Commission Nationale pour la Protection des Données

Rapport Annuel 2008

COMMISSION NATIONALE
POUR LA PROTECTION
DES DONNÉES

Rapport annuel 2008

Mission

Veiller à l'application des lois qui protègent les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée et leurs données à caractère personnel.

Superviser et assurer la transparence par :

- l'examen préalable des traitements soumis à autorisation ;
- la publicité réalisée au moyen du registre des traitements notifiés ;
- les investigations suite à des plaintes ou de sa propre initiative.

Informer et guider avec :

- la sensibilisation du public aux risques potentiels ;
- les renseignements concernant les droits des citoyens et les obligations des responsables des traitements de données ;
- l'explication des règles légales.

Conseiller et coopérer à travers :

- les avis relatifs aux projets de loi et mesures réglementaires ou administratives ;
- les suggestions et recommandations adressées au gouvernement, notamment au sujet des conséquences de l'évolution des technologies ;
- l'approbation de codes de conduite sectoriels, la promotion des bonnes pratiques et la publication de lignes d'orientation thématiques.

Table des matières

1 Avant-propos 6

2 Les activités en 2008 8

2.1. Conseil et guidance 8

2.2 Supervision de l'application de la loi 9

2.3 Information du public 11

2.4 Avis et recommandations 13

2.5 Participation aux travaux européens 13

3 Les temps forts de 2008 17

3.1 Cybersurveillance des salariés par l'employeur 17

3.2 La prise en charge des formalités légales 17

3.3 Quelques sujets délicats et arbitrages ardus 19

3.4 Investigations 25

4 Perspectives 27

5 Ressources, structures et fonctionnement de la Commission nationale 30

5.1 Rapport de gestion relatif aux comptes de l'exercice 2008 30

5.2 Renouvellement du mandat de la Commission nationale 31

5.3 Personnel et services mis en place 31

5.4 Bureaux 32

5.5 Organigramme de la Commission nationale 33

6 La Commission nationale en chiffres 34

ANNEXES :

Avis et décisions

- Avis de la Commission nationale pour la protection des données concernant le projet de loi n°5802 portant sur la libre circulation des personnes et l'immigration 37
- Délibération n° 166/2008 du 20 juin 2008 de la Commission nationale pour la protection des données relative à la demande de l'Institut Luxembourgeois de Régulation concernant la procédure « article 41 » de la loi du 2 août 2002 42
- Avis de la Commission nationale pour la protection des données relatif à l'avant-projet grand-ducal concernant la saisie et le traitement des données nominatives des élèves 45
- Avis de la Commission nationale pour la protection des données concernant le projet de règlement grand-ducal relatif à la fixation des conditions et modalités de délivrance de la documentation cadastrale 47
- Avis de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal autorisant la mise en œuvre des traitements de données à caractère personnel nécessaires à l'exécution de la loi du 29 août 2008 sur la libre circulation des personnes et l'immigration et déterminant les données à caractère personnel auxquelles le ministre ayant l'Immigration dans ses attributions peut accéder aux fins d'effectuer les contrôles prévus par la loi 50
- Avis de la Commission nationale pour la protection des données relatif à l'interprétation et l'application de l'article 20 du projet de loi N°5859 portant modification de la loi électorale modifiée du 18 février 2003 52
- Avis de la Commission nationale pour la protection des données relatif à l'avant-projet de loi modifiant la loi modifiée du 29 avril 1983 concernant l'exercice des professions de médecin, de médecin-dentiste et de médecin-vétérinaire 54
- Avis relatif à l'avant-projet de règlement grand-ducal déterminant les procédés à suivre pour constater la mort en vue d'un prélèvement 56
- Avis sur l'enregistrement d'appels téléphoniques d'urgence en vertu de l'article 4 paragraphe (3) de la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques 58
- Décision type concernant la surveillance informatique 60

Participations aux travaux européens

- Documents adoptés par le groupe « Article 29 » en 2008 73
- Article 29 Working Party – « Programme de travail 2008-2009 » 74
- Article 29 Working Party : Document de travail 1/2008 sur la protection des données à caractère personnel de l'enfant 77
- Article 29 Working Party : Avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche 90
- Article 29 Working Party : Avis 3/2008 sur le projet de norme internationale de protection de la vie privée du code mondial antidopage 115
- International Working Group on Data Protection in Telecommunications Report and Guidance on Privacy in Social Network Services 122
- International Working Group on Data Protection in Telecommunications Recommendation on the Implementation and Application of the Council of Europe Convention No. 185 on Cybercrime (a.k.a. "Budapest Convention") 132

1 Avant-propos

Le 1er novembre 2008, la Commission nationale pour la Protection des Données a fêté son sixième anniversaire. Au terme de leur premier mandat, ses membres ont pu se rendre compte du chemin parcouru mais aussi des difficultés rencontrées pour gagner une certaine reconnaissance auprès des responsables et obtenir un peu de visibilité auprès du public.

La directive 95/46/CE du 24 octobre 1995 prévoit l'institution au sein des Etats membres (et de ceux de l'EEE) d'une autorité de contrôle exerçant la surveillance de l'application de la loi aussi bien au sein des institutions, organismes et administrations publiques que par les entreprises privées, commerçants, professions libérales, dans le secteur associatif et des loisirs et sur Internet.

Ainsi la mission de la Commission nationale se définit comme suit :

- le contrôle du respect de la loi et la vérification des formalités préalables qu'elle prévoit à charge des responsables de fichiers;
- la promotion de bonnes pratiques en matière de protection de données à caractère personnel et la veille de l'évolution technologique;
- la prise de position (examen des demandes d'autorisation ou des projets de loi et règlements) sur le juste équilibre entre les libertés et droits fondamentaux des citoyens et une liberté d'action considérée comme étant raisonnable pour le bon fonctionnement des entreprises et administrations publiques;
- la sensibilisation des citoyens quant aux atteintes éventuelles à leur vie privée et l'information quant à leurs droits et aux précautions à prendre pour se protéger.

Au cours des premières années de son existence, l'activité de la Commission nationale s'est focalisée sur les formalités préalables (autorisations et notifications), la mise en place des procédures ainsi que sur l'organisation interne.

En simplifiant la législation en vigueur, la loi du 27 juillet 2007 est venue clôturer cette phase dans la vie de la Commission nationale. Ainsi, le législateur a repris à son compte les principales recommandations de la Commission nationale en vue d'un allègement des formalités visant à rendre possible un effort accru de guidance des entreprises et administrations et d'investigations sur le terrain, grâce aussi à une augmentation sensible des effectifs en personnel. Aujourd'hui, la CNPD se compose, outre ses trois membres, de trois juristes, de quatre collaborateurs administratifs ainsi que d'un attaché à la communication et à la documentation.

L'activité de la Commission nationale au cours des dernières années a par ailleurs été marquée également par une forte participation aux travaux européens, dominés par des dossiers complexes et technologiques. Cet engagement a été nécessaire pour appréhender la matière dans toute son envergure et complexité.

C'est d'ailleurs de cette collaboration internationale qu'est venue la conviction que la communication (aussi bien en direction des entreprises, des pouvoirs publics que des citoyens) joue un rôle clé dans l'action des autorités de contrôle pour rendre la protection des données plus effective.

Aujourd'hui, les membres de la Commission nationale estiment que l'autorité a atteint sa maturité en trouvant un équilibre entre ses différentes tâches et attributions qui sont :

- le travail administratif ;
- la sensibilisation du public ;
- la guidance des acteurs privés et publics ;
- le traitement des plaintes et les contrôles et investigations sur le terrain ;
- l'émission d'avis et de prises de position sur des sujets relatifs à la protection des données à caractère personnel.

La Commission nationale s'apprête d'ailleurs à venir à bout de l'engorgement qu'elle a initialement connu au niveau du traitement des formalités administratives qui lui ont été soumises depuis 2003. Le fait que ce retard n'ait pu être résorbé plus tôt s'explique par le fait que la réforme de la loi mais aussi le renforcement de ses effectifs sont arrivés plus tard qu'initialement prévus.

Ainsi, à l'avenir, la Commission nationale sera en mesure de prendre encore mieux en charge les demandes lui soumises par les citoyens, d'analyser des cas concrets avec une plus grande expertise et s'atteler à des contrôles et investigations sur les lieux tout en améliorant la guidance des acteurs privés et publics et en relançant son travail d'information par l'élaboration de nouvelles brochures et autres supports de vulgarisation et par un prochain « lifting » de son site Internet.

***

Luxembourg, le 3 avril 2009

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

2 Les activités en 2008

Plusieurs axes ont caractérisé le travail de la Commission nationale au courant de l'année 2008 :

- le conseil et la guidance des acteurs ;
- la supervision du respect de la loi avec notamment le traitement d'un nombre important de dossiers d'autorisations au cours de l'année ;
- les initiatives d'information et de communication, traduites par la poursuite des efforts d'information et de sensibilisation, et ce aussi bien du grand public que des milieux professionnels;
- la participation aux travaux sur le plan européen.

2.1 Conseil et guidance

2.1.1 Concertation avec les organisations représentatives sectorielles, les principaux acteurs économiques, l'Etat et les organismes publics

La Commission nationale a poursuivi sa politique de dialogue et de concertation avec les acteurs publics et privés, que ce soit à propos de questions spécifiques touchant un secteur ou de projets poursuivis par un département ministériel ou, de façon plus générale, afin d'échanger ses vues au sujet de l'application des principes de la protection des données dans les pratiques et procédures usuelles des activités considérées.

La Commission nationale a régulièrement participé, comme par le passé, aux travaux du Comité National d'Ethique de Recherche (CNER) et du Comité National pour la Simplification Administrative en faveur des Entreprises (CNSAE), et fourni ses multiples recommandations au cours de ces travaux.

Elle était par ailleurs en lien à propos de différents dossiers avec les ministères suivants : ministère des Affaires étrangères et de l'Immigration, ministère de la Fonction publique et de la Réforme administrative, ministère des Classes moyennes, du Tourisme et du Logement, ministère d'Etat, ministère de l'Economie et du Commerce extérieur, ministère de l'Education nationale et de la Formation professionnelle ; ainsi qu'avec diverses administrations et organismes publics comme l'administration des contributions directes, l'administration de l'emploi, le CEPS-INSTEAD, la Commission consultative des droits de l'Homme, le Centre de Recherche Publique (CRP) Henri Tudor et CRP Santé ou encore Lux-Development.

Le nombre de réunions avec le secteur public (52 contre 56 l'année précédente) s'est ainsi maintenu à un niveau élevé en parallèle avec celui des entrevues avec les représentations d'importantes entreprises privées nationales et multinationales et leurs organisations représentatives (du secteur financier notamment) ce qui traduit l'accent mis sur les efforts de promotion des bonnes pratiques et de guidance constructive. Le nombre de réunions avec le secteur privé a été de 44 en 2008.

2.1.2 Séances d'information, conférences, exposés

En 2008, la Commission nationale a assuré 11 séances d'information, conférences et exposés contre 14 en 2007.

Un accent particulier a été mis sur des présentations de la loi révisée.

Citons les formations assurées à l'INAP (Institut national de l'administration publique), ainsi que les présentations et conférences assurées en collaboration avec la Chambre des métiers ou le FNCTTFEL, ou encore lors du LUSI-Day 2008.

2.1.3 Demandes de renseignements

Le nombre de demandes de renseignements soumis en 2008 à la Commission nationale est resté à un niveau élevé mais stable, avec de nouveau quelque 1.600 demandes de renseignements par téléphone. Au total les demandes de renseignements se chiffrent pour 2008 à 1.724 contre 2018 demandes enregistrées en 2007.

Une optimisation continue, tant sur le plan organisationnel qu'au niveau de la qualité des réponses données, permet cependant de traiter désormais les demandes plus rapidement (et certainement aussi de manière de plus en plus pointue).

2.2 Supervision de l'application de la loi

2.2.1 Formalités préalables

2.2.1.1 Généralités

Le nombre de notifications ordinaires a diminué en 2008 à la suite des modifications législatives introduites en 2007. En effet, la loi prévoit désormais des exemptions de certains traitements de données pour lesquelles une notification était auparavant nécessaire. La mise en place de formalités optimisées et simplifiées à travers de nouveaux formulaires a aussi contribué à simplifier la mise en œuvre des formalités.

Ainsi, le nombre traité de notifications ordinaires est passé de 760 en 2007 à 385 pour l'année 2008. Les notifications simplifiées qui étaient encore au nombre de 537 en 2007 ont été supprimées par la modification de la loi sur la protection des données.

Les demandes d'autorisation préalable introduites en 2008 ont connu une augmentation significative par rapport à 2007, en passant de 543 dossiers au total en 2007 à 826 au total en 2008.

Le nombre total de dossiers de formalités préalables est passé de 1.840 en 2007 à 2.153 en 2008.

Fin 2008 le nombre total de dossiers introduits depuis 2003 s'établit à 14.050, 4.357 déclarants / responsables avaient accompli des formalités contre 3.754 fin 2007.

2.2.1.2 Les chargés de la protection des données

Au niveau de la désignation de chargés de la protection des données, on peut constater une très légère augmentation. Grâce aux modifications législatives de 2007, les organisations, entreprises, administrations, associations et institutions ont la possibilité de choisir une personne salariée comme chargée de la protection des données. Un nombre plus important d'entreprises devraient à l'avenir faire usage de cette faculté optionnelle pour les responsables de traitements. La contrainte du recours à une personne externe à l'entreprise et le coût afférent avaient fortement limité jusque là le succès de la fonction de chargée de la protection des données qui reste facultative. Tandis que dans le passé la Commission nationale délivrait d'abord un agrément aux personnes intéressées de remplir cette fonction avant que ces dernières ne fassent l'objet d'une désignation, il est désormais d'usage que l'agrément soit délivré quasiment en parallèle avec la désignation d'une personne interne, désignation effectuée par le responsable du traitement.

2.2.1.3 Autorisation en cas de transferts de données vers des pays tiers

La directive 95/46/CE du 24 octobre 1995 établit un régime légal harmonisé de protection des personnes à l'égard du traitement des données à caractère personnel à travers les 27 Etats membres de l'Union.

L'article 25 prévoit que le transfert vers un pays tiers ne peut en principe avoir lieu que si ce dernier assure un niveau de protection adéquat (ce qui est d'office le cas des pays faisant partie de l'espace économique européen) ou si le destinataire offre des garanties suffisantes de nature à pallier les lacunes ou insuffisances du cadre légal applicable en matière de protection de la vie privée et des libertés et droits fondamentaux des personnes.

A moins que le responsable du traitement établi à Luxembourg qui souhaite exporter des données à caractère personnel vers un pays tiers ne figurant pas sur la liste de ceux pour lesquels la Commission européenne a reconnu une protection adéquate, ne puisse invoquer l'une des dérogations (consentement indubitable, nécessité pour l'exécution d'un contrat conclu dans l'intérêt de la personne concernée, intérêt public important, …), l'examen préalable par la Commission nationale est obligatoire. La directive prévoit qu'il soit veillé ainsi à ce que les données exportées bénéficient chez leur destinataire hors Union européenne des garanties exigées. Ces dernières peuvent résulter notamment de clauses d'un contrat passé avec le destinataire par la personne physique ou morale qui procède au transfert de données. Celles-ci doivent comprendre également des stipulations en faveur des personnes concernées par les fichiers et données exportés leur assurant l'exercice des droits essentiels que le cadre légal européen de la protection des données leur garantit.

Les transferts de données vers un pays tiers opérés sur base des dérogations de l'article 19 paragraphe (1er) de la loi par un responsable de traitements établi à Luxembourg doivent être notifiés à la CNPD. Depuis la réforme de 2007, le rapport prévu au paragraphe (2) ne doit être établi que si la Commission nationale le demande expressément.

Si le pays d'exportation ne figure pas parmi ceux reconnus comme offrant une protection adéquate, une autorisation préalable doit être demandée pour le transfert conformément au paragraphe (3) dudit article 19, à moins que le destinataire ne soit de ceux pour lesquels la Commission européenne a pris une décision d'adéquation spécifique (entreprises américaines certifiées « Safe Harbor » par la FTC ou douane et administrations de la sécurité aérienne des Etats-Unis pour les données passagers relatives aux vols à destination des Etats-Unis).

En général c'est un contrat qui est passé entre la société qui détient le fichier et souhaite en exporter des données à caractère personnel et celle(s) à destination desquelles les données doivent être transmises et ce contrat reprend la plupart du temps les clauses types assurant des garanties appropriées approuvées par la Commission européenne. Ces clauses standard existent sous deux formes différentes, à savoir celles visant des transferts de données vers des sous-traitants établis dans un pays tiers qui n'assure pas une protection adéquate (décision 2002/16/CE du 27/12/2001) et celles pour des transferts à destination de sociétés/personnes appelées à effectuer un nouveau traitement pour leur propre compte de ces données (décision 2001/497/CE du 15 juin 2001 et décision 2004/5271 validant un jeu alternatif de clauses modèles).

En 2008 la Commission nationale a été saisie (après avoir mis en place une rubrique thématique consacrée à ce sujet et avoir proposé un formulaire spécifique sur son site Internet) de 37 demandes d'autorisation de la part d'entreprises voulant transférer ainsi des données vers des pays tiers sans protection adéquate.

Les autorisations afférentes ont entre temps pu être toutes accordées sauf quelques unes pour lesquelles des éléments essentiels manquaient au dossier.

2.2.1.5 Approbation de règles contraignantes d'entreprise

En juin 2003 le Groupe des autorités européennes de protection des données a publié un document de travail qui envisage une autre optique que la conclusion de contrats avec les entités hors Union Européenne vers lesquelles des données doivent être communiquées, les « règles contraignantes d'entreprises » (en anglais : BCR : binding corporate rules).

Il s'agit d'une sorte de « charte de la protection des données à caractère personnel » dont un groupe d'entreprises multinationales est appelé à se doter pour fournir les garanties dont ses entités établies dans un Etat membre de l'Union européenne doivent justifier pour l'obtention de l'autorisation de transfert de données à caractère personnel vers leurs maisons mère ou d'autres entreprises partenaires ou affiliées au même groupe établies dans des pays sans protection adéquate.

Entre 2004 et 2008 différents documents de référence ont été publiés par le groupe de l'article 29 (des commissaires européens à la protection des données) qui précisent les critères auxquels ces chartes d'entreprises doivent répondre pour être reconnues comme apportant les garanties nécessaires en termes de protection des libertés et droits fondamentaux des personnes concernées. Les représentants de la Commission nationale se sont tout de suite investis dans ces groupes de travail, persuadés que les « BCRs » constituent une simplification importante en faveur des grands groupes internationaux d'entreprises qui veulent documenter le maintien de la protection assurée aux données personnelles dans l'espace économique européen lorsqu'elles les exportent vers des pays tiers.

L'économie luxembourgeoise comprend un nombre proportionnellement important de filiales de groupes dont l'activité se déroule sur le plan mondial ou du moins qui travaillent avec des entreprises situées dans nombre de pays hors de l'Union européenne.

