérations spécifiques (réduisant ainsi le risque de vol par des personnes internes à l'organisation et de réutilisation des données à des fins non prévues). Toutefois, elles ont toutes leurs limites. Nous en examinerons quelques-unes.

P3P:

123. Les PET de base peuvent permettre la communication automatique des détails des opérations de traitement effectuées par les responsables, et un logiciel aide les personnes concernées à comprendre ces informations plus facilement que si elles devaient lire des politiques de vie privée légalistes complexes. Un système de ce type, appelé Plate-forme de préférences relatives à la protection de la vie privée (Platform for Privacy Preferences Project - P3P), a été créé à la fin des années 90. Le groupe de travail «Article 29» a indiqué que, dans un cadre juridique exécutoire, «la *P3P peut aider à normaliser les avertissements sur la vie privée. Bien que, en soi, elle n'offre pas de protection de la vie privée, elle pourrait, si elle est mise en œuvre, fortement améliorer la transparence et être utilisée pour appuyer les mesures prises pour améliorer la protection de la vie privée*».[34] La P3P a cependant été critiquée par des groupes militants, qui voient en elle un «*protocole complexe et confus qui rendra plus difficile encore la protection de la vie privée des utilisateurs de l'Internet*».[35] Son utilité reste sujette à question.

Accès en ligne pour la personne concernée:

124. Le droit d'accès prévu dans la directive doit généralement être exercé par les personnes concernées dans le cadre d'un échange de courrier long et onéreux avec les responsables du traitement. Les outils d'accès en ligne peuvent permettre aux personnes dûment authentifiées de consulter toutes les données les concernant que détient le responsable du traitement. Toutefois, il arrive fréquemment que les organisations stockent une partie des données à caractère personnel hors-ligne pour des raisons de sécurité très louables. Il est également à craindre que les individus ne soient obligés (ou simplement persuadés) d'autoriser des tiers, employeurs ou parents, par exemple à accéder à ces données. Si l'accès en ligne n'est pas assorti de garanties contre ce genre d'abus, il sera plus dangereux qu'utile.

---

34 WP 37, adopté le 21 novembre 2000

35 Electronic Privacy Information Center et Junkbusters (2000), Pretty Poor Privacy: An Assessment of P3P and Internet Privacy. Consultable à l'adresse suivante: http://epic.org/reports/prettypoorprivacy.html.

Divers:

125. Les PET plus sophistiquées du point de vue technologique possèdent des capacités contre-intuitives telles que la communication anonyme sur tout l'Internet public; l'argent électronique qui reflète le caractère anonyme de l'argent dans le monde matériel; et des authentifiants anonymes qui prouvent qu'une personne est autorisée à avoir accès à des ressources spécifiques sans révéler son identité. Une communication publiée en 2007 par la Commission européenne (COM/2007/0228) exhorte l'industrie, les autorités de réglementation et les autorités publiques à mieux informer les consommateurs et à recourir davantage aux PET afin d'améliorer *«la protection de la vie privée et aider à observer les règles relatives à la protection des données (…) complémentaire au cadre juridique et aux mécanismes de contrôles existants»*. Il demeure néanmoins difficile de déployer ces technologies sous une forme utilisable dans les logiciels de grande diffusion.

(ii) Gestion des identités respectueuse de la vie privée

126. La gestion des identités est un domaine technologique récent dont le but est d'aider les utilisateurs de l'Internet à gérer leurs relations avec les fournisseurs de services, notamment en prouvant qu'une personne est autorisée à accéder à des ressources spécifiques (par exemple, un compte client). Ces technologies ont un impact majeur sur la vie privée et peuvent être conçues de manière à faciliter le traçage et la surveillance centralisée de toutes les activités en ligne et hors ligne d'un individu; ou à réduire à un strict minimum les données à caractère personnel qui sont divulguées à des secondes ou tierces parties, permettant ainsi aux individus de bénéficier du même niveau de protection de la vie privée sur l'Internet que dans le monde réel.