C'est pour cela que nous avons été dès le début parmi les promoteurs de ce nouvel instrument destiné à consacrer la protection des données au niveau de l'activité d'un même groupe dans un seul et même document que toutes les entités affiliées s'obligent à respecter.

Après avoir reçu un dossier en 2006 et en 2007, la Commission nationale a été impliquée en 2008 dans l'analyse de 3 chartes nouvellement soumises à l'examen et à l'approbation des autorités de protection des données des Etats membres où elles sont actives. Fin 2008, l'introduction d'un dossier d'une grande entreprise de commerce et services offerts sur Internet a constitué une première alors que notre autorité nationale s'est vue reconnaître le rôle de chef de file pour la validation de ses BCRs. En conséquence elle est en train d'effectuer une analyse en profondeur des règles appliquées au sein de ce groupe, non seulement au sein de ses sociétés établies à Luxembourg mais aussi ailleurs dans le monde, et des règles qu'elle s'est fixée elle-même dans ce domaine, de l'assistance de procédures de contrôle (internes et externes) mises en place et de droits et possibilités de recours reconnus à ses clients et salariés dont les données sont traitées et transmises à travers le monde.

Mener à bien cette mission en 2009 est essentiel pour la crédibilité du Luxembourg au sein de la communauté des commissaires européens de la protection des données et peut engendrer une contribution favorable, pour l'implantation de filiales européennes à Luxembourg, en particulier par les entreprises faisant appel à des technologies informatiques avancées ou à la commercialisation à travers l'Internet.

Le renforcement des effectifs de personnel (3 juristes en 2008 et un rédacteur début 2009) a été une condition essentielle pour nous permettre de rencontrer efficacement ce « challenge ».

Les autorités nationales d'une quinzaine d'Etats membres ont entre temps fait connaître leur décision de reconnaissance mutuelle, ce qui veut dire qu'elles se rallieraient d'emblée aux conclusions de notre analyse et ne procéderaient plus à un examen détaillé du dossier pour délivrer l'autorisation requise pour les données transférées à partir de leur pays.

Nous espérons terminer l'examen de ce dossier et aboutir à l'approbation collective sur le plan européen de ladite charte intragroupe de protection des données en automne 2009.

2.2.2 Plaintes et investigations

Le nombre de plaintes et demandes de vérification de licéité a connu une nette augmentation avec 63 dossiers en 2008 contre 34 en 2007.

Il est à relever que la Commission nationale a également procédé à des actions d'investigation de sa propre initiative (sans qu'une réclamation n'ait été portée à son attention), en se concentrant notamment sur les traitements de données d'envergure ou particulièrement sensibles.

2.3 Information du public

2.3.1 Actions de sensibilisation du public

La Commission nationale a pris un certain nombre d'initiatives visant à sensibiliser le public le plus large aux enjeux de la protection des données à caractère personnel et de l'informer sur les règles applicables, notamment les droits reconnus aux personnes concernées par les traitements.

Le 28 janvier 2008 s'est tenue, à l'initiative du Conseil de l'Europe avec l'appui de la Commission européenne, la « Journée européenne de la protection des données ». Cette journée se tient chaque année le 28 janvier, date-anniversaire de l'ouverture à la signature en 1981 de la « Convention 108 de Strasbourg » pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel à laquelle 41 pays - dont le Luxembourg - ont adhéré. La journée a pour but de rappeler à travers toute l'Europe l'importance du respect de la vie privée et des droits reconnus aux citoyens à l'égard du traitement de leurs données personnelles. La Commission nationale a participé à cette journée, notamment avec une campagne de communication comportant une annonce publiée dans la presse écrite et électronique ainsi qu'une communication avec les médias sous forme de dossier de presse, suivie par une série d'articles de presse et d'interviews de son président. La journée a fourni l'occasion à la Commission nationale de sensibiliser le public sur le fait que dans la vie quotidienne de multiples informations personnelles sont collectées, enregistrées, stockées, communiquées et rapprochées sous des formes diverses, souvent à l'insu des personnes concernées.

La CNPD a entre autres participé avec un stand d'information à la journée 2008 « Luxembourg Safer Internet » organisée par LuSI les 8 et 9 octobre 2008. La journée visait particulièrement les activités de sensibilisation des élèves à propos de la sécurité sur Internet. Le stand d'information de la CNPD a porté sur les risques et opportunités de la communication sur des réseaux sociaux, blogs et chats, ainsi que sur la protection des internautes.

2.3.2 Reflets de l'activité de la Commission nationale dans la presse

Au total, on a cité la Commission nationale et le thème de la protection des données 72 fois dans la presse luxembourgeoise en 2008.

La panoplie des thèmes évoqués a été très vaste avec une large couverture de la Journée européenne de la protection des données (8 citations, respectivement articles de presse), la présentation du rapport annuel sur l'année 2007 (9 citations), différents sujets d'actualité, telle la vidéosurveillance sur les lieux publics (8 citations).

Parallèlement la Commission nationale, représentée par son président ou un autre membre effectif, est à plusieurs reprises intervenue directement dans les médias pour parler de différents sujets relatifs à la protection des données.

Outre la communication par voie de presse, la présentation des enjeux de la protection des données fait régulièrement l'objet d'exposés et de conférences publiques, notamment auprès de L'Université de Luxembourg, auprès d'organismes divers comme le Clussil et la « Luxembourg Internet Society ».

2.3.3 Outil de communication : le site Internet

Le vecteur de communication courant de la Commission nationale avec le public est le site Internet (www.cnpd.lu). Le site vise à proposer une nformation de base sur la protection des données à l'attention des citoyens et du public en général, notamment à travers les rubriques « Actualités » et « Droits des personnes concernées ». Il vise aussi à offrir une documentation approfondie par thèmes (« Dossiers thématiques ») pour les lecteurs avertis, conseillers et responsables d'entreprise avec des liens facilitant des recherches sur les thèmes importants. Le site se veut finalement aussi une plateforme interactive pour l'accomplissement en ligne des formalités prescrites par la loi, la consultation du registre public des traitements (« fichier des fichiers ») et les réactions des citoyens.

En effet, les formalités de notification peuvent être remplies quasiment « avec un clic » sur le site Internet de la Commission nationale.

Ainsi, en 2008, 60% des notifications ont été remplies en ligne par le biais du formulaire électronique. Il est prévu d'adapter prochainement la procédure de notification par voie électronique pour permettre l'utilisation du certificat Luxtrust (signature électronique) au lieu d'une signature manuelle sur papier.

Le site Internet de la Commission nationale a affiché au total 224.833 visites en 2008, ce qui correspond à une moyenne de 614 visites par jour (sur 366 jours), et allant jusqu'à 1.130 visites journalières. Sur la base des réflexions précédentes, ce sont les mois d'avril et de mai 2008, avec respectivement quelque 27.000 visites contre une moyenne mensuelle de 18.736 visites, qui ont affiché le plus de visites.

Le site Internet constitue un moyen d'information important pour la Commission nationale qui a fait le choix d'utiliser cet outil de communication pour informer de manière permanente et continue sur les évolutions en matière de protection des données à caractère personnel et ce aussi bien sur le plan national qu'européen et international.

Au cours de cette année, le site Internet sera refondu, afin d'en améliorer essentiellement l'accessibilité et la maniabilité.

2.3.4 Formations et conférences

La Commission nationale saisit régulièrement l'occasion d'expliquer les règles légales dans le cadre d'exposés ou formations destinées à un public averti ou aux professionnels d'un secteur déterminé. La Commission nationale a ainsi effectué des présentations des modifications apportées en 2007 à la loi sur la protection des données au Collège médical, à la Chambre de commerce, ainsi qu'à la FNCTTFEL.

Outre les formations et conférences précitées, il y a lieu de relever l'intervention de la Commission nationale dans le cadre de la formation « Management de la Sécurité des Systèmes d'Information» (MSSI) à l'Université de Luxembourg. Les objectifs de cette formation consistent à sensibiliser les responsables de la sécurité des systèmes d'information à la problématique de la protection des données à caractère personnel (renseignements sur le site de l'Université de Luxembourg). La remise des diplômes aux premiers lauréats de ce cycle a eu lieu en automne 2008.

2.4 Avis et recommandations

A la demande du gouvernement, la Commission nationale a émis sept avis en 2008 sur des projets de loi ou des dispositions réglementaires. La Commission nationale a adopté lors de sa séance du 11 janvier 2008 un avis sur le projet de loi n° 5802 portant sur la libre circulation des personnes et l'immigration suivi de son avis du 18 juillet 2008 sur le projet de règlement grand-ducal autorisant et réglant certains traitements de données dans le cadre de l'exécution des dispositions de la loi du 29 août 2008. Elle a en outre été consultée directement par la Chambre des Députés à l'initiative de la commission parlementaire compétente sur une modification de la loi électorale. Un avis a été émis sur demande de l'Institut Luxembourgeois de Régulation et un autre avis sur demande de la Ville de Luxembourg. D'autres prises de position concernent des avant-projets de loi ou de règlement grand-ducal, notamment dans le domaine de la médecine. Ces avis sont reproduits dans les annexes de ce rapport annuel, de même qu'une décision type à titre d'exemple pour celles adoptées généralement par la Commission nationale dans les dossiers de demande d'autorisation en matière de surveillance de l'usage d'Internet et du courrier électronique sur le lieu du travail.

2.5 Participation aux travaux européens

Au courant de l'année 2008, la Commission nationale a continué à participer à différents groupes et sous-groupes de travail au niveau européen.

Il s'agit notamment :

- du groupe « Article 29 » sur la protection des données (établi en vertu de l'article 29 de la directive 95/46/CE) qui regroupe toutes les CNPD européennes,
- du sous-groupe « Flux internationaux de données »,
- du sous-groupe « Technologies » ;
- du « groupe de Berlin », dédié à la protection des données privées dans le secteur des communications électroniques,
- du séminaire européen biannuel d'échanges d'expériences dans le traitement des cas pratiques («Case Handling Workshop »),
- du Comité consultatif de la Convention 108 du Conseil de l'Europe (T-PD), et
- de la Conférence annuelle des Commissaires à la protection des données.

Ainsi, les représentants de la Commission nationale ont participé à plus de 20 réunions sur le plan européen. Ces réunions se caractérisent fréquemment par un niveau élevé de technicité et demandent par conséquent généralement une préparation approfondie et un suivi continu des matières traitées.

Par ailleurs, les membres de l'autorité de contrôle de l'article 17 participent en alternance aux réunions des autorités conjointes de contrôle européennes d'Europol, du système d'information « Schengen » et des autorités douanières.

Le membre effectif de la Commission nationale, informaticien de formation, a participé aussi à un colloque de spécialistes consacré à la sécurité informatique et à la protection de la vie personnelle.

2.5.1 Le groupe « Article 29 »

Au cours de l'année 2008, le groupe de travail a émis plusieurs avis à l'adresse de la Commission européenne et adopté plusieurs documents de travail. Parmi ces avis et documents, la CNPD aimerait en relever ci-après les plus importants.

Une grande partie des travaux a porté sur les règles d'entreprise contraignantes (« Binding corporate rules » BCR), alors que le groupe « Article 29 » a adopté pas moins de trois documents sur ce sujet. Les transferts internationaux de données personnelles à partir de l'UE vers des pays tiers entre filiales d'un même groupe d'entreprises peuvent avoir lieu sur base de règles d'entreprise contraignantes (BCR) lesquelles doivent être considérées comme une garantie appropriée, au sens de la directive 95/46/CE. L'instrument des BCR est ainsi une solution, convenant aux sociétés multinationales, qui leur permet de remplir leurs obligations légales et de garantir un niveau adéquat de protection des données à caractère personnel lors du transfert de données à l'extérieur de l'UE. En 2003 et 2005, le groupe « Article 29 » avait déjà élaboré deux documents de travail sur ce sujet. Durant 2008, le groupe « Article 29 » s'est efforcé d'expliquer et de clarifier davantage ses deux documents de travail précédemment adopté en 2003 et 2005 à travers l'élaboration de trois nouveaux documents de travail :

- sur les questions fréquemment posées (FAQ) concernant les règles d'entreprise contraignantes,
- établissant un cadre pour la structure des règles d'entreprise contraignantes,
- établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes.

Ces documents de travail ont pour but d'aider et de guider les sociétés multinationales dans l'élaboration de leurs règles d'entreprise contraignantes ainsi qu'à obtenir leur approbation auprès des autorités de contrôles nationales.

Au mois de février 2008 le groupe « Article 29 » a adopté un document de travail sur la protection des données à caractère personnel de l'enfant. Ce document a été élaboré dans le contexte de l'initiative générale de la Commission européenne décrite dans sa communication « *Vers une stratégie européenne sur les droits de l'enfant* ». Il a comme objectif d'analyser les principes fondamentaux applicables en les illustrant par des références à l'école (p.ex. données scolaires ; données biométriques - accès à l'école et à la cantine ; vidéosurveillance dans les écoles ; état de santé des enfants ; photos des élèves ; sites Internet des écoles ; cartes scolaires ; etc.). Le groupe de travail souligne encore que si nos sociétés veulent créer une véritable culture de la protection des données, en particulier, et de la vie privée, en général, il convient de commencer par les enfants en leur apprenant l'importance de ces principes dès leur plus jeune âge.

Le groupe « Article 29 » a aussi été consultée par la Commission européenne pour donner son avis sur le projet de norme internationale de protection de la vie privée du code mondial antidopage. Si le groupe de travail salue dans son avis l'initiative de l'Agence Mondiale Antidopage en faveur de l'adoption de normes minimales de protection de la vie privée et des données à caractère personnel des sportifs, il n'a cependant pas encore donné son aval au projet de texte international en question, alors que celui-ci n'a pas encore atteint les niveaux minimaux requis par la réglementation européenne sur la protection des données.

La Commission européenne ayant adopté une proposition de modification de la directive 2002/58/CE concernant le traitement de données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (transposée au Luxembourg par la loi du 30 mai 2005), le groupe « Article 29 » a été demandé en son avis sur cette proposition de directive modificative. Le principal objectif de celle-ci est d'améliorer la protection des données personnelles et de la vie privée des individus dans le secteur des communications électroniques, notamment en renforçant les dispositions liées à la sécurité et les mécanismes coercitifs (i.e. notification des violations de sécurité). Dans son avis y relatif, le groupe de travail a formulé un certain nombre de recommandations et d'améliorations.

Il a encore émis un avis sur les aspects de la protection des données liés aux moteurs de recherche sur Internet. Pour plus de détail sur ce sujet, il est renvoyé au point 2.5.2 du présent rapport.

La liste avec les références des avis et documents de travail adoptés en 2008 par le groupe « Article 29 »,

par les différents sous-groupes et autres Comités figure en annexe du présent rapport d'activités.

2.5.2 Le sous-groupe « Technologies »

Internet fait désormais partie de notre vie quotidienne. Qu'il s'agisse de rechercher des informations, de réserver ses prochaines vacances ou d'acheter des produits par Internet, les moteurs de recherche sont devenus indispensables.

Des moteurs de recherche tels que Google ou Yahoo! collectent lors de chaque recherche de nombreuses informations sur les utilisateurs : un cookie personnel, l'adresse IP de la machine et le contenu de la requête. Ces données sont alors conservées pendant des durées variables. Ensuite, elles peuvent être anonymisées ou effacées. Les moteurs de recherche enregistrent ainsi pour chaque utilisateur, l'ensemble de ses requêtes et les publicités auxquelles ils ont été sensibles.

Pour parvenir à retracer les recherches d'une seule et même personne sur une longue période, plusieurs possibilités existent : si l'utilisateur dispose d'une adresse IP statique, il est très facile d'identifier ses différentes visites. L'adresse IP étant bel et bien une donnée personnelle qui doit être protégée en tant que telle, ceci entraîne une série de conséquences en particulier à propos de leur exploitation à des fins publicitaires, commerciales et autres. Mais généralement les fournisseurs d'accès à l'Internet utilisent des adresses IP dynamiques pour leurs abonnés, c'est-à-dire des adresses qui changent à chaque connexion. Dans ce cas-là, les moteurs de recherche ont recours aux cookies permanents : des petits mouchards installés sur les PC des utilisateurs avec un numéro d'identification fixe permettent de reconnaître chaque visiteur lorsqu'il se connecte sur le site. L'identification est par ailleurs encore plus simple lorsque les utilisateurs s'authentifient pour utiliser un des services des moteurs de recherche.

Suite aux travaux du sous-groupe « Technologies », le groupe de travail « Article 29 » a adopté le 4 avril 2008 un avis dressant une liste précise des responsabilités qui incombent aux fournisseurs de moteurs de recherche. Le principal objectif de cet avis est de parvenir à un équilibre entre les besoins légitimes des fournisseurs de moteurs de recherche et la protection des données à caractère personnel des internautes.

L'une des principales conclusions de l'avis est que la directive européenne sur la protection des données s'applique généralement au traitement des données à caractère personnel par les moteurs de recherche, même lorsque le siège de ces derniers se trouve en dehors de l'EEE. L'avis relève aussi que les fournisseurs de moteurs de recherche ne doivent utiliser les données à caractère personnel qu'à des fins légitimes. Les fournisseurs de moteurs de recherche sont obligés de supprimer ou de rendre les données à caractère personnel totalement anonymes dès qu'elles ne servent plus les finalités déterminées et légitimes pour lesquelles elles ont été collectées. Les fournisseurs de moteurs de recherche doivent aussi être à tout moment en mesure de justifier le stockage et la durée de vie des « cookies » envoyés. L'avis du groupe de travail « Article 29 » rappelle aussi que les moteurs de recherche sont tenus d'informer clairement les utilisateurs à l'avance de toutes les utilisations prévues de leurs données, et de respecter leur droit de consulter, de vérifier ou de corriger aisément ces données personnelles.

2.5.3 Le « groupe de Berlin »

Au cours de ses réunions biannuelles, ce groupe a mis l'accent dans ses travaux sur la problématique des réseaux sociaux virtuels.

De nombreuses personnes recourent fréquemment à des réseaux sociaux tels *Facebook, myspace, hot.lu* et à d'autres communautés virtuelles. Ces réseaux sociaux offrent des services innovants, et généralement gratuits, souvent en contrepartie d'une utilisation commerciale des données personnelles, parfois à l'insu des utilisateurs eux-mêmes. Une fois en ligne, les informations sont plus ou moins largement diffusées, indexées et analysées.

En rendant public des informations sur ses habitudes de vie, ses connaissances amicales ou encore ses convictions politiques et religieuses, les utilisateurs de réseaux sociaux rendent publiques de nombreuses informations sur leur vie privée et permettent aux exploitants des sites de constituer des fichiers contenant une multitude d'informations, qui peuvent faire l'objet de nombreuses exploitations commerciales.

Une bonne utilisation d'Internet suppose des utilisateurs informés et économes de leurs données, particulièrement si elles peuvent avoir des répercussions sur l'intégrité de leur vie privée. Elle présuppose également la mise en place de dispositifs de la part des fournisseurs de ces plateformes qui permettent d'éviter les risques. En effet, un problème qui se pose est que les configurations par défaut des réseaux sociaux favorisent fréquemment la diffusion des données parce qu'elles ne sont pas suffisamment restrictives.

Les jeunes sont souvent de meilleurs internautes que les adultes, mais constituent aussi des cibles idéales, notamment pour les spécialistes du marketing commercial. Mettant à profit le goût du jeu et la crédulité des mineurs, des personnes ou organisations peuvent, à bon prix, se constituer des fichiers d'informations de nature privée, sociale et économique sur les jeunes et leurs familles. Toutes sortes d'individus ou d'organisations promoteurs d'incitations douteuses touchant notamment aux mœurs, au racisme ou aux sectes peuvent aussi accéder à des informations parfois sensibles.

C'est dans ce sens que le « groupe de Berlin » a adopté le 4 mars 2008 un rapport et un guide au sujet de la protection des données personnelles et de la vie privée dans les réseaux sociaux virtuels (« Report and Guidance on Privacy in Social Network Services »). Le document en question s'adresse aux régulateurs, aux fournisseurs de services de réseaux sociaux ainsi qu'aux utilisateurs (cf. Annexe).

Dans un objectif de sensibiliser davantage les jeunes aux risques liés à l'utilisation des réseaux sociaux en termes de protection de leur sphère privée et de leurs données personnelles, la CNPD a participé au cours de l'année 2008 à des activités telles que l'édition 2008 du LusiDay.

2.5.4 Le séminaire biannuel européen « Case Handling Workshop »

Aux mois d'avril et de septembre 2008, la Commission nationale a participé aux séminaires consacrés aux expériences dans le traitement de cas pratiques « Case Handling Workshop » qui ont eu lieu respectivement à Ljubljana et à Bratislava.

Lors de ces travaux, une large panoplie de sujets a été discutée. Il y a lieu de relever les thèmes et sujets suivants :

- surveillance sur le lieu de travail : caméras vidéo, enregistrement des conversations téléphoniques, e-mail/Internet, etc. ;
- vidéosurveillance dans les lieux privés et publics ;
- réseaux sociaux (« social networking »), en particulier quant à leur utilisation par les enfants et adolescents ;
- collecte des données personnelles sur Internet et droits des personnes concernées;
- protection des données dans le secteur bancaire et financier;
- protection des données et liberté d'expression dans les médias;
- biométrie ;
- dispositifs d'alerte professionnelle (« whistle-blowing »).

3 Les temps forts de 2008

Les travaux de la Commission nationale ont été marqués par un certain nombre de dossiers et de priorités, soit imposés par le contexte politique et/ou l'actualité, soit choisis par la Commission nationale en fonction de l'importance de la thématique par rapport aux principes de la protection des données à caractère personnel.

3.1 Cybersurveillance des salariés par l'employeur

Dans la matière complexe de la cybersurveillance des salariés par l'employeur, la Commission nationale a élaboré en 2008 une décision type qui vise à concilier respect de la sphère privée des salariés sur le lieu de travail et intérêts légitimes des employeurs. Dans sa décision type, la Commission nationale met en avant la nécessité d'une proportionnalité des mesures de surveillance adoptées, ainsi que d'une règle de jeu équilibrée. Les questions que soulèvent la plupart des demandes d'autorisation soumises à la Commission nationale ont notamment trait à la vie privée des salariés sur leur lieu de travail, aux usages à des fins privées d'outils mis à disposition par l'employeur, ainsi qu'aux limites à la surveillance et au contrôle des salariés par l'employeur.

La décision type a été élaborée en tenant compte des nombreuses demandes d'autorisation et des demandes de renseignement soumises à la Commission nationale. Elle retient ainsi un catalogue limitatif de finalités pour lesquelles des mesures de surveillance peuvent être acceptées. Il s'agit de mesures qui concernent la sauvegarde du fonctionnement technique des systèmes informatiques de l'entreprise, des droits de propriété intellectuelle, des secrets d'affaires et de fabrications, des informations auxquelles est attaché un caractère de confidentialité, ainsi que la prévention d'actes de concurrence déloyale.

Une difficulté de la cybersurveillance réside en effet dans le fait qu'il n'est souvent pas possible de distinguer clairement entre ce qui relève de la vie professionnelle et ce qui relève de la vie privée. La décision type arrêtée par la Commission nationale retient en ce qui concerne le contrôle des courriels que l'employeur ne peut pas contrôler des courriels privés même s'il a interdit toute utilisation de la messagerie à des fins privées. La consultation des courriels professionnels pendant l'absence ou après le départ du salarié afin d'assurer la bonne poursuite des activités de l'entreprise est possible. Les données relatives aux courriels par les collaborateurs consultés dans ces circonstances ne devront cependant pas être utilisées par l'employeur à l'égard du collaborateur pour l'évaluation de celui-ci, à des fins disciplinaires ou dans d'autres litiges.

Les fichiers sauvegardés par le salarié sur son ordinateur professionnel sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel. Le responsable du traitement ne peut accéder aux dossiers ou fichiers identifiés comme privés sans la présence de la personne concernée.

Une ligne directrice de la décision type élaborée par la Commission nationale est la proportionnalité dans la surveillance. Il s'agit ainsi d'éviter toute surveillance permanente qui serait à considérer comme excessive. Le principe de la proportionnalité exige la limitation de la surveillance à une surveillance ponctuelle et le respect d'une graduation dans l'intensification de la surveillance (selon la notion allemande de la « *progressive Kontrollverdichtung* ») qui doit être justifié chaque fois par des indices et des soupçons précis. Ces vérifications ne peuvent être intensifiées graduellement qu'à l'égard des personnes contre lesquelles des indices d'abus ou de comportements irréguliers ont été détectés.

3.2 La prise en charge des formalités légales

Etant donné que la révision de la loi du 2 août 2002 relative à la protection des personnes à l'égard des traitements de données à caractère personnel a apporté un certain nombre de clarifications, ainsi que des allègements et simplifications des démarches administratives imposées aux responsables de fichiers et traitements, les difficultés qu'avait pu rencontrer la Commission nationale pour traiter dans les délais normaux les notifications et demandes d'autorisation qui lui étaient soumises ont pu être surmontées.

Avec l'entrée en vigueur des modifications apportées à la loi, le traitement des données sensibles (opinions politiques, convictions religieuses, appartenance syndicale et renseignements relatifs à la santé) n'est plus soumis à autorisation, mais à notification préalable, tout en n'étant licite que dans les seuls cas expressément prévus aux articles 6 et 7 de la loi.

Les traitements des employeurs nécessaires dans le cadre de l'organisation, du déroulement des élections sociales et du fonctionnement des organes de représentation des salariés font désormais l'objet d'une notification unique (procédure simplifiée). Les employeurs qui doivent nécessairement recourir à ces traitements afin de respecter les dispositions afférentes du droit du travail n'ont plus qu'à notifier un engagement formel de conformité. Les traitements de données en rapport avec les candidatures à l'élection et avec la composition des organes représentatifs du personnel doivent être gérés avec soin par les responsables d'entreprise. Les informations portant sur l'appartenance syndicale des salariés sont en effet considérées comme des données sensibles par la loi sur la protection des données. De nombreuses entreprises ont utilisé cette possibilité en 2008.

Les demandes d'autorisation non encore examinées concernent pour l'essentiel des traitements de données à des fins de surveillance, parmi lesquels figurent quelque 400 dispositifs de vidéosurveillance au sujet desquels la CNPD doit encore se prononcer.

Etant donné que la Commission nationale a élaboré en 2008 une décision type concernant la cybersurveillance des salariés par l'employeur (qui envisage de multiples cas de figure et circonstances spécifiques), les demandes d'autorisation restées en attente de décision de la part d'employeurs souhaitant être autorisés à mettre en place un système de surveillance de l'utilisation d'Internet et du courrier électronique par leurs salariés vont pouvoir être évacuées au cours des mois à venir.

Même si la rapidité de l'examen des demandes d'autorisation a pu être optimisée, il faut souligner que les critères de légitimité et de proportionnalité, de caractère compatible avec la finalité initiale, la durée et les conditions de conservation des données prévues par la loi, doivent être appréciés au cas par cas, en fonction des circonstances et du contexte particulier de chaque demande. Ils rendent ainsi impossible une standardisation maximale dans l'examen des dossiers.

Suite aux modifications opérées par la loi du 27 juillet 2007, on peut noter en revanche une régression notable du nombre des notifications reçues depuis l'automne 2007.

Cette diminution s'explique par le fait que les traitements « anodins » les plus courants sont désormais exemptés de notification. Pour un grand nombre de petites et moyennes entreprises, les modifications de la loi ont donc amené une simplification non négligeable des formalités administratives.

L'examen par la Commission nationale des demandes présentées par les responsables de traitements de données à caractère personnel qui restent soumis à une autorisation préalable a pu être accéléré de façon significative par des mesures d'organisation interne.

Au cours de l'année 2008, près de 800 traitements ont été autorisés (souvent avec certaines restrictions ou conditions à observer dans la mise en œuvre) et le nombre de traitements de données figurant dans le registre public (consultable en ligne sur www.cnpd.lu) dépasse désormais les 12000.

S'il n'y a dorénavant plus de retard dans la prise en charge des notifications, il faudra toutefois compter encore quelques mois avant de venir à bout de l'engorgement actuel au niveau des demandes d'autorisation (en particulier de l'autorisation de dispositifs de vidéosurveillance ou de surveillance sur le lieu du travail).

Le renforcement de ses ressources en personnel et les simplifications intervenues récemment, en même temps que l'approfondissement permanent des connaissances et de l'expérience acquise désormais dans ce domaine, permet néanmoins à la Commission nationale d'aborder l'année 2009 avec davantage de sérénité.

3.3 Quelques sujets délicats et arbitrages ardus

3.3.1 La e-restauration

Sur intervention de la Commission nationale auprès du Ministère de l'éducation nationale, la durée de conservation des données saisies relatives à la consommation des utilisateurs des cantines scolaires a été sensiblement réduite. La possibilité d'un opt-out de l'enregistrement a également été introduite en faveur des adultes et des élèves âgés de 16 ans et plus. Le nombre de données à caractère personnel enregistrées a également été réduit laissant place à la saisie sous forme de chiffres agrégés des informations qui ne doivent pas absolument être mis en relation avec des personnes identifiables.

Cette intervention de la Commission nationale qui faisait suite à quelques plaintes reçues de la part d'utilisateurs des cantines scolaires s'inscrit également dans le contexte des démarches entreprises par les autorités de protection des données au niveau européen pour renforcer le droit fondamental des enfants à la protection des données. Etant donné que la vie d'un enfant se déroule autant à l'école qu'au sein de la famille, il est naturel que plusieurs questions relatives à la protection des données se posent dans le cadre de la vie scolaire des enfants. La surveillance des achats des enfants dans le cadre de la restauration scolaire pose des questions quant à sa compatibilité avec le respect de la vie privée de l'enfant, particulièrement à partir d'un certain âge.

3.3.2 Identifiant unique

L'année sous revue a été celle de la finalisation du projet de loi n°5950 relatif à l'identification des personnes physiques, au registre national des personnes physiques et à la carte d'identité et celle au cours de laquelle la Commission nationale était amenée à arrêter sa position afférente après de longues discussions menées en amont avec les représentants des ministères impliqués.

Le projet de modification de la législation relative au numéro d'identification nationale des personnes est directement lié aux travaux effectués par le Comité National pour la Simplification Administrative en faveur des Entreprises (CNSAE).

Ce comité, créé en date du 16 décembre 2004 et coordonné par le Ministère des Classes Moyennes, du Tourisme et du Logement en collaboration avec le Ministère de l'Economie et du Commerce extérieur, a été mis en place dans le cadre de la mise en œuvre du programme gouvernemental du 4 août 2004.

Le Conseil du Gouvernement a reçu du CNSAE une note du 31 mars 2006 intitulée « *identifiant unique* » qui suggère de réformer la loi du 30 mars 1979 instituant l'identification numérique des personnes. Suite à cette note, un groupe de travail interministériel ad hoc a vu le jour.

Par ailleurs, l'identification numérique a fait l'objet de plusieurs questions parlementaires.

Dans sa réponse du 12 juin 2006 à la question parlementaire du 4 juin 2006 No 1.056 posée par l'honorable députée Madame Colette Flesch (Sur ce même thème, elle a également posé les questions parlementaires No 1.127, 1.128 en date du 20 juin 2006 et No 2.205 le 8 janvier 2008), Monsieur le Ministre des Communications Jean-Louis SCHILTZ a affirmé ce qui suit :

> *« Des évolutions récentes montrent également que l'utilisation fréquente du numéro d'identité national dans les procédures et usages administratifs vient de diluer la ligne de démarcation entre les usages licites et non licites dudit numéro tel qu'elle avait été tracée par la loi de 1979.*
>
> *La généralisation de l'emploi du numéro d'identité national en pratique mérite aujourd'hui une réflexion profonde sur les conditions d'utilisation du numéro d'identité et du répertoire général des personnes ainsi que sur les garanties susceptibles de satisfaire aux exigences de protection de données de la personne concernée.*
>
> *C'est la raison pour laquelle le Gouvernement a instauré un groupe de travail chargé de se pencher sur cette question et de faire des propositions pour réviser la législation sur le répertoire général des personnes physiques et morales en général et l'utilisation du numéro d'identité en particulier ».*

D'abord il faudra mettre une législation adéquate. Ensuite l'idée de créer un répertoire général des entreprises au sens large (entrepreneurs individuels, personnes morales, établissements publics, ASBL, fondations etc.) et un répertoire distinct pour les personnes physiques a été approuvée par le Conseil en Gouvernement »

Le groupe interministériel était donc visiblement confronté à l'attente de deux objectifs potentiellement contradictoires.

D'une part, le gouvernement souhaitait parvenir à une simplification des démarches administratives.

Et d'autre part, il estimait qu'il était devenu nécessaire de proposer de nouvelles garanties en matière de protection de données car il constatait que les règles et principes de protection des données posés par la loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales (ci-après : la loi du 30 mars 1979) étaient dépassés et n'étaient plus respectés. Dans son avis du 9 janvier 2004, la Commission nationale avait déjà développé cette problématique (Délibération 2/2004 Avis au sujet de l'avant-projet de règlement grand-ducal concernant l'accès au répertoire général des personnes physiques et morales par les officiers publics et autres créateurs ou exécuteurs d'actes translatifs de propriété immobilière ou de constitution d'hypothèque).

Elle a été consultée périodiquement entre 2006 et 2008 par ce groupe de travail.

Lors d'une première audition, la Commission nationale avait suggéré au groupe de travail de se poser la question de savoir si la réforme allait ou non apporter une ouverture face à la demande croissante d'élargissement de l'utilisation de l'identifiant numérique au-delà du cercle restreint des administrations publiques actuellement autorisées par voie de règlement grand-ducal.

Elle a alors donné à considérer que l'élargissement à certains acteurs privés de l'usage de l'identifiant unique pouvait être envisagé pour tenir compte de l'évolution de la société actuelle mais devait alors être accompagné du recours à une palette plus large des garanties juridiques et techniques encadrant l'utilisation de l'identifiant numérique et les flux de données. Dans ce contexte le groupe interministériel lui donna l'occasion de présenter les avantages respectifs en termes de protection des données de différents systèmes adoptés dans d'autres pays européens comme pistes de réflexion.

Il convient en effet de se souvenir que tous les pays européens n'ont pas mis en place un tel identifiant unique destiné à être utilisé à l'occasion de toutes les démarches administratives.

La constitution de certains pays interdit parfois l'utilisation d'un identifiant national multisectoriel unique (Par exemple, l'article 35 de la Constitution au Portugal).

En Allemagne, l'utilisation d'un tel identifiant n'est pas interdit formellement par la Constitution, mais le Bundestag a estimé que la Cour constitutionnelle d'Allemagne avait décidé dans son arrêt du 15 décembre 1983 que l'utilisation d'un identifiant unique multisectoriel pouvait être inconstitutionnel.

Il est vrai que l'utilisation d'un identifiant unique présente certains avantages pratiques.

Ainsi, l'administration est en mesure de croiser des informations sur une personne pour vérifier l'exactitude de ses affirmations et parer aux éventuelles fraudes. Le Comité Lindop au Royaume-Uni mettait également en exergue le fait qu'avec « *un seul et unique identifiant le coût global pour l'utilisateur serait réduit. De même le citoyen n'aurait plus à se souvenir des divers identifiants, spécifiques à chacune de ses nombreuses activités* » *(Rapport du Comité pour la protection des données 1978, chapitre 29 paragraphe 6).*

Mais la mise en place et l'utilisation d'un identifiant unique peut aussi présenter des risques au niveau des libertés et droits des citoyens.

En France, la Commission Nationale Informatique et Libertés (ci-après : la CNIL) a affirmé que « *l'utilisation généralisée d'un identifiant unique dans l'ensemble des fichiers, en ce qu'elle faciliterait leur interconnexion, permettrait de tracer les individus dans tous les actes de la vie courante* ».

Le danger majeur de l'utilisation d'un identifiant numérique multisectoriel résulte donc de la possibilité de croiser les informations contenues dans divers fichiers et s'appliquant à une même personne. Grâce à une clé unique : les informations éparpillées dans les fichiers d'administrations distinctes poursuivant des missions et finalités différentes entre elles sont toutes susceptibles d'être rassemblées pour tout savoir sur le titulaire du numéro d'identification unique.

Cette idée a été traduite par le spectre de *Gläserner Bürger* : la personne est comme « *transparente* » aux yeux de tiers car toutes les informations qui la concernent sont susceptibles d'être disponibles.

Enfin, il existe un risque réel de détournement de finalité : des personnes travaillant dans une administration autorisée à recourir au numéro d'identification seraient en mesure d'obtenir des informations personnelles sur des administrés alors que ces informations ne sont pas nécessaires et/ou utiles dans le cadre de leurs activités. La recherche d'informations pourrait être mue simplement par la curiosité. Pour d'aucuns, ce risque serait d'autant plus accru dans un pays de petite taille.

A notre connaissance, le premier texte à s'être prononcé sur l'identifiant unique est la Recommandation (86)1 relative à la protection des données à caractère personnel utilisées à des fins de sécurité sociale adoptée par le Comité des Ministres du Conseil de l'Europe le 23 janvier 1986.

Cette recommandation rappelle d'abord ce qui suit :

> *« Un équilibre doit être trouvé entre la nécessité d'utiliser des données à caractère personnel dans le domaine de la sécurité sociale, d'une part, et, d'autre part, la nécessité d'assurer la protection de l'individu notamment lorsque les données font l'objet d'un traitement automatisé ».*

Dans son paragraphe 5, elle précise que :

> *« L'introduction ou l'utilisation d'un numéro de sécurité sociale uniforme et unique ou de tout autre moyen analogue d'identification devrait s'accompagner de garanties adéquates prévues par le droit interne. »*

La Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et à la libre circulation de ces données (ci-après : la directive 95/46/CE), transposée en droit interne par la loi du 2 août 2002, se prononce également sur l'identifiant unique.