127. Diverses solutions ont été proposées. Les systèmes centralisés initiaux (tels que le système Passport de Microsoft) présentaient des risques de graves atteintes à la vie privée, parmi lesquels un point de recoupement pour la surveillance des utilisateurs et un identificateur persistant qui pouvait être utilisé pour relier les informations relatives aux utilisateurs entre différents fournisseurs de services. Passport a été retiré face, notamment, aux inquiétudes des consommateurs concernant la protection de la vie privée. Les systèmes de gestion des identités «à authentification unique» et «fédérés», plus récents, tels que Open ID souffrent également de certains de ces problèmes mais sont pourtant largement utilisés par des entreprises telles que Yahoo! et Google.

128. Les systèmes de gestion des identités centrés sur l'utilisateur tels que CardSpace de Microsoft, Idemix d'IBM et les prototypes de projets du programme Privacy and Identity Management for Europe (PRIME) du 6e Programme-cadre assurent une meilleure protection de la vie privée. Ils permettent à l'utilisateur de contrôler ses propres informations d'identification et de minimiser les informations personnelles demandées par les fournisseurs de services. Grâce à ces systèmes, il devient impossible pour plusieurs organisations de relier entre elles des informations concernant des personnes spécifiques, et les utilisateurs peuvent fournir des «authentifiants» anonymes qui prouvent différentes caractéristiques (par exemple, l'autorisation de conduire ou d'acheter des produits réservés aux personnes d'un certain âge) sans révéler aucune information identificatoire. CardSpace est aujourd'hui intégré dans des versions récentes du système d'exploitation et du navigateur Web de Microsoft, bien que, jusqu'à présent, il n'ait pas été accueilli avec grand enthousiasme par les fournisseurs de services. Ces technologies sont donc très peu utilisées actuellement. Nous pensons que,

pour qu'elles aient plus de succès à l'avenir, il pourrait être nécessaire de renforcer la coordination au niveau des administrations et la normalisation, et de prendre des mesures en matière d'approvisionnement afin de donner aux consommateurs, aux entreprises et aux concepteurs de systèmes des incitations suffisantes.

129. La gestion de la relation vendeur (Vendor Relationship Management - VRM) est un concept connexe qui aide les individus à gérer leurs relations et les échanges de données à caractère personnel avec les entreprises plutôt que l'inverse, comme c'est souvent le cas avec les systèmes de gestion de la relation client (Customer Relationship Management - CRM). Les systèmes VRM qui permettent aux utilisateurs de stocker des données sur leurs propres systèmes protègent mieux la vie privée que ceux qui conservent les données sur des serveurs centraux. Mais encore une fois, ces systèmes n'en sont qu'au premier stade de leur développement.

130. De nombreux pays où il existe un système de carte d'identité nationale ajoutent une fonctionnalité de gestion des identités aux cartes afin de faciliter les relations en ligne entre les utilisateurs et l'administration et, dans certains cas, le secteur privé. Les systèmes les plus simples permettent aux utilisateurs de «prouver», physiquement et à distance, qu'ils sont détenteurs d'une carte et d'un numéro national d'identification correspondant, avec tout ce qu'implique pour la vie privée l'utilisation d'un identificateur général à long terme. Certaines cartes sont dotées de fonctionnalités de protection de la vie privée telles que le contrôle de l'accès (seules les parties autorisées peuvent utiliser les informations contenues dans la carte), l'utilisation d'identifiants spécifiques à un domaine (ce qui empêche la communication fortuite d'informations personnelles entre différents services administratifs), et la communication sélective des informations destinées à une application spécifique. L'Autriche et l'Allemagne sont les deux pays qui ont intégré le plus grand nombre de fonctionnalités de protection de la vie privée dans les cartes nationales. Pourtant, elles sont elles aussi confrontées aux failles inhérentes au système. Il convient d'ajouter que, à défaut de normalisation à l'échelon européen, il est peu probable que les systèmes nationaux aient un impact sur le marché mondial.

(iii) Évaluation des facteurs relatifs à la vie privée et prise en compte du respect de la vie privée dès la conception

131. Les technologies renforçant la protection de la vie privée et la gestion des identités respectueuse de la vie privée présentent un potentiel non négligeable pour la protection de la vie privée. Néanmoins, le plus important est de convaincre les décideurs et les chefs d'entreprise d'accorder l'attention qu'il se doit aux répercussions des nouveaux systèmes d'information sur la protection de la vie privée, et ce avant qu'ils ne soient mis en service. La quantité de données à caractère personnel collectées et traitées peut être considérablement influencée par des détails décidés bien longtemps avant que les architectes et les programmateurs des systèmes ne commencent à fabriquer de nouvelles applications de bases de données. Il est beaucoup plus facile de produire des systèmes respectueux de la vie privée si les problèmes de protection des données sont pris en compte dès le début de la phase de conception, en accordant une attention particulière à la minimisation et à la sécurité des données. L'utilisation de systèmes contenant des données à caractère personnel sensibles concernant des millions ou des dizaines de millions de personnes, auxquelles ont accès des centaines de milliers d'employés et qui peuvent être conservées pendant de longues périodes (comme dans de nombreuses

applications d'administration en ligne), peut conduire à des violations de la vie privée, auxquelles il est très difficile de remédier a posteriori.

132. Deux mesures spécifiques prises pour tenter d'inciter les organisations à tenir compte de la vie privée dès la première phase de planification valent la peine d'être mentionnées. Les évaluations des facteurs relatifs à la vie privée (Privacy Impact Assessments - PIA) sont désormais obligatoires sur de nombreux territoires, y compris aux États-Unis, et exigent des agences gouvernementales qu'elles dressent une évaluation des risques des nouvelles politiques en matière de vie privée avant que les systèmes ne soient mis en service. Comme nous l'avons indiqué précédemment, le Gouvernement australien propose également de doter le Commissaire à la vie privée du pouvoir d'imposer ces évaluations aux agences gouvernementales. Le Commissaire britannique à l'information encourage l'administration et les entreprises à procéder à des évaluations afin de régler les problèmes liés au respect de la vie privée dès le début des projets, en utilisant un processus systématique qui gère le risque et qui tienne compte du point de vue de toutes les personnes concernées par les nouveaux systèmes. Privacy By Design (prise en compte du respect de la vie privée dès la conception) est une approche élaborée par le Commissaire à la protection de la vie privée de l'Ontario, qui encourage la production et l'exploitation de systèmes qui minimisent la collecte, le stockage, le traitement et la conservation des données à caractère personnel. Elle englobe les politiques et les pratiques des entreprises ainsi que les détails des technologies utilisées. Elle utilise les évaluations des facteurs relatifs à la vie privée tout au long du cycle de vie d'un système, depuis la conception initiale, lors des mises à niveau, et jusqu'à sa mise hors service. Pour être efficace, cette méthode doit avoir l'appui des cadres dirigeants, qui doivent veiller à ce que les besoins en matière de respect de la vie privée soient pris en compte dans les analyses de rentabilité des nouveaux systèmes et à ce qu'ils soient satisfaits tout au long du cycle de vie du système.

(iv) Contrôle de la protection de la vie privée par l'utilisateur et paramètres par défaut

133. De nombreux sites Internet donnent aux utilisateurs des informations détaillées sur la quantité de données à caractère personnel qui sont collectées et sur la façon dont les données sont traitées, et leur donnent la possibilité de contrôler ces paramètres. Le protocole P3P a été conçu pour spécifier aux navigateurs Web les pratiques des différents sites en matière de vie privée, mais ces fonctionnalités n'ont pas été utilisées à grande échelle, notamment en raison de la controverse au sujet des politiques de paramétrage par défaut et d'autres problèmes de définitions. Les navigateurs proposent souvent la fonctionnalité «bloquer les cookies» qui permet de gérer les informations échangées avec les sites (bien que certains sites limitent l'accès lorsque tous les cookies sont bloqués). Les utilisateurs finaux font un usage très limité de la fonctionnalité de gestion des cookies, dès lors les paramètres par défaut (souvent permissifs) sur les navigateurs ont un impact non négligeable sur le niveau général de protection de la vie privée.