L'article 8 relatif aux « *traitements portant des catégories particulières de données* », communément appelées « *données sensibles* » dispose que :

> *« 7. Les États membres déterminent les conditions dans lesquelles un numéro national d'identification ou tout autre identifiant de portée générale peut faire l'objet d'un traitement. »*

Les conditions auxquelles la directive en question fait référence sont, sous une autre expression, les garanties appropriées exposées par le Conseil de l'Europe dans sa recommandation précitée.

Les limitations, les conditions ou garanties accompagnant la mise en place et l'utilisation des numéros d'identification peuvent revêtir différentes formes.

Concernant les garanties juridiques, il peut par exemple s'agir d'un formalisme préalable à l'utilisation du numéro d'identification. Actuellement au Luxembourg, une des garanties consiste dans l'exigence légale de l'autorisation par voie de règlement grand-ducal de toute utilisation du numéro d'identification.

Il peut également s'agir d'une condition (notamment dans l'autorisation par les comités sectoriels dans le régime belge) subordonnant le recours au numéro d'identification à des finalités clairement délimitées ainsi que d'une mesure pour parer à d'éventuels abus dans l'utilisation du dit numéro.

Quant aux garanties techniques, celles-ci doivent être suffisantes compte tenu des règles de l'art : si elles sont obsolètes ou dépassées, elles ne protègent plus. Ces garanties peuvent consister en la mise en place d'une journalisation des saisies et/ou des consultations et/ou des transmissions ou encore d'un historique d'utilisation, de cryptage informatique ou toute autre architecture complexe permettant de contrôler les flux d'utilisation du numéro.

Aux yeux de la Commission nationale, il est tout à fait possible à l'heure actuelle de parvenir à un équilibre entre la protection des données à caractère personnel et la simplification administrative tout en conservant un numéro d'identification unique multisectoriel. Elle s'est donc efforcée à passer en revue avec les membres du groupe de travail interministériel les bénéfices et inconvénients respectifs des systèmes d'autres pays européens qui offrent des garanties de protection de la vie privée sur le plan juridique et technique.

Le meilleur exemple de garanties appropriées nous a semblé être celui mis en place en Autriche. D'autres systèmes proposent également des garanties significatives, comme le système belge des banques-carrefour contrôlées par des comités sectoriels dans lesquels l'autorité de protection des données détient un droit de vote majoritaire.

En Suisse, le numéro d'identification était composé de onze chiffres et laissait apparaître des informations sur son titulaire (date et lieu de naissance notamment) avant l'entrée en vigueur de la loi fédérale du 23 juin 2006. Ce système était très ressemblant à celui qui existe actuellement au Luxembourg.

Désormais la structure du numéro d'identification est inscrite dans la loi. Le numéro d'identification est non parlant, composé de treize chiffres attribués de manière aléatoire.

De plus, l'utilisation dudit numéro est encadrée : la loi détermine expressément les utilisateurs autorisés à y recourir et précise chaque fois la finalité poursuivie.

Contrairement aux craintes exprimées au Luxembourg qui conduisent les auteurs du projet de loi à envisager une double période de transition, voire à reporter aux calendes grecques la mise en place d'un numéro non parlant qui ne dévoile plus d'informations personnelles comme l'âge et le sexe, celle-ci n'a nécessité en Suisse qu'une brève période de transition (une année et demie seulement). Tout en reconnaissant les améliorations par rapport au système antérieur, le Préposé Fédéral suisse à la protection des données a regretté toutefois (Vers une société sous surveillance ? Jean-Philippe WALTER, Publications de l'EPFL, août 2006. http://ditwww.epfl.ch/SIC/SA/SPIP/Publications/spip.php?article1117) que le système ne prévoit pas de mesure pour prévenir les interconnexions abusives de données :

> *« (…) il ne suffisait pas de prévoir dans la loi l'utilisation d'un numéro non parlant pour garantir le respect de la protection des données. Il était indispensable de prévoir un modèle qui empêchait techniquement des interconnexions et des utilisations de données non autorisées et non nécessaires. Un tel modèle excluait de recourir au numéro d'assuré social comme clé d'accès à d'autres registres. Ce numéro devait ainsi être réservé au secteur des assurances sociales uniquement. L'objectif légitime et non contesté de l'harmonisation des registres, l'amélioration de l'outil statistique ou le développement de l'administration électronique pouvaient être réalisés sans recourir au numéro d'assuré social en tant qu'identifiant unique. A l'instar de notre voisin autrichien, il convenait d'étudier la mise en place d'un modèle basé sur des numéros sectoriels et une série de transformations cryptographiques à partir d'un numéro de référence unique attribué à chaque individu. (…) ».*

Après avoir illustré les importants enjeux de la révision législative, la Commission nationale est en train de formuler dans un avis remis au gouvernement ses observations à l'égard des dispositions du projet de loi N°5950 traitant des aspects de protection des données.

Elle y examine en particulier les aspects relatifs :

a. au rôle du registre national et au droit d'accès ;
b. à l'utilisation élargie du numéro d'identification national ;
c. au choix de la structure de l'identifiant ;
d. à la problématique du traçage des échanges de données entre les personnes autorisées à utiliser le numéro d'identification nationale ;
e. à l'enregistrement d'un historique de consultation du registre national des personnes physiques.

Elle s'est résolue à ne pas remettre en cause le recours à un numéro d'identification unique à utilisation multiple pratiqué depuis près de trente ans et qui, de plus, ne heurte plus guère la sensibilité de l'opinion publique.

Par contre, la nécessité de reconstituer des garanties qui se révèlent aujourd'hui insuffisantes, voire défaillantes et/ou d'adjoindre des mesures de protection nouvelles mettant à profit notamment de nouveaux progrès techniques, nous a semblé indispensable alors que le projet de loi sous examen est censé préparer une nouvelle ère de l'administration publique dans la société de l'information.

3.3.3 Traitement ultérieur à des fins statistiques, scientifiques ou historiques

La question du traitement ultérieur de données à des fins statistiques, scientifiques ou historiques pose des enjeux importants. Dans ce domaine, la Commission nationale a pris une position qui vise à concilier deux principes : le principe strict de finalité et les exigences de la recherche qui peuvent exiger que des données soient utilisées ultérieurement à d'autres fins.

A titre d'illustration, on peut citer l'exemple d'un projet de recherche médicale ayant été soumis à la Commission nationale et qui a eu comme objet d'analyser à travers une étude observationnelle rétrospective un échantillon de personnes ayant été victimes d'un accident vasculaire cérébral au Grand-Duché de Luxembourg et pris en charge à partir du 1er mars 2006 dans les établissements hospitaliers luxembourgeois. Le projet de recherche scientifique était censé fournir des informations sur la prise en charge des AVC ainsi que des recommandations en termes de santé publique et de politique sociale afin de parvenir à une réduction des risques et l'amélioration de la vie quotidienne des victimes d'AVC et de leur famille. Pour mener cette recherche, il fallait disposer de données issues des dossiers médicaux des patients, ainsi que des fichiers des organismes de sécurité sociale. Or, ces données n'ont pas été recueillies dans le souci de mener ce projet de recherche mais dans le cadre de leur prise en charge lors de leur hospitalisation, respectivement pour la prise en charge des soins par les organismes sociaux.

Un autre exemple d'une étude scientifique utilisant des données collectées initialement à d'autres fins concerne une étude portant sur l'évaluation de politiques publiques mises en place par la loi du 21 décembre 2006 promouvant le maintien dans l'emploi et définissant des mesures spéciales en matière de sécurité sociale et de politique de l'environnement (ci-après : la loi du 21 décembre 2006). Le ministère du Travail souhaite disposer de l'évaluation de l'efficacité de ces mesures au moyen d'une étude longitudinale. Pour cela, il est nécessaire d'étudier les trajectoires professionnelles précises des personnes inscrites auprès de l'ADEM. Les données de l'étude doivent être recueillies dans les fichiers de l'ADEM (période d'inactivité) et dans les fichiers de l'IGSS (affiliation, date de commencement d'un emploi). Les personnes concernées sont obligées de fournir ces renseignements à l'ADEM et à l'IGSS et ne s'attendent pas que leurs données soient utilisées à d'autres fins, aussi légitimes soient-elles.

La Commission nationale a décidé après une analyse approfondie d'autoriser les traitements de données liées à la recherche sur les AVC, ainsi que les traitements de données liées à l'étude sur l'évaluation des politiques publiques. Les bases légales de cette décision sont la directive européenne du 24 octobre 1995 qui se prononce sur les traitements ultérieurs de données à des fins historiques, statistiques ou scientifiques, en précisant que des garanties appropriées peuvent être prises pour les données conservées à ces fins, ainsi que la loi du 2 août 2002 sur la protection des personnes à l'égard des traitements de données à caractère personnel dispose que ces traitements sont soumis à l'autorisation préalable de la Commission nationale. La Commission nationale a par conséquent vérifié si la mise en place du traitement de données offre des garanties appropriées. Lors de son travail de contrôle préalable, la Commission nationale vérifie notamment si le traitement peut être réalisé sur base de données rendues anonymes, sinon sur base de données codées ou pseudonymisées le plus tôt possible. Si les données ne peuvent pas être anonymisées, par exemple dans le cadre d'une étude longitudinale qui consiste à suivre des personnes clairement identifiées pendant une certaine durée, la Commission nationale

exige alors que ces personnes soient identifiées à travers un code de recherche aléatoire et qu'une liste de concordance entre l'identité réelle et leur code de recherche, qui ne doit pas être circulée, soit gardée en lieu sûr.

3.3.4 Traitement de données sensibles, biométriques et génétiques

Outre les sujets ayant donné lieu à un avis officiel repris dans les annexes du présent rapport, la Commission nationale a été amenée à étudier en 2008 un certain nombre de questions en rapport avec le traitement des données de santé par les instances médicales et les autorités sanitaires et administratives.

Le projet e-Santé mis en chantier par le Ministère de la santé débouchera à terme sur la création d'un dossier électronique du patient qui contiendra l'historique des soins et traitements dont il a fait l'objet et permettra sous des conditions restant à préciser aux personnel traitant d'accéder aux diagnostics, images et résultats provenant d'analyse et consultations extérieures (auprès d'autres médecins et hôpitaux).

La gestion des identités revêtira un rôle central dans les discussions à mener sur la sécurisation du système, la limitation et le contrôle des accès aux dossiers de même que sur les solutions adoptées au niveau du stockage (décentralisé de préférence) des données relatives aux actes médicaux et de soins et de celles relatives aux patients.

Ces discussions promettent de devenir complexes compte tenu du nombre d'acteurs impliqués et des intérêts en jeu (financiers, techniques et de vie privée).

Des premiers contacts ont eu lieu en 2008 avec le Ministère, avec les organisations de médecins et devront s'étendre prochainement à d'autres intervenants concernés, notamment l'entente des hôpitaux avec laquelle la Commission nationale a prévu de passer également en revue de façon plus détaillée les questions soulevées par l'informatisation de plus en plus poussée des dossiers des patients et par les accès et communications de données au sein même des établissements hospitaliers, voire vers l'extérieur.

En 2005 et 2006 la Commission nationale a autorisé un nombre non négligeable de traitements de données sensibles et relatives à la santé. Ces derniers, bien que très strictement encadrés par les dispositions limitatives des articles 6 et 7 de la loi, ne donnent plus lieu désormais à autorisation préalable. La Commission nationale conserve bien entendu, même après la modification de la loi, le droit d'investiguer et de se prononcer dans le cadre de son pouvoir de contrôle a posteriori.

Parmi les types de traitements de données à caractère personnel qui restent soumis à autorisation, les traitements à des fins de surveillance (article 10 de la loi) et les surveillances sur le lieu de travail mis en œuvre par l'employeur (article 11 de la loi et L.261-1 du Code du Travail) fournissent le plus grand nombre de demandes introduites, encore que le recours à des données biométriques tend lui aussi à générer de plus en plus d'appétits. Les délibérations tournent donc essentiellement autour de la mise en balance des intérêts en cause et de l'appréciation des critères de nécessité et de proportionnalité. Pour le surplus, les questions d'interconnexion de fichiers et d'utilisation à des fins autres que celles pour lesquelles les données personnelles furent initialement collectées sont les plus complexes et les plus délicates. Il s'agit principalement des projets d'études à mener (notamment par les Centres de recherche publics, l'Université, le CEPS-Instead ou d'autres instituts de recherche et de statistiques) qui entendent mettre à contribution des fichiers existants susceptibles de contenir des données utiles à l'enquête.

Dans ce dernier domaine les intérêts mis en avant répondent généralement aux critères de légitimation prévus par la loi, mais c'est la question de la nécessité et de la proportionnalité aux finalités poursuivies qui donne matière à discussion.

Aussi la Commission nationale s'efforce-t-elle de limiter respectivement d'encadrer sérieusement la prolifération de bases de données biométriques et les accès et échanges de données entre les administrations publiques poursuivant des missions distinctes.

Finalement le projet gouvernemental d'implantation en collaboration avec des partenaires étrangers d'une bio-banque à Luxembourg appelée à collecter

des échantillons de tissus, de prélèvement sanguins et d'analyses cliniques et génétiques et à les mettre à disposition de la recherche, a conduit la Commission nationale à s'investir dans l'étude des questions complexes de bioéthique et d'application des principes de la protection des données dans ce domaine très avancé de la recherche biomédicale et à accompagner de ses conseils ce projet ambitieux.

3.4 Investigations

Conformément à la loi modifiée du 2 août 2002, la Commission nationale dispose d'un pouvoir d'investigation en vertu duquel elle recueille toutes les informations nécessaires à l'accomplissement de sa mission de contrôle. A cette fin, elle a un accès direct aux locaux autres que les locaux d'habitation où a lieu le traitement ainsi qu'aux données faisant l'objet du traitement et procède aux vérifications utiles.

C'est ainsi que la Commission nationale a mené des investigations en vue de vérifier le respect des obligations légales suite à des plaintes respectivement des demandes de vérification de licéité d'un traitement, à savoir :

- analyse et la vérification du fonctionnement d'un dispositif de contrôle d'accès basé sur la reconnaissance des empreintes digitales à Mondorf ;
- vérifications sur place d'installation de dispositifs de vidéosurveillance ;
- vérifications sur place de désactivation respectivement enlèvement de dispositifs de vidéosurveillance.

La Commission a également mené des investigations suite à la demande d'action commune de contrôle au niveau européen.

En effet, les autorités de protection des données des Etats membres de l'Union européenne avaient lancé une action coordonnée de contrôle à l'échelle européenne, dans le cadre des activités de leur groupe de travail dit groupe «Article 29». L'objectif de cette action commune avait pour objet les traitements de données personnelles effectués par les entreprises privées offrant des services d'assurance santé dans les 27 Etats membres de l'Union européenne. Ce secteur a été sélectionné pour deux raisons principales, d'une part parce que le traitement de données sensibles est un élément clé des activités en question et d'autre part parce que le non-respect des règles applicables dans ce secteur aurait un impact important sur un grand nombre de citoyens européens.

La Commission nationale a aussi procédé à des actions d'investigation de sa propre initiative (sans qu'une demande n'ait été portée à son attention), se concentrant notamment sur les traitements de données d'envergure ou particulièrement sensibles comme l'analyse à laquelle ont été soumises en 2005/2006 les mesures organisationnelles internes et de sécurité des données pratiquées au Centre Commun de la Sécurité Sociale et de l'Assurance Maladie. Une importance particulière a alors été attachée aux questions de sécurité des infrastructures et des réseaux, de limitation des accès aux données, aux moyens d'empêcher et de constater des fraudes ou des abus ainsi qu'à la responsabilisation et la sensibilisation du personnel.

Une étude similaire est actuellement en cours dans le secteur des communications électroniques. Ainsi la Commission nationale a mené au cours des années 2007-2008 une mission de vérification de la conformité des traitements de données du département «Télécommunications» de l'Entreprise des P&T à la législation sur la protection des données. L'objectif était d'évaluer avec l'aide d'un expert externe le niveau de sécurité appliqué et de contrôler l'implémentation correcte des exigences légales.

A notre grande satisfaction, l'investigation :

- s'est déroulée avec une collaboration volontariste et constructive des responsables de l'entreprise des P&T,
- a fait ressortir que l'entreprise des P&T est très soucieuse des questions relevant de la protection des données de ses clients et

- a permis de constater un niveau très élevé de conformité du traitement des données aux exigences légales.

Néanmoins la Commission nationale a émis dans son rapport final certaines recommandations pour des améliorations supplémentaires à mettre en œuvre au cours des années à venir.

Actuellement la Commission nationale poursuit ses investigations dans ce secteur « sensible » où le public est en droit d'être assuré que la confidentialité des informations relatives aux communications soit rigoureusement respectée. Ainsi au début de l'année en cours, la Commission nationale a choisi d'étendre cette investigation aux opérateurs privés, notamment de téléphonie mobile.

4 Perspectives

La loi a fixé de multiples responsabilités et champs d'action à la Commission nationale. Aujourd'hui, la Commission nationale a atteint son rythme de croisière et elle peut s'attacher davantage à certaines tâches prioritaires découlant de sa mission notamment celle de renseigner les citoyens en ce qui concerne le respect de leurs droits, d'informer les responsables de fichiers sur leurs obligations, de promouvoir les bonnes pratiques en la matière et de veiller au respect des principes légaux par le biais de contrôles et d'investigations et d'une guidance constructive appliquée aux situations concrètes.

Etant sur le point de résorber en cours d'année, le retard accumulé dans l'examen des demandes d'autorisation en souffrance, la Commission nationale peut se consacrer à d'autres champs d'activités. La Commission nationale peut dorénavant faire face de façon équilibrée à ses différentes missions étant donné qu'elle s'est largement dégagée de la part importante occupée pendant longtemps par ses fonctions purement administratives.

Parmi les priorités qui seront développées à l'avenir, on peut citer des efforts en termes de guidance. Le but est notamment celui de mieux faire connaître les décisions de la Commission nationale, afin de créer un effet boule de neige à travers un mécanisme d'entraînement qui pousse d'autres acteurs à prendre mieux en compte la protection des données. Il s'agit d'avancer, en coopération avec les autorités et les professionnels, dans la recherche de solutions praticables et dans la publication de recommandations thématiques et sectorielles. A travers ces efforts, le but est d'encourager les acteurs qui traitent des données personnelles à adopter des bonnes pratiques. Des documents de guidance pourront ainsi être publiés à propos de la vidéosurveillance ou encore de la surveillance des communications électroniques sur le lieu de travail.

La Commission nationale portera aussi une attention particulière à la sensibilisation des jeunes. Des sondages ont en effet montré que plus les personnes étaient jeunes, moins elles étaient sensibles au sujet. La propagation du recours à Facebook et à d'autres communautés virtuelles, en particulier parmi les jeunes, impose de renforcer le travail de sensibilisation en direction de ce public par rapport aux risques de ces plateformes de communication.