134. La plupart des réseaux publicitaires en ligne se conforment au code de déontologie du Bureau de la publicité sur Internet (Internet Advertising Bureau) concernant le «ciblage des publicités en fonction du comportement», qui stipule que les utilisateurs doivent avoir la possibilité de refuser d'être soumis à la publicité sur la base de leur comportement de navigation antérieur. Google permet aux utilisateurs de mettre à jour le profil de leurs intérêts établi lors de la navigation sur les sites du réseau AdSense. Les

sites de réseaux sociaux tels que Facebook proposent des options détaillées pour contrôler l'accès aux profils individuels et au contenu partagé (bien que les chercheurs aient constaté que ces contrôles sont souvent difficiles à utiliser et ne sont pas suffisamment visibles). Les paramètres d'origine sont rarement modifiés par les utilisateurs et ont donc un impact significatif (ce qui a conduit le groupe de travail «Article 29» à proposer, dans un avis publié récemment (5/2009), qu'ils protègent la vie privée par défaut.

135. En règle générale, bien que «l'habilitation de l'utilisateur» ait été un axe clé de la politique d'amélioration de la protection de la vie privée en ligne depuis les débuts de la mondialisation de la toile, ces outils sont souvent trop complexes pour les utilisateurs non techniciens. Une étude d'économie comportementale menée récemment a également révélé que peu de personnes avaient le temps ou l'envie de se lancer régulièrement dans des analyses de risques approfondies sur les dangers potentiels abstraits de futures violations de la vie privée, limitant ainsi l'efficacité de ces solutions isolément.

136.

(iii) Autoréglementation et coréglementation sectorielles

137. La directive, en son article 27, encourage l'utilisation de codes de déontologie sectoriels, aux niveaux national et européen. Le WP29 a donné des directives détaillées sur les domaines qui doivent être couverts par ces codes, et sur la «valeur ajoutée» qu'ils doivent apporter.[36] Le statut exact des codes dont la conformité avec la législation nationale pertinente est «établie» est laissé relativement ouvert: la directive ne demande pas que l'évaluation équivale à une «approbation» formelle de ces codes ni qu'il leur soit conféré un statut officiel dans les systèmes juridiques des États membres, et les pratiques varient. Ainsi, aux Pays-Bas, l'«approbation» d'un code par l'autorité chargée de la protection des données ne rend pas celui-ci obligatoire pour les tribunaux tandis que, en Irlande, les codes peuvent être intégrés de façon plus formelle dans le régime légal et devenir juridiquement contraignants. Toutefois, quel que soit le statut officiel exact d'un code, dès lors qu'il a été déclaré conforme à la loi, il joue un rôle important, au moins quasi-législatif. En ce sens, la référence explicite à ces codes dans la directive confirme une tendance plus générale à une confusion des normes légales et des normes *soi-disant* d'autoréglementation mais en réalité quasi-législatives.[37] Les codes de déontologie se muent donc lentement en systèmes plus formels de la législation subsidiaire, comme en atteste l'établissement de «normes simplifiées» par l'autorité française de protection des données. Dans le secteur public, l'accent semble être mis sur la réglementation subsidiaire, dans le secteur privé sur les codes de déontologie (bien que, au Royaume-Uni, les codes de déontologie n'ayant pas force obligatoire et les «protocoles» soient aussi – ce qui est contestable – largement utilisés dans le secteur public, et pour le partage de données entre organismes publics et entre organismes publics et privés). Dans les deux cas, les règles sont souvent le résultat d'une étroite collaboration entre les autorités de réglementation (ministères, autorités chargées de la protection des données, etc.) et le(s) secteur(s) concerné(s), généralement (mais malheureusement pas toujours) avec la contribution de groupes représentant d'autres parties intéressées (souvent les principales parties intéressées) tels que consommateurs, patients, etc.

138. L'approche des codes adoptée par le WP29 a été appliquée au système le plus récent de mesures similaires au niveau des entreprises, les «règles d'entreprise contraignantes» (BCR).[38]

139. Nous n'analyserons pas ici l'utilité générale des mesures d'autoréglementation (ou quasi-autoréglementation), ou des codes de déontologie et des BCR de manière

---

[36] Voir en particulier le document de travail du WP29 Évaluation des codes d'autoréglementation sectoriels: quand peut-on dire qu'ils contribuent utilement à la protection des données dans un pays tiers? (WP07 du 14 janvier 1998). Bien que ce document aborde la question des conditions auxquelles un code peut être considéré comme offrant une protection «adéquate» pour permettre les transferts de données vers des pays tiers qui ne disposent pas de lois adéquates en matière de protection des données, les critères appliqués à ces codes sont tout aussi pertinents pour l'évaluation des codes des États membres et des codes européens. Les codes de déontologie sont traités en détail dans l'ouvrage de Douwe Korff, Data Protection Law In Practice In The EU, FEDMA/DMA, Bruxelles/New York, 2005, pp. 159 à 166; le texte ci-dessus s'inspire de ce chapitre du livre.

[37] Voir la section (rédigée par le chef d'équipe de la présente étude) relative aux «*Regulatory Trends and New Media»* dans l'étude de la Commission The Future of Media and Advertising (généralement appelée étude Admedia), DG XIII/E, novembre 1995, Partie D.1.

[38] Voir document de travail du WP29 Transferts de données personnelles vers des pays tiers: Application de l'article 26 (2) de la directive de l'UE relative à la protection des données aux règles d'entreprises contraignantes applicables aux transferts internationaux de données (WP77 du 3 juin 2003).

générale. Nous nous contenterons de faire remarquer que, au niveau européen, ce processus a connu un succès limité, le Code de déontologie européen en matière d'utilisation de données à caractère personnel dans le marketing direct de la FEDMA en étant le principal exemple positif (bien que, même à cet égard, les règles supplémentaires concernant le marketing aux mineurs n'aient pas encore été adoptées ou approuvées, après de nombreuses années de discussion). L'industrie a en effet reproché au WP29 et à la Commission leur lenteur et leur attention méticuleuse qui, selon elle, sont la principale raison pour laquelle un nombre si limité de projets de codes ont été soumis à leur approbation. Les règles d'entreprise contraignantes ont été soumises pour approbation par les autorités nationales chargées de la protection des données, essentiellement pour ce qui concerne les données relatives au personnel des multinationales - jusqu'à présent, elles n'ont pas offert une protection très solide aux autres personnes concernées, telles que les clients.

140. En dehors de l'UE/EEE, les codes ont joué un rôle très limité en Australie et à Hong Kong. D'autre part, un certain nombre de «lignes directrices» sectorielles (par exemple, les lignes directrices du METI) ont joué et continuent de jouer un rôle clé au Japon – mais elles ne sont pas souvent élaborées par des personnes appartenant au secteur, elles sont plutôt imposées par le Ministère.

141. Nous pensons que, d'une part, il faut encourager les règles sectorielles ou les règles internes des entreprises car elles permettent de clarifier l'application des règles des directives, souvent vagues et complexes, à des situations concrètes. D'autre part, elles ne doivent pas être utilisées pour permettre aux responsables du traitement, ou à des groupes de responsables, de contourner les obligations de base des directives en interprétant de façon «créative» ou en tournant les règles des instruments européens. L'élaboration de ces règles nécessitera donc immanquablement des efforts considérables et des consultations intensives – et donc du temps. Il serait néanmoins utile, dans tout processus de révision de la directive, de discuter des moyens de renforcer l'efficacité de ce processus et de le rendre moins difficile pour le WP29. Peut-être le système utilisé dans le cadre du Label européen de protection de la vie privée, qui fait l'objet de la sous-section suivante, peut-il être utile. Dans ce système, des experts indépendants agréés sont chargés des travaux préparatoires (payés par les parties concernées privées qui, dans le cas des codes, seraient l'industrie), et font l'objet d'une évaluation très rigoureuse et (si celle-ci est favorable) d'une accréditation par un organisme officiel auquel participent les autorités nationales chargées de la protection des données. Comme nous l'expliquons dans la sous-section suivante, il pourrait être intéressant d'envisager de créer un bureau spécial des DPA de l'UE/EEE, qui traiterait ce genre d'affaires sur une base quasi-commerciale (ou du moins d'autofinancement intégral). Si l'idée avancée dans cette sous-section est jugée digne d'intérêt, elle pourrait se révéler utile pour l'élaboration des codes de déontologie et des BCR.