La Commission nationale s'est fixée pour but de mener des contrôles ponctuels concentrés sur des cas graves et des investigations menées spontanément à titre préventif pour des fichiers importants et sensibles où la confiance du public dans certaines institutions exige que le respect de la loi soit parfaitement assuré.

Les cas récents de vols de données personnelles en Allemagne ont suscité de l'intérêt au Luxembourg. Le débat a été déclenché lorsque la centrale de consommateurs du Land de Schleswig-Holstein a reçu début août 2008 un CD-Rom avec les données de 17.000 personnes. Ces données, comprenant entre autres des numéros de téléphone personnels et des numéros de comptes bancaires, circulaient de façon illicite et avaient été utilisées par un «Call center» (centre d'appel) pour retirer de l'argent de comptes bancaires, sans accord des détenteurs des comptes. Ce cas de fraude a suscité un vif intérêt de la part de plusieurs députés qui ont ainsi posé des questions parlementaires à Monsieur le Ministre des Communications, s'interrogeant notamment si la protection des consommateurs luxembourgeois était adéquate.

Les cas allemands de trafic de données confidentielles ont montré que la protection des données ne concerne pas que l'Etat et les communes, mais aussi le secteur privé. Apparemment le scandale de trafic de données privées en Schleswig-Holstein n'était que la face émergée de l'iceberg. Des supports de données contenant des millions de paquets de données issues du marché noir de la revente de noms et d'adresses de clients circuleraient ainsi en Allemagne. Elles contiennent des noms, adresses, numéros de téléphone et aussi de nombreux numéros de comptes bancaires de personnes qui avaient apparemment achetées des billets de Lotto chez certaines sociétés allemandes de Lotto, abonnées à des journaux ou à des revues ou avaient encore participé à des loteries ou à des sondages par Internet.

Le législateur allemand s'apprête par ailleurs à renforcer par une loi spécifique la protection de la vie privée des salariés face à la tentation de certains

employeurs peu scrupuleux de vouloir espionner le comportement de leur personnel ainsi que leur vie privée, y compris en dehors du lieu de travail. Les scandales (Télécom, Lidl, DB) révélés par la presse démontrent que le législateur luxembourgeois n'a pas introduit à la légère des dispositions limitant les atteintes aux libertés et droits fondamentaux et à la vie privée des travailleurs sur le lieu de travail (ancien article 11 de la loi du 2 août 2002; article L. 261-1 du Code de travail) en instaurant un contrôle a priori de la légitimité, nécessité et proportionnalité des traitements à des fins de surveillance mis en œuvre par l'employeur.

De l'avis de la Commission nationale, il lui reste toutefois à compléter encore le catalogue limitatif des cas d'ouverture par quelques hypothèses qui pourraient être considérées dans certaines circonstances comme justifiant une surveillance limitée mais nécessaire (« *1° pour assurer la prévention, la recherche et la détection d'actes illicites ou susceptibles d'engager la responsabilité de l'employeur ; 2° pour la protection des intérêts économiques, commerciaux ou financiers de l'employeur ; 3° pour des besoins de formation des travailleurs ou l'évaluation et l'amélioration de l'organisation du travail* ») reconnue également comme légitime et non excessive dans d'autres pays européens si la balance des intérêts met en évidence des risques réels pour l'employeur. La Commission nationale maintient à cet égard ses recommandations formulées dans son avis du 5 décembre 2005 relatif au projet de loi N°5554 portant modification de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (révision de la loi).

Les lacunes actuelles sapent à notre avis la crédibilité du régime légal d'encadrement de la surveillance exercée sur le lieu du travail par ailleurs très protecteur pour le respect de la vie privée des travailleurs et pourraient même dans des cas isolés se révéler comme obstacles au bon fonctionnement des entreprises ou comme facteurs défavorables sur le plan de l'attractivité économique du site luxembourgeois. Le rajout de critères de légitimation supplémentaires, à l'endroit de l'article L. 261-1 du Code de travail, n'aura pas comme effet d'abaisser le niveau de protection des droits et libertés fondamentaux des travailleurs, alors que les traitements à des fins de surveillance sur le lieu de travail, dans les cas de figure visés, resteront bien évidemment soumis à un contrôle a priori par la Commission nationale à travers la procédure de l'autorisation préalable, contrairement à ce que prévoient les régimes des autres pays européens en la matière. Une garantie supplémentaire pourrait consister à soumettre ces traitements à l'accord préalable du comité mixte d'entreprise.

Depuis la conférence internationale de Montreux (septembre 2005), la communauté des commissaires à la protection de la vie privée et des données personnelles fait état de la nécessité d'adaptation de leur cadre d'action aux réalités technologiques, politiques, économiques et sociales globalisées d'aujourd'hui.

Les défis recensés découlent notamment de l'évolution fulgurante d'Internet et des technologies de l'information et de la communication, des techniques de marketing devenues de plus en plus agressives qui poussent le traçage et le profilage comportemental jusqu'aux derniers recoins de notre vie privée, des mesures mises en place par les pouvoirs publics pour la sauvegarde de la sécurité publique face à la résurgence des menaces terroristes et appellent des réponses globales pour la protection des libertés publiques et droits fondamentaux des citoyens.

Dans un monde sans frontières la protection de la vie privée doit pouvoir être considérée et revendiquée comme droit universel applicable à l'échelle de la planète ce qui présuppose un rapprochement des conceptions juridiques et pratiques.

On parle de convergence nécessaire entre les approches de la « privacy » américaine et du bassin d'Asie/ Pacifique avec nos valeurs européennes et latines.

Dans ce contexte de renouveau et de revitalisation du droit à la protection des personnes à l'égard du traitement des données à caractère personnel, les représentants de la CNPD luxembourgeoise s'apprêtent à participer aux discussions qui auront lieu au niveau de l'Union européenne et du Conseil de l'Europe.

Les 19 et 20 mai 2009 la Commission européenne organise à Bruxelles un grand colloque autour des nouveaux défis

que soulève le recours accru aux données personnelles et lancera ainsi implicitement le long processus de réflexion qui conduira à terme à la révision de la directive 95/46/CE sur la protection de données.

Une telle démarche, de par la remise en question des solutions existantes, recèle certes par nature des risques et des opportunités.

L'objectif ultime de la modernisation de la directive consiste à rendre le cadre légal communautaire plus effectif en termes de protection réelle des citoyens face aux dangers significatifs pour leurs libertés et leur vie privée et à le refaçonner en simplifiant certains instruments juridiques et en mettant un accent plus poussé sur des incitations positives, amenant les organisations à mieux mettre en pratique dans leurs activités de tous les jours les règles applicables.

5 Ressources, structures et fonctionnement de la Commission nationale

5.1 Rapport de gestion relatif aux comptes de l'exercice 2008

L'activité de la Commission nationale au cours de l'année 2008 a été marquée par :

- la formation et l'intégration des nouveaux collaborateurs ;
- l'optimisation de l'infrastructure informatique et des procédures internes et le traitement d'un nombre substantiel de demandes d'autorisation introduites ;
- la concertation avec de nombre ministères et d'organismes publics au sujet de dossiers et projets justifiant des recommandations relatives aux traitements de données personnelles ;
- l'examen de l'important projet de loi no 5950 relatif à l'identification des personnes physiques, au registre national des personnes physiques et à la carte d'identité ;
- l'adoption d'une dizaine d'autres avis relatifs à des projets de loi ou règlements grand-ducaux ;
- les actions menées en vue de la sensibilisation du public et de la guidance des responsables de traitements, notamment à travers le site Internet www.cnpd.lu, diverses séances d'information et la participation à la journée européenne de la protection des données ;
- les investigations menées en vue de vérifier le respect des obligations légales dans le secteur des communications électroniques en commençant par l'Entreprise des P&T.

Dépenses de fonctionnement

Les loyers et charges locatives supportés pour les locaux provisoires de la CNPD (pris en location dans l'attente de son implantation dans le 1er bâtiment administratif à ériger par l'Etat à Belval-Ouest) ont atteint 92.109,96.- € et sont en ligne avec les prévisions.

Les effectifs en personnel de la Commission nationale se composaient en 2008 outre des trois membres effectifs, de deux fonctionnaires de la carrière moyenne (rédacteurs) prenant en charge les formalités légales de déclaration et autorisation préalable, d'un employé de l'Etat et d'un employé bénéficiant du statut de travailleur handicapé assurant le secrétariat et l'administration, de quatre attachés à la direction stagiaires dont trois affectés au service juridique et un à la communication et à la documentation.

Les charges relatives au personnel permanent ont progressé par rapport à l'exercice 2007 principalement du fait du renforcement des effectifs par un attaché à la communication. Néanmoins compte tenu du fait que le poste d'employé administratif au secrétariat ainsi que le poste d'attaché à la communication n'ont été que partiellement occupés en 2008 les dépenses sont restées en-dessous des prévisions.

Un rédacteur stagiaire supplémentaire viendra rejoindre les effectifs en personnel au cours de l'exercice 2009 au cours duquel les juristes attachés de direction passeront l'examen de fin de stage.

Un grand effort fut accompli au cours de l'exercice 2008 permettant de résorber le retard dans l'enregistrement des notifications reçues en application des articles 12 et 13 de la loi et d'accélérer substantiellement le traitement des demandes d'autorisation dont il reste plusieurs centaines à examiner par la Commission nationale.

Le niveau des mesures de sécurité organisationnelle et technique qui représente un volet important des garanties appropriées pour la protection des données personnelles est vérifié dans chaque dossier d'autorisation préalable. Cet aspect a donné lieu par ailleurs en cours de l'exercice 2008 à diverses investigations dont la Commission nationale a pris l'initiative depuis 2005 même en dehors des plaintes et demandes de vérification dans les secteurs de la sécurité sociale, de l'assurance maladie complémentaire mutuelle ou privée et dans celui des communications électroniques.

Pour les audits et vérifications à effectuer à ce niveau, la Commission nationale a eu recours à un expert externe spécialisé dans les questions de sécurité informatique et de bonnes pratiques organisationnelles.

Parmi les dépenses d'honoraires et frais d'experts et prestataires externes figurent également les honoraires d'avocats et factures de la fiduciaire qui tient la comptabilité et établit le bilan de l'établissement public.

Les frais d'entretien des locaux, les fournitures de bureau, frais de port et de télécommunications et autres charges générales d'exploitation ont connu une progression linéaire suivant l'augmentation du nombre de collaborateurs en activité.

Le dépassement des prévisions budgétaires au niveau des dépenses d'information du public et de communication (67.033,87€) s'expliquent par la nécessité de faire connaître les nouvelles dispositions introduites par la loi du 27 juillet 2007 (entrée en vigueur le 1er septembre 2007 modifiant la loi du 2 août 2002).

Les frais de déplacement et de séjour à l'étranger sont relatifs à la participation des membres effectifs de la Commission nationale aux différentes réunions, séances de travail et conférences organisées sur le plan européen dans le domaine de la protection des données où le Luxembourg se doit d'être représenté.

Les frais relatifs à la gestion et maintenance des systèmes et réseaux ont connu une augmentation par rapport aux estimations budgétaires en raison de l'optimisation de l'infrastructure informatique au sein de la Commission nationale.

Les amortissements comptabilisés atteignent un montant total 28.180,56€.

Le total des frais de fonctionnement encourus par l'établissement public au cours de l'exercice 2008 s'élève à 1.406.519,28€.

Investissements

Au cours de l'exercice 2008 les dépenses d'investissement effectuées restent à un niveau très modeste. Une augmentation n'est toutefois pas à exclure, en particulier pour une mise à niveau du site Internet et une implémentation de la signature électronique dans les formulaires existants qui devraient être adaptés en conséquence et au cours des exercices à venir.

Recettes

Le montant des redevances perçues en application des articles 37 paragraphe (4) et 13 paragraphe (4) de la loi s'élevant à 67.196€ est resté conforme à nos prévisions. En outre des produits financiers (intérêts créditeurs) ont pu être enregistrés à hauteur de 13.832,55€.

Résultat d'exploitation

Compte tenu de la dotation annuelle de 1.395.480€ dont la Commission nationale a bénéficié en 2008 de la part de l'Etat en application de l'article 37 paragraphe (4) de la loi, le résultat d'exploitation de l'établissement public s'établit à 69.989,27€ au 31 décembre 2008 qui sera reporté à nouveau sur l'exercice suivant.

5.2 Renouvellement du mandat de la Commission nationale

Par arrêté grand-ducal du 7 octobre 2008, les mandats des membres de la CNPD ont été renouvelés pour une durée de six ans. La Commission nationale se compose dorénavant des membres titulaires suivants : Gérard Lommel, Thierry Lallemang et Pierre Weimerskirch (membres effectifs), ainsi que de Josiane Pauly, Marc Hemmerling et Tom Wirion (membres suppléants).

5.3 Personnel et services mis en place

La procédure à suivre et le fonctionnement de la Commission nationale ont été formalisés par un règlement intérieur (adopté le 29 novembre 2002) et un schéma de notification (adopté le 26 février 2003 et actuellement en voie de modification pour tenir compte des récentes modifications légales). Les avis prévus à l'article 43 paragraphe 1er de la loi ont été publiés dans les quotidiens le 7 mars 2003 et au Mémorial B N°22 du 11 avril 2003.

Conformément à son règlement intérieur, les services suivants ont été mis en place depuis 2003 :

- service juridique et de documentation ;
- service informatique et de la logistique ;

- tenue du registre public et prise en charge administrative des notifications, demandes d'autorisation et requêtes diverses ;
- administration générale et finances ;
- service presse et communication.

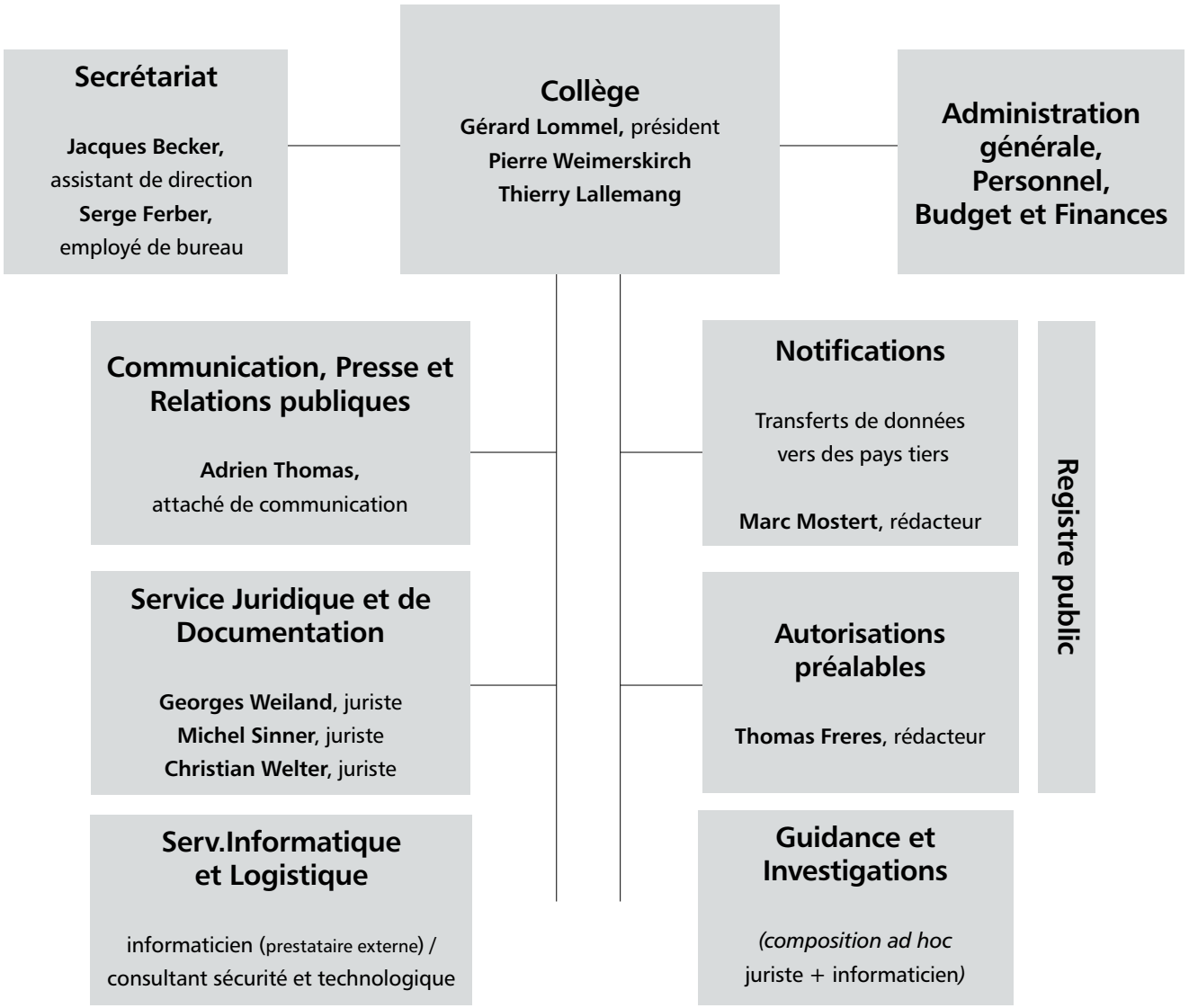
Membres effectifs
Gérard LOMMEL, président (juriste) Thierry LALLEMANG (juriste) Pierre WEIMERSKIRCH (informaticien)
Membres suppléants
Josiane PAULY (juriste) Marc HEMMERLING (informaticien) Tom WIRION (juriste)
Service juridique et de documentation
Georges WEILAND, juriste Michel SINNER, juriste Christian WELTER, juriste
Tenue du registre public et prise en charge administrative des notifications et demandes d'autorisations
Marc MOSTERT, rédacteur principal Thomas FRERES, rédacteur principal
Service informatique et de la logistique
Administration générale et finances
Jacques BECKER, assistant de direction Serge FERBER, assistant administratif
Service presse et communication
Adrien THOMAS, attaché de communication

En 2008 les effectifs permanents ont été portés de 8 à 11 fonctionnaires et employés publics (y compris les 3 membres permanents). Il s'agit de la titularisation des juristes et de l'engagement d'un attaché à la communication et à la documentation. Un poste supplémentaire de rédacteur sera pourvu seulement au cours de l'année 2009.

5.4 Bureaux

La Commission nationale occupe actuellement des bureaux provisoires à Luxembourg, 41 avenue de la Gare, au 4ème étage, bureaux qu'elle occupe depuis l'époque où les locaux du 68, rue de Luxembourg à Esch-sur-Alzette se sont avérés trop exigus pour être partagés avec l'antenne régionale de l'Inspection du Travail et des Mines. Elle conserve toutefois son siège officiel à Esch-sur-Alzette où il est prévu qu'elle emménage dans l'enceinte du « 1er Bâtiment administratif » que l'Etat construit sur le site des friches industrielles de Belval-Ouest. L'adoption récente par la Chambre des Députés de la loi du 19 décembre 2008 autorisant la construction de ce bâtiment permet de prévoir pour le début de l'année 2012 la localisation définitive de la Commission nationale à Esch-sur-Alzette qui s'inscrit dans le cadre de la politique de décentralisation des administrations publiques.