(iv) Labels de protection de la vie privée

142. Les labels de protection de la vie privée ont mauvaise presse: voir les critiques virulentes mais justifiées de Trust Guard, TRUST-e, BBB, etc., dans le rapport concernant les États-Unis (où sont nés la plupart des labels mondiaux).[39] Comme nous l'expliquons, le principal problème des labels volontaires est celui des incitations:[40]

[39] Chris Hoofnagle, Country Report on the USA, pp. 46 à 48, qui contient des références détaillées. Voir le rapport concernant le Japon, qui fait mention de critiques similaires de la marque de protection de la vie privée

> Les programmes de labels de protection de la vie privée souffrent d'un problème fondamental d'incitation: certaines entreprises qui comptent de nombreux utilisateurs sont peu encouragées à faire certifier leurs pratiques en matière de protection de la vie privée. Par exemple, Google et MySpace n'ont pas de labels TRUSTe. Inversement, des sites Internet plus marginaux cherchant à élargir leur base d'utilisateurs sont fortement incités à obtenir une certification. TRUSTe et d'autres programmes de labels tirent leurs revenus de la délivrance des labels et doivent donc trouver un équilibre entre leur objectif, qui est de garantir des pratiques responsables, et la tentation de générer des revenus supplémentaires grâce à des entreprises aux pratiques marginales.

143. Une initiative a déjà entreprise pour tenter de régler ce problème, dans une certaine mesure, dans le cadre de la loi relative à la protection des données du *Land* allemand de Schleswig-Holstein. Dans ce *Land*, la loi demande expressément aux organismes publics d'accorder la préférence, pour leur approvisionnement, aux produits et services informatiques dont la conformité à la loi locale en la matière a été certifiée par un label délivré par l'autorité chargée de la protection des données du Schleswig-Holstein, l'ULD.[41] Il a été jugé que cette mesure ne constituait pas une restriction abusive à la concurrence loyale – au contraire, elle signifie que les produits et services conformes à la loi peuvent être compétitifs face à leurs concurrents moins respectueux de la vie privée.

144. Le système utilisé dans le Schleswig-Holstein a servi de modèle pour la création récente d'un Label européen de protection de la vie privée, *EuroPriSe*, géré par l'ULD mais en coopération avec d'autres DPA, françaises et espagnoles en particulier. EuroPriSe a été créé sur la base d'un projet pilote financé par la Commission européenne dans le cadre de son programme «e-TEN». Le projet a reçu la plus haute note possible de la part des évaluateurs européens, qui l'ont jugé «très bon» pour le critère «contribue aux politiques de l'UE en matière de protection des données, de conformité et d'application et concerne directement les politiques européennes en termes de fiabilité et de sécurité». Par ailleurs, le label EuroPriSe a été accueilli favorablement par la Commissaire (alors en place) Viviane Reding et a reçu le plein appui du Superviseur à la protection des données de l'UE, Peter Hustinx. Un rapport sur la protection de la vie privée à l'ère numérique (*La vie privée à l'heure des mémoires numériques*), publié au mois de juin de cette année par la Commission des lois du Sénat français et considéré comme l'une des plus importantes initiatives législatives en France dans le domaine de la protection de la vie privée et de la protection des données depuis la mise en œuvre de la directive européenne de 2004 sur la protection des données, vante également les mérites du label EuroPriSe et déclare que cette initiative est un exemple pour les systèmes nationaux et qu'elle doit être poussée plus avant.

145. EuroPriSe devrait faire l'objet de discussions plus approfondies dans le cadre de la révision de la directive. Nous pensons qu'il serait très utile d'inclure dans la directive une règle similaire à celle mise en place par le Schleswig-Holstein, qui demande aux autorités publiques des États membres et aux organes de l'UE, d'acquérir, lorsque cela est possible, des produits et services respectueux de la vie privée. Si cela ne peut pas

---

dans ce pays.

[40] *Idem*, p. 48.

[41] Voir: https://www.datenschutzzentrum.de/guetesiegel/index.htm ou, pour des résumés en anglais: https://www.datenschutzzentrum.de/faq/guetesiegel_engl.htm.