5.5 Organigramme de la Commission nationale



6 La Commission nationale en chiffres

• *Formalités préalables*

	2003	2004	2005	2006	2007	2008	
a) Notifications							**TOTAL**
- notifications ordinaires	2.646	850	500	250	760	385	5.391
- notifications simplifiées	750	900	720	890	537	-	3.797
- engagements de conformité	-	-	-	-	-	942	942
(Total a)	**3.396**	**1.750**	**1.220**	**1.140**	**1.297**	**1.327**	**10.130**
b) Autorisations préalables							
- demandes d'autorisation	765	406	317	295	392	606	2.781
- engagements de conformité	718	14	17	19	151	220	1.139
(Total b)	**1.483**	**420**	**334**	**314**	**543**	**826**	**3.920**
(Total général a) + b))	**4.879**	**2.170**	**1.554**	**1.454**	**1.840**	**2.153**	**14.050**
Déclarants (responsables ayant accompli des formalités)	2.220	2.500	2.850	3.300	3.754	4.357	

• *Demandes de renseignements*

	2004	2005	2006	2007	2008
a) Demandes de renseignements par courrier					
- administrations publiques	18	7	8	6	5
- entreprises	49	10	8	5	12
- professions libérales	3	4	9	2	2
- citoyens	12	9	7	12	8
- associations	7	5	2	4	3
(Total a)	**89**	**35**	**34**	**29**	**30**
b) Demandes de renseignements par courriel					
(Total b)	**67**	**82**	**116**	**119**	**108**
c) Demandes de renseignements par téléphone					
(Total c)	**1.780**	**1.550**	**1.930**	**1.870**	**1.586**
(Total général a) + b) + c))	**1.936**	**1.667**	**2.080**	**2.018**	**1.724**

• *Plaintes et investigations*

	2003	2004	2005	2006	2007	2008
- plaintes, demandes de vérification de licéité et investigations :	**15**	**38**	**40**	**30**	**34**	**63**

• *Séances de délibération*

	2004	2005	2006	2007	2008
	39	36	39	40	40

• *Participations aux groupes de travail sur le plan européen*

	2004	2005	2006	2007	2008
	28	33	23	22	22

• *Prises de contacts et concertations avec des organisations représentatives sectorielles ou acteurs*

	2004	2005	2006	2007	2008
- secteur public	47	62	32	56	52
- secteur privé	30	38	12	40	44
(Total)	**77**	**100**	**44**	**96**	**96**

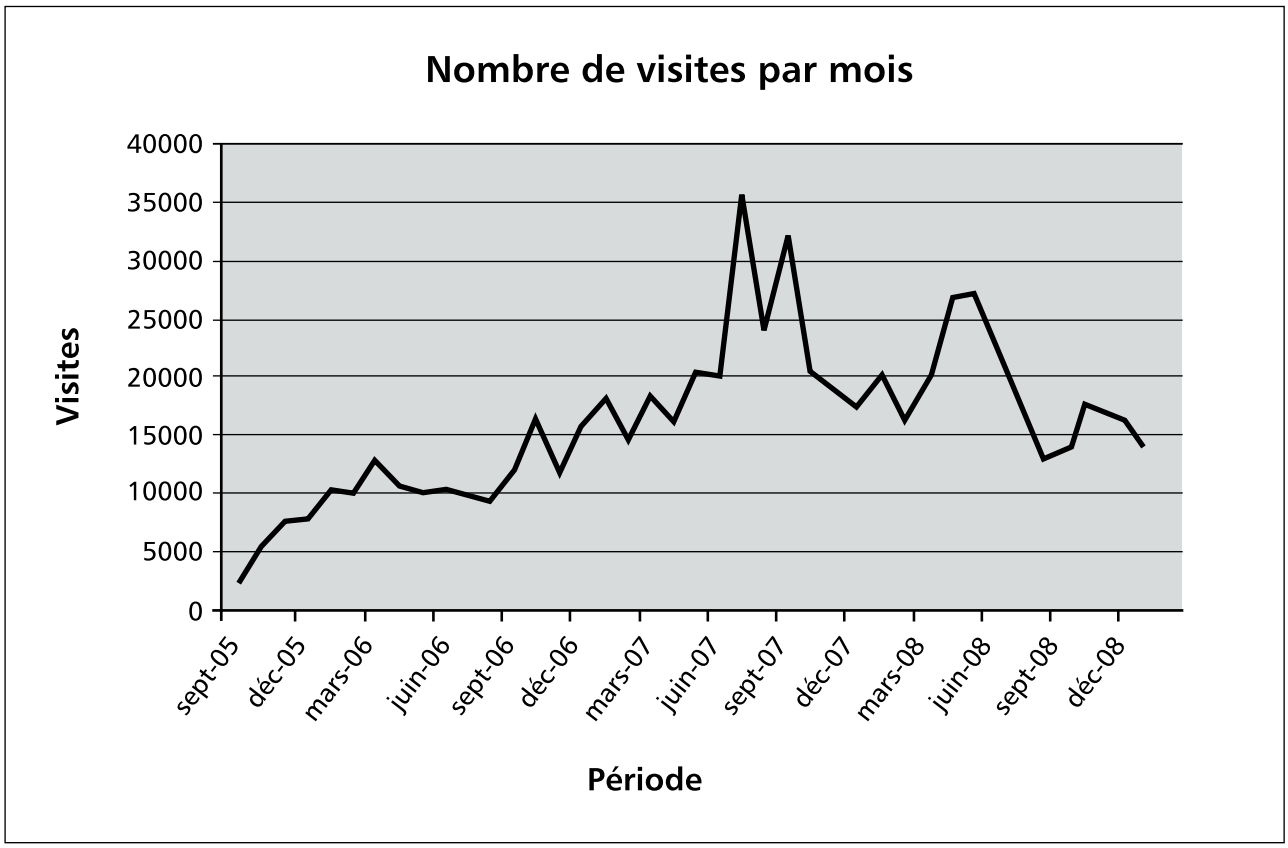
• *Séances d'information, conférences, exposés*

	2004	2005	2006	2007	2008
	4	10	11	14	11

• *Reflets de l'activité de la Commission nationale dans la presse*

	2004	2005	2006	2007	2008
Articles et interviews parus dans :					
- les quotidiens	14	16	67	127	59
- les hebdomadaires	5	6	4	9	11
- les mensuels	0	7	5	4	2
- les médias audiovisuels	1	3	3	3	16
(Total)	**20**	**32**	**79**	**143**	**88**

• *Fréquentation du site Internet*



ANNEXES

Avis et décisions

Avis de la Commission nationale pour la protection des données concernant le projet de loi n°5802 portant sur la libre circulation des personnes et l'immigration

Délibération n°1/2008 du 11 janvier 2008

Conformément à l'article 32 paragraphe (3) lettre (e) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après désignée « la loi du 2 août 2002 »), la Commission nationale pour la protection des données a notamment pour mission d'« être demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi ».

C'est dans cette optique, et faisant suite à la demande lui adressée par Monsieur le Ministre des Affaires étrangères en date du 25 octobre 2007 que la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet du projet de loi pré-mentionné.

La Commission nationale entend limiter son avis aux dispositions traitant des aspects de la protection des données, dispositions qui se trouvent insérées dans le chapitre six du projet de loi sous examen relatif aux contrôles sur les conditions d'entrée et de séjour des étrangers.

Remarques préliminaires

Le projet de loi sous examen transpose un ensemble de directives européennes[1] ayant trait à l'entrée et au séjour des étrangers. Les auteurs du projet de loi sous examen entendent également adapter la législation sur l'immigration aux réalités actuelles des flux migratoires et du marché du travail.

Les directives en question reconnaissent aux Etats membres la possibilité de procéder à des contrôles sur les conditions d'entrée et de séjour des étrangers.

Force est de constater que les dites directives laissent aux Etats membres le soin de dégager les moyens à employer pour rendre effectif ce contrôle. A cet effet, le projet de loi donne la possibilité au ministre chargé de l'immigration et aux personnes agissant en son nom, de bénéficier d'un accès informatique direct aux bases de données limitativement énumérées à l'article 139 et dont les responsables sont d'autres administrations et organismes étatiques. Ces fichiers contiennent des informations utiles aux contrôles requis par le projet de loi sous examen.

Le projet de loi ne donne pas d'information sur l'organisation concrète des accès informatiques directs aux différents fichiers des administrations et organismes publics visés à l'article 139. En l'absence de précision sur la façon dont cette communication ou ce partage de données à caractère personnel sera implémenté en pratique, ni sur l'architecture informatique choisie, la Commission nationale part du postulat, dans le présent avis, que les accès auront lieu dans le cadre d'une interconnexion de données.

Les recommandations que la Commission nationale formule ci-après, notamment dans la conclusion du présent avis, s'avèrent toutefois également justifiées et transposables à l'hypothèse de communications ou de partages de données autres que sous forme d'interconnexion.

1 Et plus précisément les directives 2003/86/CE du Conseil du 22 septembre 2003 relative au regroupement familial, 2003/109/CE du Conseil du 25 novembre 2003 relative au statut des ressortissants de pays tiers résidents de longue durée, 2004/38/CE du Parlement européen et du Conseil du 29 avril 2004 relative au droits des citoyens de l'Union et des membres de l'Union et des membres de leur famille de circuler et de séjourner librement sur le territoire des Etats membres, 2004/81/CE du Conseil du 29 avril 2004 relative au titre de séjour délivré aux ressortissants de pays tiers qui sont victimes de la traite des êtres humains ou ont fait l'objet d'une aide à l'immigration clandestine et qui coopèrent avec les autorités compétentes, 2004/114/CE du Conseil du 13 décembre 2004 relative aux conditions d'admission des ressortissants de pays tiers à des fins d'études, d'échange d'élèves, de formation non rémunérée ou de volontariat, 2005/71/CE du Conseil du 12 octobre 2005 relative à une procédure d'admission spécifique des ressortissants de pays tiers aux fins de recherche scientifique.

Les textes légaux ou réglementaires autorisant une interconnexion de données doivent respecter la *ratio* des dispositions de l'article 16 de la loi du 2 août 2002[2]. Conformément à son paragraphe (1), l'interconnexion peut valablement être autorisée par voie légale.

La Commission nationale se propose d'analyser le projet de loi sous examen en passant en revue les différentes conditions posées aux paragraphes (2) et (3) dudit article 16.

Ainsi, le paragraphe (3) en question traite-t-il des finalités des traitements interconnectés. Le paragraphe (2) pose quatre conditions cumulatives supplémentaires à savoir 1) des objectifs légaux ou statuaires présentant un intérêt légitime pour les responsables du traitement, 2) le fait de ne pas entraîner de discrimination ou de réduction des droits, libertés et garanties pour les personnes concernées, 3) la mise en place de sécurité appropriées et 4) la qualité des données faisant l'objet de l'interconnexion.

1. La compatibilité des finalités des traitements interconnectés

En vertu du paragraphe (3) de l'article 16 de la loi du 2 août 2002, les finalités des fichiers interconnectés doivent être compatibles entre elles.

La notion de « compatibilité » n'est pas définie par la loi. Le critère de compatibilité est lié à l'un des principes majeurs de la législation de protection des données, à savoir la transparence des traitements de données à l'égard des personnes concernées par les données[3].

Ce critère est traditionnellement interprété comme signifiant prévisible par les personnes concernées, cette prévisibilité pouvant d'ailleurs naître seulement postérieurement à la collecte des données, par exemple par le seul fait d'une disposition légale ou réglementaire prévoyant l'utilisation ultérieure des données pour une finalité nouvelle.

En l'espèce, la personne qui demande à entrer et/ou séjourner au Grand-Duché doit fournir les justificatifs relatifs à sa condition de ressources et/ou son activité professionnelle et, dans le cadre du regroupement familial, il doit justifier ses liens familiaux et décliner l'identité de ces personnes. En vertu du principe de la préférence communautaire, les non-ressortissants des Etats membres doivent encore justifier que le poste qu'il souhaite pourvoir ne peut être occupé par un ressortissant européen.

Du fait que la personne étrangère doit fournir l'ensemble des pièces justificatives, elle doit pouvoir légitimement s'attendre à ce que l'administration chargée de lui remettre les autorisations d'entrée et de séjour procède à des vérifications subséquentes et ce afin d'écarter toute éventuelle fraude.

Par conséquent, les finalités des traitements interconnectés sont compatibles au sens de l'article 16 paragraphe (3) de la loi du 2 août 2002.

La Commission nationale entend encore préciser qu'en vertu de l'article 4 paragraphe (1) lettre (a) de la loi du 2 août 2002, les données sont collectées pour des finalités déterminées, explicites et légitimes et ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités : en d'autres mots, les personnes procédant aux contrôles institués aux articles 134 à 139 du projet de loi sous examen, ne doivent pas profiter de l'accès à ces fichiers pour un usage autre que le contrôle des conditions d'entrée et de séjour des étrangers. Dans le cas contraire, il y aurait une utilisation qui dépasse le cadre de la finalité initiale, voire un détournement de finalité.

2. Les objectifs présentant un intérêt légitime pour les responsables du traitement

L'objectif recherché par la personne qui accède aux fichiers d'un autre responsable du traitement doit être inscrit, soit dans la loi, soit dans ses statuts.

Chacun des responsables du traitement, dont les données sont interconnectées, a un intérêt légitime

2 doc. parl. N° 4735/13, p. 30

3 « La Protection de la vie privée dans la société de l'information », Tomes 3 à 5, Chapitre 4, Cécile de Terwangne, pages 91 et suivantes, éd. Presse Universitaires de France, Cahier des sciences morales et politiques

individuel au niveau du traitement qui les concerne directement et dont il en a la charge.

De plus, il ressort clairement du projet de loi et des commentaires et exposés des motifs données par les auteurs de la loi que la finalité poursuivie par les auteurs du projet de loi est de combattre la fraude dans les demandes d'entrée et de séjour des étrangers.

3. L'absence de discrimination ou de réduction des droits, libertés et garanties pour les personnes concernées

En vertu du principe selon lequel l'interconnexion ne doit pas conduire à une discrimination ou une réduction des droits, libertés et garanties pour les personnes concernées, la balance entre les intérêts des responsables du traitement et les intérêts des personnes concernées doit être maintenue en équilibre.

En d'autres mots, si l'interconnexion permet d'obtenir par des moyens simples et rapides des informations sur une personne, cela ne doit pas se faire au détriment de ses droits et libertés.

L'interconnexion doit dès lors être nécessaire pour atteindre la finalité poursuivie. La Commission nationale relève à ce propos que dans la perspective de rechercher la fraude à la législation sur l'immigration, l'interconnexion aux fichiers détaillés à l'article 139 du projet de loi est une opération nécessaire. En effet, dans le cas contraire, le ministre chargée de l'immigration – ainsi que les personnes qui agissent sous son autorité – devra à chaque fois faire une demande expresse auprès de chacune des administrations concernées, ce qui conduit à une perte de temps significative.

De plus, le recours aux fichiers interconnectés doit être justifié. En effet, ces fichiers n'ont pas été créés dans le but de rechercher les fraudes aux conditions d'entrée et de séjour des étrangers, de sorte que leur consultation doit être limitée. Cette condition nous semble être remplie en l'espèce au vu de l'alinéa 3 *in fine* de l'article 139 du projet de loi sous examen.

Ensuite, toujours dans la perspective de ne pas conduire à une discrimination ou de porter atteinte aux droits, libertés et garanties des personnes concernées, les contrôles doivent porter exclusivement sur l'entrée et le séjour des étrangers.

4. Les mesures de sécurité

Le droit de la protection des données s'appuie sur l'idée fondamentale que le responsable du traitement doit s'assurer que les données à caractère personnel qu'il détient soient traitées loyalement et licitement et ne soient pas ultérieurement traitées de manière incompatible avec les finalités déterminées et légitimes pour lesquelles il les a initialement collectées ou obtenues. En particulier, il doit s'en assurer lorsqu'il communique ces données à des destinataires ou lorsque des personnes placées sous son autorité directe sont habilitées à traiter les données. Il a également l'obligation de mettre en œuvre toutes les mesures techniques et l'organisation appropriées pour assurer la sécurité des traitements.

A cela s'ajoute que l'interconnexion de données est une opération délicate qui doit être entourée d'un maximum de garanties[4].

Dans le projet de loi sous examen, le mode de transmission des données est passif en ce sens que le ministre chargé de contrôler les conditions d'entrée et de séjour des étrangers – ainsi que les personnes qui agissent sous son autorité – peut directement accéder aux différents fichiers énumérés à l'article 139 du dit projet de loi, sans intervention des responsables des différents fichiers consultés.

Le responsable du traitement étant en quelque sorte le garant des données et de la compatibilité des finalités, il doit veiller à ce que la communication des données à caractère personnel à un tiers se fasse selon le même principe de finalité et soit compatible avec le traitement initial.

Le principe de responsabilisation adopté par la loi du 2 août 2002 ne paraît pas conciliable avec le cas de figure envisagé où des données à caractère personnel

4 Avis du Conseil d'Etat du 30 janvier 2007 relatif au projet de loi n°5554

pourraient être consultées, extraites, copiées par un tiers - fussent-ils des autorités administratives centralisées dans le cadre de leurs missions légales - à l'insu des responsables des différents traitements qui assumeraient, dans des conditions difficiles, la sécurité et la confidentialité de leurs traitements respectifs.

Dès lors, des mesures de sécurité renforcées doivent être adoptées.

Dans le cadre de ces mesures, le projet de loi précise à l'article 139 alinéa (2) qu'un règlement grand-ducal déterminera les catégories de personnes qui seront habilitées et autorisées à accéder aux fichiers interconnectés et l'alinéa (3) dudit article prévoit encore le traçage des accès.

La Commission nationale est satisfaite que les auteurs prévoient des mesures de protection.

Elle recommande toutefois d'inscrire dans la loi le principe de garantie pour assurer la confidentialité des données et la sécurité des traitements conformément aux articles 21 à 23 de la loi du 2 août 2002.

De plus, dans les limites des règles de l'art et de ce qui est techniquement réalisable, la Commission propose aussi un accès parcellaire aux traitements interconnectés : l'accès doit être possible uniquement aux données qui intéressent le ministère et non pas à l'intégralité des données figurant sur les fichiers et relatifs à la personne sur qui la recherche et le contrôle sont effectués. A cet effet, la première phrase du dernier alinéa de l'article 139 du projet de loi pourrait, par exemple, être complétée de la manière suivante :

> « *Le système informatique par lequel l'accès direct est opéré doit être sécurisé de façon appropriée et aménagé* (…) ».

5. Les données faisant l'objet de l'interconnexion

L'article 16 paragraphe (2) de la loi prévoit que le type de données doit être pris en compte dans l'opération d'interconnexion dans le souci de vérifier que les garanties pour les personnes concernées sont appropriées.

Les auteurs du projet de loi sous examen laissent le soin au pouvoir réglementaire de déterminer les données qui peuvent faire l'objet d'un accès dans le cadre de l'article 139.

Au stade actuel, le législateur se trouve dès lors dans l'impossibilité d'apprécier et d'identifier les catégories de données qui feront l'objet d'une communication ou d'un partage de données à caractère personnel.

Il lui est donc difficile de vérifier s'ils sont entourés de garanties suffisantes.

La Commission nationale recommande donc que le projet de loi soit complété par une indication précise et détaillée des données échangées par les différents organismes publics.

Si les auteurs du projet de loi ne souhaitent pas figer cette énumération dans le projet de loi, cette précision pourra alternativement faire l'objet d'un projet de règlement grand-ducal. Il serait préférable que celui-ci soit disponible avant la fin de la procédure législative. La Commission note que, dans une hypothèse similaire, un projet de loi[5] est actuellement analysé ensemble avec les projets de règlement grand-ducaux y relatifs.

Conclusion

La Commission nationale estime que le projet de loi sous examen est conforme aux prescriptions de la législation en matière de protection des données à caractère personnel, sous réserve des limitations qui suivent.

Tout d'abord, l'usage des données à caractère personnel faisant l'objet de la communication ou du partage des données prévues à l'article 139 du projet de loi doit être limité à la finalité prévue, à savoir les contrôles des conditions relatives à l'entrée et au séjour des étrangers pour y déceler des éventuelles fraudes.

5 Projet de loi n° 5563 relative à l'accès des magistrats et officiers de police judiciaire à certains traitements de données à caractère personnel des personnes morales de droit public et portant modification du code d'instruction criminelle et de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la Police

La Commission nationale propose également que le projet de loi intègre une énumération des données, respectivement les catégories de données partagées et échangées sinon de la prévoir dans un projet de règlement grand-ducal qui soit disponible pendant la procédure législative.

Il est encore souhaitable de voir insérer dans le corps même du projet de loi le principe de garantie dans la perspective d'assurer la sécurité et la confidentialité des données. Dans les limites de ce qui est techniquement possible et des règles de l'art, l'accès doit être limité aux seules données qui intéressent le ministre chargé de l'immigration et non pas à l'intégralité des traitements des autres administrations et organisations étatiques.

Enfin, les recommandations formulées ci-avant sont, le cas échéant, également valables dans l'hypothèse où la communication ou le partage de données ne constituerait pas une interconnexion.

Délibération de la Commission nationale pour la protection des données relative à la demande de l'Institut Luxembourgeois de Régulation concernant la procédure « article 41 » de la loi du 2 août 2002

Délibération n° 166/2008 du 20 juin 2008

I. Contexte

Dans sa délibération du 25 mai 2007, la Commission nationale pour la protection des données a autorisé, à la demande de l'Institut Luxembourgeois de Régularisation (ILR), la mise en place du système entièrement automatisé de l'accès de plein droit prévu par l'article 41 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, en jugeant suffisantes les mesures de sécurité détaillées dans les documents soumis par l'ILR.

Avant la mise en service de ce système, l'ILR avait fait réaliser un audit externe par la société Ernst & Young. Cet audit avait pour mission d'identifier d'éventuelles faiblesses du système dénommé « Article 41 ». Le rapport conséquent du 22 octobre 2007 avait ensuite conclu que certains objectifs de sécurité n'étaient pas atteints, notamment pour la raison que l'ILR avait encore entièrement mainmise sur le système Anti-Abus.

Suite à ce rapport, l'ILR s'est efforcé de mettre en œuvre certaines recommandations lui soumises (rapport du 6 décembre 2007) et a également fait réaliser une étude intitulée « Analyse des risques et des impacts » par Fujitsu Services et Ubizen concernant le système d'information « Article 41 ». Ces conclusions sont reprises dans un rapport datant du 8 février 2008.

Ces rapports ont ensuite été envoyés à la Commission nationale pour la protection des données par le biais du Ministère des Communications afin de l'analyser d'un «*point de vue de la nécessité des mesures proposées et du respect du principe de proportionnalité* ».

Le présent document reprend les conclusions de ces premières analyses.

II. Les conclusions du rapport d'audit d'Ernst & Young

Ce rapport statue par des conclusions bien précises sur les points ayant été soumis à contrôle sur les limites de l'étude ainsi que sur les failles et faiblesses identifiées.

Un des défauts majeurs restant à corriger et résultant de la conception du système était le fait que l'IRL ne devait plus avoir la possibilité d'avoir accès aux informations à caractère personnel qui font l'objet d'une recherche par les autorités dans le cadre de l'application de l'article 41 de la loi.

La Commission nationale, tout en n'ayant pas analysé la totalité des recommandations dans leurs moindres détails, constate néanmoins certains problèmes :

- la possibilité aux administrateurs réseaux ILR de prendre le contrôle complet des serveurs, des bases de données et des applications du système d'information « Article 41 » ;
- la possibilité aux administrateurs réseaux ILR de lire, modifier et restaurer des backup du système d'information « Article 41 » ;
- la présence de données issues de tests ou lors du développement des applications dans l'environnement de production ;
- l'utilisation d'une imprimante non-sécurisée pour imprimer des rapports PC-SAA (PC for anti abuse system) ;
- la protection insuffisante contre des attaques internes concernant les clés d'encryptions enregistrés dans le « Hardware Security Module » ;
- la protection insuffisante des serveurs contre des incidents environnementaux comme le feu, l'inondation, etc. ;

- la protection insuffisante contre un « capacity overrun » ;
- l'insuffisance de la documentation des procédures organisationnelles ;
- l'insuffisance de personnes ILR pouvant garantir une maintenance du système 24 h/24 et 7 jours/7.

III. Les réponses de l'ILR face aux recommandations d'Ernst & Young

Le 6 décembre 2007, l'IRL a pris position par rapport à chaque recommandation présentée dans ledit rapport d'audit. Or, il n'est pas très clairement mentionné combien de recommandations ont effectivement été acceptées, combien ont déjà été mises en place ou bien encore combien doivent être mises en place.

Même si chaque recommandation est abordée par l'ILR, cette dernière n'en tire pas toutes les conclusions quant aux différents points. Il semble d'ailleurs que, même si l'ILR entend suivre ces recommandations, les modifications n'ont pas encore été mises en œuvre (ceci résulte notamment des points 2.2, 2.3, etc.).

Les réponses de l'ILR indiquent en effet que des améliorations ont été apportées, mais le rapport ne permet pas encore de déterminer de façon certaine si l'ensemble des défauts soulevés dans le rapport d'audit ont été corrigés.

Pour cette raison, la CNPD préconise que l'Institut établisse un plan indiquant clairement les recommandations déjà mises en place et celles qui le seront ultérieurement, ainsi qu'un calendrier prévisionnel afférent.

Sous cet aspect, la Commission nationale ne peut pas constater si les mesures de sécurité proposées par le rapport sont opérationnelles et si le système répond aux exigences légales.

IV. L' analyse des risques et des impacts effectuée par Fujitsu Services et Ubizen

1) Avis sur la portée de l'analyse

Ce rapport fait état de plusieurs vulnérabilités découvertes lors de l'analyse des différentes parties du système. Cependant, ce rapport ne peut être considéré comme une « analyse de risques » au sens des normes ISO (cf. ISO 13335-2 ou 27005) car il fait défaut de certaines considérations :

1. L'envergure de l'analyse n'est pas indiquée.
2. Il n'y a pas d'estimation des différents paramètres des risques comme l'impact et la probabilité d'occurrence.
3. Le rapport ne décrit ni les menaces ni les scénarios d'éventuelles attaques.
4. Le rapport ne donne pas d'estimation du niveau des différents risques.

Étant donné qu'il y a absence de ces informations, tels que le niveau de risque sur le système actuel et l'absence d'une indication des coûts des contre-mesures, la Commission nationale n'est pas en mesure d'analyser la proportionnalité du traitement prévu par le système, sur base des conclusions de ce rapport.

Pour ce faire, la CNPD devrait disposer d'un plan de traitement de risques qui qualifierait les mesures déjà mises en place, les mesures retenues pour leur mise en place, les risques résiduels et une justification détaillée pour chaque mesure de sécurité initialement proposée mais non retenue. Un tel plan de traitement des risques est décrit dans la norme ISO 27005.

2) Avis sur le contenu du rapport

Malgré l'absence de précisions additionnelles concernant les points mentionnés ci-dessus, certaines conclusions de ce rapport apparaissent d'ores et déjà inquiétantes.

En particulier le fait qu'une réinitialisation du système suite à une panne nécessiterait une durée comprise entre 1 jour et 6 semaines (cf. p. 28). Si cela s'avérait exact, il parait indispensable à la Commission nationale à ce que l'Institut en charge prenne les mesures nécessaires pour rendre le système conforme aux attentes du législateur, étant donné que ledit système a été prévu pour protéger la vie des victimes devant être localisées ou qu'elle développe au moins une procédure d'urgence qui offrirait aux autorités une possibilité « manuelle » en cas de système hors fonction.

Certaines informations techniques ou conclusions suggérées dans le rapport nous apparaissent discutables, tel le calcul déterminant la nécessité d'une présence de 5,15 personnes pour assurer un service 24h/24 sur 7jours/7. Ce calcul se base notamment sur l'hypothèse dans laquelle le système tournerait en présence d'une personne. Or il nous semble qu'avec le système Alarmtilt, il suffit d'un service de permanence, mais non d'une présence pour assurer le service 24 h/24 sur 7 jours/7.

Conclusion

En vue d'une mise en place correcte des mesures de sécurité invoquées dans sa délibération du 25 mai 2007 la Commission nationale recommande de faire adapter le système d'information analysée de façon à pallier aux insuffisances mises en évidence dans les rapports d'audit et d'analyse de risques et d'impactes et de présenter un plan et un calendrier de mise en œuvre.

Avis de la commission nationale pour la protection des données relatif à l'avant-projet de règlement grand-ducal concernant la saisie et le traitement des données nominatives des élèves

Délibération n° 167/2008 du 20 juin 2008

1. Observations quant à la forme

1.1. Depuis l'abrogation de la loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques par la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, les termes « données nominatives » ne sont plus utilisés dans les textes légaux ou réglementaires. La Commission nationale propose dès lors d'employer les termes « données à caractère personnel ».

1.2. Le traitement de données à caractère personnel faisant l'objet de l'avant-projet de règlement grand-ducal concernant la saisie et le traitement des données nominatives des élèves est susceptible de correspondre à ceux exemptés de notification et prévus aux lettres (i) et (j) de l'article 12 paragraphe (3) de la loi modifié du 2 août 2002. La Commission nationale se demande s'il n'est pas indiqué de mentionner les références de ces dispositions légales dans le visa de l'avant projet de règlement grand-ducal.

2. Observations quant au fond

2.1. Le responsable du traitement

Il ne résulte pas clairement des textes en projet qui est le responsable du traitement. La détermination précise du responsable du traitement est importante, alors que ce dernier a l'obligation de veiller à la confidentialité et à la sécurité des données et de mettre en place l'organisation appropriée des mesures techniques.

Si l'article 27 du projet de loi portant organisation de l'enseignement fondamental précise que c'est le « *titulaire de classe* » qui « *rassemble dans un fichier les données personnelles des élèves …* », l'article 3 de l'avant-projet de règlement grand-ducal énonce quant à lui que « *l'administration communale transmet à chaque titulaire de classe un relevé des élèves inscrits dans cette classe …* ».

A la lecture de ces dispositions, la Commission nationale comprend qu'il est dans l'intention des auteurs des textes d'attribuer la responsabilité du traitement à l'administration communale, tout en voulant confier en pratique aux titulaires de classe la mission de saisir les données à caractère personnel et de les tenir à jour.

La Commission nationale suggère de clarifier ce point dans les dispositions en projet.

2.2. L'origine des données à caractère personnel

Les dispositions ne renseignent pas sur l'origine des données. La Commission nationale estime utile de préciser de quelle façon les données sont collectées, du moins pour ce qui est des données à caractère personnel qui ne sont pas issues des fichiers des registres de la population, tenus par les communes, telles que les informations relatives à la langue habituellement parlée à la maison, la date d'arrivée au Grand-Duché de Luxembourg, la catégorie socioprofessionnelle. Certaines données sont-elles, le cas échéant, collectées directement auprès des parents d'élèves ?

2.3. Destinataires des données à caractère personnel

L'article 1er de l'avant-projet de règlement grand-ducal a notamment pour objet de réglementer l'accès aux données traitées. La Commission nationale vient à se demander si la formulation utilisée qui énumère entre autres le « bourgmestre » et le « ministre ayant l'Education nationale dans ses attributions » n'est pas trop générale. Cette formulation peut laisser entendre que l'ensemble des personnes travaillant sous l'autorité du bourgmestre ou du ministre aient accès aux données. Il faudrait limiter l'accès aux

données aux seules personnes qui dans le cadre de leur fonction ont besoin des données en question (p. ex les personnes en charge du service scolaire au niveau communal. Il est suggéré de préciser l'article 1 sur ce point.

2.4. Nature des données à caractère personnel

L'article 2 de l'avant-projet de règlement grand-ducal énumère les différentes données qui sont enregistrées dans le fichier. La commission nationale n'a pas d'objections à formuler, sauf en ce qui concerne les informations relatives à la catégorie socioprofessionnelle des familles des élèves. Elle se demande si la notion de catégorie socioprofessionnelle n'est pas trop large et imprécise.

En effet, cette notion peut inclure plusieurs éléments :

- niveau de revenu des parents,
- niveau de formation des parents,
- métiers exercés par les parents,
- l'état d'inactivité des parents pour raison de chômage, d'incapacité de travail, d'invalidité,
- etc.

L'intention d'englober les informations relatives à la catégorie socioprofessionnelle renferme le danger que celles-ci soient trop détaillées pour figurer dans un fichier permanent et accessible à un nombre important de personnes. L'enregistrement de telles informations détaillées n'est pas nécessaire et serait à considérer comme disproportionné par rapport à la plupart des finalités du fichier. Dans un souci de protection des données ainsi que pour éviter des risques d'abus, la Commission nationale recommande de limiter cette catégorie de données à la seule profession des parents.

Elle comprend parfaitement le souci légitime et l'utilité de disposer d'informations plus détaillées pour réaliser des études dans le cadre de la définition et de la mise en œuvre de la politique éducative. Il serait préférable de collecter ponctuellement dans le cadre d'études statistiques des informations détaillées sur la catégorie socioprofessionnelle des familles des élèves (p. ex. par le biais de l'IGSS), le cas échéant rendues anonymes et accessibles à un nombre restreint de personnes plutôt que d'enregistrer ces informations dans un fichier permanent.

2.5. Conservation des données

La Commission nationale suggère de préciser à l'article 5 de l'avant-projet de règlement grand-ducal les modalités et conditions d'accès aux données archivées.

Avis de la Commission nationale pour la protection des données concernant le projet de règlement grand-ducal relatif à la fixation des conditions et modalités de délivrance de la documentation cadastrale

Délibération n° 176/2008 du 4 juillet 2008

Conformément à l'article 32 paragraphe (3) lettre (e) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après désignée « la loi du 2 août 2002 »), la Commission nationale pour la protection des données a notamment pour mission d'« être demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi ».

C'est dans cette optique, et faisant suite à la demande lui adressée par Monsieur André PEFFER, Directeur de l'Administration du Cadastre et de la Topographie en date du 20 novembre 2007 que la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet du projet de règlement grand-ducal pré-mentionné.

Observations préliminaires

Le cadastre contient des données à caractère personnel relatives aux propriétaires fonciers et à tous les autres titulaires de droits réels immobiliers recensés, de sorte qu'il constitue un traitement de données au sens de la loi du 2 août 2002.

Le projet de règlement grand-ducal sous examen doit concilier les règles de protection des données à caractère personnel avec les règles relatives, d'une part, à la publicité du cadastre, instituée à l'article 2 lettre 2) de la loi du 25 juillet 2002 portant réorganisation de l'administration du cadastre et de la topographie, et, d'autre part, au principe du libre accès aux documents administratifs et de la réutilisation des informations publiques.

La Commission nationale entend limiter ses commentaires aux seules dispositions soulevant des questions de protection des données.

1. Le principe de finalité

Le principe de finalité est le « *fil conducteur* » de la loi du 2 août 2002 : « *c'est par la finalité que tout commence et tout finit* [car elle] *doit être antérieure à la mise en œuvre du traitement, justifie la collecte, doit être connue de la personne concernée, limite le champ d'utilisation des données collectées (…)* »[6]. Ce principe repose sur le « *postulat que la menace pour la vie privée que constituent les traitements de données à caractère personnel réside davantage dans la finalité qu'ils poursuivent que dans la nature des données traitées* »[7].

Conformément à l'article 4 paragraphe (1) lettre (a) de la loi du 2 août 2002, les données doivent être « *collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités*».

L'utilisation des données doit donc être compatible avec les finalités originaires du cadastre.

La Commission nationale accueille avec satisfaction les efforts des auteurs du projet de règlement grand-ducal sous rubrique pour les précisions apportées sur la thématique de l'utilisation conforme des données cadastrales aux articles 13, 25 et 29 et notamment sur l'obligation de signer un acte d'engagement lorsque les informations sont fournies sur support papier ou sur des fichiers informatiques.

6 Documents parlementaires n°4735, page 87

7 Id.

Compte tenu de l'importance du principe de finalité, la Commission nationale recommande de prévoir une disposition expresse pour insister sur le respect du principe de finalité. Cette disposition écrite en termes généraux sera applicable pour toutes les demandes d'information à partir des registres cadastraux.

Cette disposition supplémentaire pourra être insérée dans le chapitre 2, soit dans l'article 7, soit dans un nouvel article et elle pourrait avoir la teneur suivante :

> « *Toute personne doit respecter les finalités des registres du cadastre. Les finalités pour lesquelles la consultation ou la demande d'information est envisagée doivent être en rapport avec celles du cadastre et ne pas être incompatibles entre elles».*

A titre d'exemple, la Commission belge de la protection de la vie privée a retenu que les documents cadastraux ne doivent pas être diffusés ou utilisés à des fins commerciales[8]. Pour sa part, la Commission Nationale de l'Informatique et des Libertés (ci-après : la CNIL) a retenu que « *les informations ne peuvent être utilisées à des fins commerciales, politiques ou électorales ou de manière qui porterait atteinte à l'honneur ou à la réputation des personnes ou au respect de la vie privée*[9] ».

2. Les informations cadastrales délivrées par les préposés de l'Administration du Cadastre et de la Topographie sur support papier ou sur fichiers informatiques (articles 16 à 37)

2.1. L'objet des demandes de renseignement

L'article 16 du projet de règlement grand-ducal sous rubrique énumère limitativement les cas d'ouverture pour lesquels une demande d'information est possible. Sa rédaction procède de la volonté de ne pas donner la possibilité de consulter les données de tiers à partir de ses données d'identification. Cette limitation est satisfaisante et respectueuse de la loi du 2 août 2002.