être stipulé officiellement dans la directive, rien n'interdit d'encourager d'autres manières ce type de règles d'approvisionnement, par exemple par l'adoption d'une telle approche par la Commission et les États membres dans les politiques. En principe (mais sous réserve de la remarque ci-dessous, et de l'avertissement plus général au paragraphe 146), les règles relatives à l'approvisionnement et les politiques de ce type sont celles qui, jusqu'à présent, offrent la meilleure incitation à une protection des données solide et efficace et à un strict respect des règles relatives à la protection des données de la part des organismes commerciaux qui proposent des produits et services sensibles du point de vue de la protection de la vie privée.

Remarque: Toute mesure de ce type doit bien sûr tenir compte des législations européennes en matière de concurrence et de libre circulation des biens et des services (ainsi que des règles de l'OMC). Ces systèmes doivent être conçus de manière à éviter tout risque d'effet contraire à la concurrence ou d'influence déloyale sur les échanges commerciaux entre les États membres. Or, le système mis en place dans le Schleswig-Holstein montre que cela est possible.

146. Une autre caractéristique du label EuroPriSe (déjà mentionné) est la création d'une autorité de certification chargée de la délivrance des labels, ainsi que l'accréditation d'experts indépendants spécialement formés à cet effet et ayant fait leurs preuves, qui procèdent à l'évaluation principale des produits. L'autorité de certification est essentiellement constituée des DPA participants, et les experts suivent une formation rigoureuse et sont soumis à un examen très strict. Le système se finance lui-même au travers du paiement de droits par les entreprises qui sollicitent le label (qui paient également les experts mais de façon séparée, suivant des arrangements individuels). Comme nous l'avons fait remarquer ci-dessus, dans le *Land* du Schleswig-Holstein, la DPA est officiellement autorisée à agir de la sorte. Au niveau européen, cela s'est avéré plus compliqué dans le sens où les DPA nationales ne peuvent pas toutes participer officiellement au système, selon la législation en vigueur dans leur pays. Lors de la révision de la directive, la participation à ce système pourrait être mentionnée dans la liste des missions des DPA (cf. article 28 actuel).

147. Il pourrait en effet être utile d'envisager la création d'un organisme ou d'un bureau spécial regroupant les DPA de l'UE/EEE, qui travaillerait en étroite collaboration avec le WP29 et la Commission et qui traiterait de ce genre d'affaires sur une base quasi-commerciale (ou du moins sur la base d'un autofinancement total), de façon très analogue au système ULD. Comme nous l'avons déjà évoqué, cet organisme ou bureau pourrait être chargé non seulement du Label européen de protection de la vie privée mais peut-être aussi de la préparation de codes de déontologie européens, ainsi que des règles d'entreprise contraignantes – les premiers travaux seraient laissés aux experts indépendants (mais évalués et dûment accrédités), l'évaluation finale et la certification étant effectuées par le bureau sur une base semi-commerciale (autofinancement).

Remarque: La question du statut de cet organisme, et de ses liens officiels avec les DPA nationales et les organes de l'UE, est une question complexe, comme constaté dans le projet pilote «e-TEN» d'*EuroPriSe*. Toutefois, la création d'organismes nationaux de certification et d'accréditation est un phénomène très fréquent en Europe. En effet, il existe un règlement publié récemment, Règlement (765/08) relatif à l'accréditation et à la surveillance du marché, qui, pour la première fois, dès le 1er janvier 2010, fournira un cadre juridique pour les services d'accréditation à travers l'Europe, et définira les conditions de fonctionnement du système d'accréditation pour les évaluations de la conformité volontaires et les évaluations requises par la loi. Le principe de base de certification et d'accréditation du Label européen de protection de la vie privée pourrait être examiné dans ce cadre plus large et s'en inspirer.

148. Il convient cependant de se montrer prudent à cet égard. Tout dépend de la sévérité des conditions imposées par le label et de sa mise en œuvre. Le système EuroPriSe obtient de bons résultats sur ces deux points, précisément parce que les critères appliqués sont très stricts et définis par les autorités chargées de la protection des données dans des pays qui offrent une protection efficace, et parce que le système est essentiellement géré par les DPA, qui ne sont pas motivées par la nécessité d'optimiser le rendement ou de faire des bénéfices (dans de nombreux pays, en effet, la loi interdit aux DPA de participer à des activités lucratives). Il est peu probable que les systèmes qui ne prévoient pas ce genre de garanties se conforment réellement aux normes de l'UE/EEE.

149. Il s'agit bien entendu de simples suggestions. Néanmoins, nous sommes convaincus qu'il sera important, dans le nouvel environnement socio-technique, de mettre en place de nouveaux systèmes pouvant traiter de manière efficace et pas trop bureaucratique les mesures destinées à garantir une protection des données appropriée dans des secteurs, entreprises (multinationales) ou contextes spécifiques. Mais contrairement aux labels (etc.) précédents, largement discrédités, ces systèmes doivent (comme le système EuroPriSe) être étroitement liés aux autorités de réglementation officielles et ne pas être motivés par des intérêts commerciaux.

(v) Conclusion

150. Nous craignons qu'il n'existe pas de «balle magique» pour garantir une protection adéquate des données. La loi est, par nature, souvent difficile à interpréter et à appliquer, et soit trop vague soit trop rigide, tandis que les mesures supplémentaires et alternatives (non juridiques ou quasi-juridiques) ont montré de graves lacunes, souvent intrinsèques. Certaines mesures et technologies se sont révélées n'être que des cache-misère. Toute révision doit être fondée sur une évaluation réaliste et techniquement correcte de ces mesures. Cela ne veut pas dire qu'elles doivent être rejetées d'emblée. Elles devront toutefois être soumises à un examen minutieux par des experts techniques et juridiques: comme l'indique clairement l'article de Paul Ohm au sujet de la désidentification et de la réidentification (un sujet crucial), les législateurs et décideurs du monde entier ont souvent mal compris les nouvelles technologies et leurs conséquences.

151. De manière générale, comme nous l'avons expliqué dans les dernières sous-sections, la question des incitations et de l'aspect économique de la protection de la vie privée et de la sécurité des données est une question centrale. Si la loi rend économiquement attrayante la protection de la vie privée (par exemple, via des incitations en termes d'approvisionnement, associées à la délivrance de labels sérieux de protection de la vie privée, comme nous l'avons évoqué), ou si elle punit les violations des règles en matière de protection et de sécurité des données (en attribuant la responsabilité de la protection à ceux qui sont le mieux placés pour la garantir plutôt qu'en les autorisant à en faire assumer le coût par les autres, par exemple les consommateurs), alors la protection des données a peut-être un avenir. Nous pensons que cela demande une combinaison harmonieuse de lois et de règles et de mécanismes d'autoréglementation. Nous espérons que les considérations ci-dessus susciteront une réflexion à ce sujet.

- o – O – o -

Experts permanents:
Douwe Korff, chef d'équipe
Ian Brown, co-chef d'équipe

Experts spéciaux:
Peter Blume
Graham Greenleaf
Chris Hoofnagle
Lilian Mitrou
Filip Pospíšil
Helena Svatošová
Marek Tichy

Conseillers:
Ross Anderson
Caspar Bowden
Katrin Nyman-Metcalf
Paul Whitehouse

ANNEXES :

- Document de travail n°1 **The challenges to European data protection laws and principles**
  (Un aperçu des évolutions sociales et techniques au niveau mondial et des défis qu'elles posent en matière de protection des données)

- Document de travail n°2 **Data protection laws in the EU**
  (Une étude comparative-analytique des difficultés rencontrées par la législation pour faire face aux défis que posent les évolutions sociales et techniques au niveau mondial)

- Rapports par pays **Pays européens :**

  – Allemagne
  – Danemark
  – France
  – Grèce
  – République tchèque
  – Royaume-Uni

  Pays et territoires non européens :

  – Australie
  – États-Unis :
    ✓ Niveau fédéral
    ✓ Californie
    ✓ New Jersey
  – Hong-Kong
  – Inde
  – Japon

- Tableau comparatif des législations nationales

- o – O – o -

NB: Outre les annexes ci-dessus, qui font officiellement partie de l'étude, les auteurs ont également transmis à la Commission plusieurs autres rapports, mentionnés dans le texte ou dans des notes en bas de page, auxquels ont participé un ou plusieurs membres de l'équipe d'experts et dont ils ont donc pu s'inspirer (sauf si la Commission était déjà en possession de ces rapports).