A titre superfétatoire, il semblerait que des erreurs de terminologie se soient glissées dans le texte du projet de règlement grand-ducal sous examen. En effet, l'article 16 paragraphe (1) mentionne « *une situation ponctuelle* » alors qu'il semble s'agir « *d'une demande ponctuelle* ». De plus, l'adjectif « *distincte* » inscrit aux articles 16 paragraphe (3) et 23 paragraphe (3) paraît avoir été inséré à la place de « déterminée ». Dans le même ordre d'idée, les article 17 paragraphe (2) et 24 paragraphe (2) mentionnent « *une personne intéressante* » pour évoquer, semble-t-il, la personne dont émane la demande.

En tout état de cause, la Commission nationale relève qu'une demande ponctuelle puisse porter sur une grande dimension géographique.

2.2. L'énumération limitative des données transmises

La Commission nationale note que le projet de règlement grand-ducal sous examen n'énumère pas les données qui peuvent être communiquées. Le problème se pose en particulier sur l'éventuelle communication du numéro d'identification national des personnes qui figurent dans les registres cadastraux.

Ainsi il a été retenu que « *seul le propriétaire foncier ou son mandataire puisse obtenir communication des informations le concernant, les date et lieu de naissance du propriétaire, les mentions relatives aux motifs d'exonération des taxes foncières (…) ne puisse être communiquées au public, l'adresse du domicile du propriétaire ne puisse être délivrée qu'en présence d'une motivation légitime* » [10].

Compte tenu du principe de finalité des registres cadastraux et des intérêts en présence, la Commission nationale suggère que l'article 16 ou un nouvel article à insérer entre les articles 16 et 17 énumèrent avec précision les données à caractère personnel qui peuvent être communiquées.

8 avis d'initiative relatif à l'organisation de la publicité cadastrale n°32/201 du 10 septembre 2001

9 délibération 2004-105 du 14 décembre 2004 portant autorisation unique de traitements de données à caractère personnel comportant un système d'information géographique mis en œuvre par les collectivités locales ou leurs groupements (cadastre et urbanisme)

10 délibération précitée de la CNIL n°2004-105 du 14 décembre 2004

Le texte pourrait être rédigé comme suit :

> *« Les propriétaires et les autres titulaires de droit réel immobiliers sont en droit d'obtenir communication de l'intégralité des données les concernant figurant dans les registres cadastraux.*
>
> *Cette règle s'applique également à leur mandataire, ayant-droit ou représentant légal.*
>
> *Tout autre tiers ne pourra prendre connaissance que des données foncières stricto sensu ainsi que les nom/s, prénom/s et adresse du/des personnes concernées.* »

Dans un souci de cohérence, il serait appréciable que l'article 23 point (3) précise que le demandeur puisse être la personne concernée elle-même, son mandataire, son représentant légal ou encore son ayant-droit.

3. La Consultation directe du cadastre (chapitre 9)

La consultation directe présente des avantages incontestables pour les utilisateurs : elle est un exemple de la simplification administrative car l'accès aux données est permanent et immédiat. Mais elle présente également des risques d'atteinte à la confidentialité et à la sécurité des données à caractère personnel. L'Administration du Cadastre et de la Topographie ne pourra pas vérifier *a priori* si chaque consultation est conforme à la législation, et notamment à la loi du 2 août 2002 et au principe de finalité.

La Commission nationale relève avec satisfaction que le projet de règlement grand-ducal sous examen détaille un éventail de mesures susceptibles d'encadrer l'utilisation de la consultation directe par la détermination de groupes de bénéficiaires (article 38) et des restrictions d'accès (article 39). Elle propose d'étoffer ces mesures par l'insertion de dispositions ayant trait au principe de finalité et à la sécurité de l'architecture technique de la consultation directe.

3.1. Le rappel du principe de finalité

A l'instar des demandes de renseignements formulées directement à l'Administration du Cadastre et de la Topographie, la Commission nationale propose d'inclure une disposition rappelant le principe de finalité dans un nouveau paragraphe (7) de l'article 39 du projet de texte.

Cette disposition pourrait être rédigée dans les termes suivants :

> *« Toute consultation directe doit s'opérer dans le cadre exclusif et strictement nécessaire des fonctions et missions professionnelles des bénéficiaires et dans le respect des finalités d'intérêt public qui leur sont confiées par ou en vertu de la loi ou d'un règlement grand-ducal.* »

3.2. Les mesures de sécurité technique

Les articles 22 et 23 de la loi du 2 août 2002 ont trait aux mesures techniques que doit impérativement appliquer le responsable du traitement « *pour assurer la protection des données qu'il traite contre la destruction accidentelle ou illicite (…) l'accès non autorisé (…) ainsi que contre tout autre forme de traitement illicite* ».

La Commission nationale recommande que des mesures de sécurité technique de la consultation directe soient inscrites dans le chapitre neuf du règlement grand-ducal sous examen. Sa mise en œuvre doit se faire sur base d'un système prévoyant des mesures techniques assurant un accès sécurisé, limité et contrôlé. Ce contrôle devrait s'opérer au moyen d'une journalisation des accès qui permet la consultation d'un historique des accès, à savoir, les dates et heures des consultations, l'identification du bénéficiaire de l'accès et la personne physique habilitée.

Avis de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal autorisant la mise en œuvre des traitements de données à caractère personnel nécessaires à l'exécution de la loi du 29 août 2008 sur la libre circulation des personnes et l'immigration et déterminant les données à caractère personnel auxquelles le ministre ayant l'Immigration dans ses attributions peut accéder aux fins d'effectuer les contrôles prévus par la loi

Délibération n° 202/2008 du 18 juillet 2008

Conformément à l'article 32, paragraphe 3, lettre (e) de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après désignée « la loi du 2 août 2002 »), la Commission nationale pour la protection des données (ci-après « la Commission nationale ») a entre autres pour mission d'« être demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi ».

C'est dans cette optique, et faisant suite à la demande lui adressée par Monsieur le Ministre des Affaires étrangères et de l'Immigration en date du 14 juillet 2008 que la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet du projet de règlement grand-ducal pré-mentionné.

Lors de la phase d'élaboration de l'avant-projet de règlement grand-ducal en question, la Commission nationale a déjà été consultée par le ministère des Affaires étrangères et de l'Immigration. Elle lui a fait parvenir ses commentaires et recommandations par courrier du 26 juin 2008 dont le contenu était le suivant :

« *Nous estimons que l'article 139 du projet de loi n° 5802, faisant simplement référence à différents fichiers, ne détermine pas assez précisément les données ou catégories de données à caractère personnel pouvant être consultées. C'est pourquoi la Commission nationale a recommandé dans son avis du 11 janvier 2008 relatif au projet de loi n° 5802 de prévoir dans le projet de loi lui-même ou dans un règlement grand-ducal « une indication précise et détaillée des données échangées par les différents organismes publics ».*

En l'absence de précisions textuelles, le ministre ayant l'immigration dans ses attributions aura vocation à accéder à toutes les données figurant dans les différents fichiers. Or, la Commission nationale est d'avis (cf. avis précité) que l'accès devrait être possible uniquement aux données qui intéressent le ministre et non pas à l'intégralité des données figurant dans les différents fichiers et relatives à la personne sur qui la recherche et le contrôle sont effectués.

Nous pensons par ailleurs que pour des raisons de sécurité juridique, un haut degré de précision des données est nécessaire. Une précision textuelle détaillée des données permettra au cours de la procédure un contrôle a priori du principe de proportionnalité d'une part, et un contrôle a posteriori de la mise en œuvre du système informatique, d'autre part.

En effet, il ne faut pas perdre de vue que les responsables de traitement des différents fichiers accédés sont en quelque sorte les garants des données et de la compatibilité des finalités et que ceux-ci doivent veiller à ce que la communication des données à caractère personnel à un tiers se fasse selon le même principe de finalité et soit compatible avec les traitements initiaux.

En l'espèce, le mode de transmission des données est passif en ce sens que le ministre chargé de contrôler les conditions d'entrée et de séjour des étrangers – ainsi que les personnes qui agissent sous son autorité – peuvent directement accéder aux différents fichiers énumérés à l'article 139 du prédit projet de loi, sans intervention des responsables des différents fichiers consultés, qui eux perdent en quelque sorte la maîtrise sur les données contenues dans leurs fichiers.

Dans ce contexte et à titre d'exemple, nous voudrions nous référer à la procédure législative du projet de loi n° 5563 qui comprend parallèlement un projet de règlement grand-ducal[11] *prévoyant une énumération précise et limitative des données de dix fichiers publics auxquelles pourront accéder les magistrats du ministère public et officiers de police judiciaire.*

Etant donné que le ministre ayant l'immigration dans ses attributions exploitera lui-même une « nouvelle » banque de données dans le contexte de l'article 139, la Commission nationale suggère, par référence à l'article 12 paragraphe (3) lettre (j) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, que le projet de règlement grand-ducal en élaboration contienne, outre les exigences de l'article 139 alinéa 2, les éléments et précisions suivants :

- *L'indication du responsable du traitement, c'est-à-dire le ministre ayant l'immigration dans ses attributions.*
- *La finalité du fichier, à savoir les contrôles effectués en vertu des articles 134 et 139.*
- *L'indication détaillée des données à caractère personnel que contiendra le « nouveau » fichier exploité par la ministre ayant l'immigration dans ses attributions.*
- *L'indication sur l'obtention des données traitées : les données recueillies auprès des personnes concernées elles-mêmes et les données obtenues à partir des différents fichiers mentionnés à l'article 139.*
- *L'indication détaillée des données accédées dans les différents fichiers mentionnés à l'article 139.*
- *L'indication des personnes auxquelles le droit d'accès est réservé* ».

La Commission nationale exprime sa satisfaction que presque toutes ses observations et recommandations qu'elle avait formulées au stade de l'avant-projet de règlement grand-ducal ont été reprises dans le texte du projet de règlement grand-ducal actuellement sous examen.

Dans le présent avis, elle voudrait encore émettre les remarques et recommandations suivantes :

- Quant à la forme

Sous le régime de la loi abrogée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques, les banques de données relevant de l'Etat devaient obligatoirement être autorisées par une loi ou un règlement grand-ducal. Or, la législation actuelle en la matière, à savoir la loi modifiée du 2 août 2002, n'a pas été conçue sous cette optique.

Ainsi, d'un point de vue purement terminologique, la Commission nationale propose de modifier l'article 1 paragraphe (1) du projet de règlement grand-ducal en remplaçant les mots « est autorisé à mettre en œuvre » par les termes « met en œuvre ». Dans la première phrase de l'article 2, les mots « …est autorisé à accéder… » pourraient être remplacés par les termes « …peut accéder ».

Enfin, dans le même ordre d'idées, l'intitulé du règlement d'exécution pourrait commencer par « Règlement grand-ducal portant création des traitements … ».

- Quant au fond

Dans son courrier du 26 juin 2008, la Commission nationale avait recommandé que le règlement grand-ducal contienne, en plus de l'énumération détaillée des données accédées dans les fichiers des différents organismes publics, une énumération exhaustive de toutes les données traitées (données accédées et données recueillies directement auprès des personnes concernées) dans la base de données nouvellement créée.

Le texte actuel ne tenant pas compte de cette recommandation, la Commission nationale suggère que les auteurs du projet de règlement grand-ducal précisent encore les données collectées et traitées dans le nouveau fichier – données qui ne proviennent pas des six fichiers pouvant être accédés.

11 portant exécution de l'article 34-1 de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la police

Avis de la Commission nationale pour la protection des données relatif à l'interprétation et l'application de l'article 20 du projet de loi N°5859 portant modification de la loi électorale modifiée du 18 février 2003

Délibération n°339/2008 du 28 octobre 2008

Faisant suite à la demande lui adressée par l'intermédiaire de Monsieur le Président de la Chambre des Députés, pour la Commission des Affaires Intérieures et de l'Aménagement du Territoire, en date du 1er octobre 2008, la Commission nationale pour la protection des données entend présenter ci-après ses réflexions et commentaires au sujet de l'article 20 du projet de loi N°5859 portant modification de la loi électorale du 18 février 2003, telle que modifiée (ci-après « *la loi électorale* »).

La loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après désignée « la loi du 2 août 2002 ») prévoit qu'un traitement n'est licite que s'il est mis en œuvre pour une finalité déterminée, explicite et légitime. L'article 20 de la loi électorale actuellement en vigueur prévoit déjà la faculté pour les citoyens de prendre inspection des listes électorales et d'en obtenir copie. Le projet de loi N°5859 ne fait que reprendre en son article 20 le principe de la communication d'une copie des listes électorales actualisées à tout citoyen qui en fait la demande. Il n'y a là aucune entorse à la loi du 2 août 2002.

Les dispositions de l'article 4 de la loi du 2 août 2002 érigent le principe de finalité d'un traitement de données en un principe essentiel dans le domaine de la protection des données. La finalité de la tenue des listes électorales consiste en la constatation de la qualité d'électeur des personnes physiques remplissant les conditions reprises dans le Titre I de la loi électorale.

Le droit d'inspection des listes électorales, ainsi que le droit d'en prendre copie rentrent dans le cadre de cette finalité, notamment aux fins de vérifier l'exactitude des listes électorales ou de constater et de vérifier le nombre d'électeurs inscrits au sein d'une commune. Le droit ouvert à chaque citoyen de se pourvoir en justice contre toute personne indûment inscrite, omise ou rayée sur les listes électorales constitue le corollaire nécessaire de cette finalité, qui s'inscrit dans un but de contrôle démocratique. La Commission nationale considère que la prospection des électeurs inscrits par les divers partis politiques, notamment pour leur adresser les programmes politiques, rentre également dans le cadre de cette finalité électorale.

Si le droit de prendre inspection des listes électorales ne comporte pas de risques de diffusion, d'utilisation illégitime, d'abus ou de détournement de finalités des données personnelles y figurant, il en va autrement dans l'hypothèse de délivrance de copies.

Le collège des bourgmestres et échevins, en sa qualité de responsable du traitement, devra s'assurer que les données des listes électorales seront utilisées loyalement et licitement et qu'elles ne seront pas traitées ultérieurement de manière incompatible avec leur finalité électorale, après communication aux citoyens. Les données une fois communiquées, le responsable du traitement perd en fait tout contrôle sur leur utilisation, de sorte qu'il y a un risque qu'elles puissent être utilisées à des fins autres qu' « électorales ».

Le droit de prendre copie soulève donc le problème du respect de la finalité par le destinataire. Il paraît dès lors souhaitable de voir entourer le droit de prendre copie d'un certain nombre de précautions et de garanties.

En France, chaque électeur, candidat et parti ou groupement politique peut prendre communication et copie de la liste électorale, à condition de s'engager à ne pas en faire un usage purement commercial.

En Belgique, la Commission de la protection de la vie privée note que les personnes ayant reçu des exemplaires ou copies d'une liste des électeurs ne peuvent pas les communiquer à des tiers, ni les utiliser

pour d'autres finalités (par exemple commerciales). Le demandeur est en outre obligé d'adresser, par lettre recommandée, au bourgmestre une demande écrite, endéans un certain délai, en vue d'obtenir une copie des listes électorales.

La Commission nationale recommande de retenir également au Grand-Duché du Luxembourg le principe d'une demande écrite pour la délivrance de copies, ainsi que d'une notice d'information rendant le demandeur attentif au fait que les données ne doivent pas être transmises à des tiers, ni faire l'objet d'une quelconque utilisation – par exemple commerciale – incompatible avec la finalité électorale. Dans un souci de sécurité juridique, la Commission nationale préconise de compléter l'article 20 du projet de loi en ce sens.

Les considérations ci-dessus valent également en ce qui concerne la délivrance de copies des listes de « réclamations » prévues à l'article 15, paragraphe (2) du projet de loi.

Pour ce qui est de la forme de la communication des copies, chaque demandeur, après avoir introduit une demande écrite, pourra obtenir délivrance d'une copie des listes électorales, ou bien sous forme papier ou bien sous forme de fichier électronique sur un support à déterminer.

Une alternative par voie de courriel n'est pas à exclure de manière absolue, mais une telle procédure devra toutefois être sécurisée de façon appropriée, ce qui, en l'état actuel de la technique, présuppose le recours à la signature électronique et au cryptage des données transmises.

Le projet de loi pourrait être précisé en ce sens par l'ajout d'un alinéa qui pourrait prendre la teneur suivante : « *La copie sera délivrée ou bien sous forme papier ou numérique en mains propres du demandeur ou bien par un moyen de communication sécurisé de façon appropriée* ».

Avis de la Commission nationale pour la protection des données relatif à l'avant-projet de loi modifiant la loi modifiée du 29 avril 1983 concernant l'exercice des professions de médecin, de médecin-dentiste et de médecin-vétérinaire

Délibération n°369/2008 du 21 novembre 2008

Faisant suite à la demande lui adressée par l'intermédiaire du Collège médical, en date du 1er octobre 2008, la Commission nationale pour la protection des données entend présenter ci-après ses réflexions et commentaires au sujet de l'avant-projet de loi modifiant la loi modifiée du 29 avril 1983 concernant l'exercice des professions de médecin, de médecin-dentiste et de médecin-vétérinaire et plus particulièrement sur son article 33 paragraphe (7) qui prévoit la mise en place d'un annuaire public des médecins, des médecins-dentistes et des médecins-vétérinaires (ci-après : les médecins) exerçant au Grand-Duché de Luxembourg. Cet annuaire, disponible sur Internet, précisera encore si ces professionnels font l'objet d'une interdiction, respectivement d'une suspension d'exercice professionnel.

La diffusion sur Internet des données relatives à l'interdiction ou à la suspension d'exercer soulève certaines questions ayant trait à la protection des données.

La Commission nationale relève tout d'abord que la mise à disposition du public de la liste des médecins consultable sur Internet peut présenter un risque pour la protection de la vie privée des personnes concernées. En effet, des informations issues de l'annuaire public pourraient devenir disponibles sur Internet de manière permanente car les moteurs de recherche copient ces informations dans leur index et il n'est pas garanti que celles-ci ne soient pas non plus copiées à leur tour par des tiers et ne se retrouvent par après également accessibles sur Internet sur d'autres sites, sans mises à jour et sans contrôle de l'autorité chargée de la diffusion de l'annuaire public.

Par ailleurs, le texte sous examen ne précise pas si seules les décisions définitives seront mentionnées dans l'annuaire. Il existerait en effet un risque que l'annuaire mentionne des sanctions non définitives susceptibles donc d'être modifiées.

De plus, aux termes de l'article 4 paragraphe (1) lettre (a) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après : la loi du 2 août 2002), les données sont « *collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités* ». La lettre (b) précise encore que les données doivent être « *adéquates, pertinentes et non excessives au regard des finalités* ».

En ce qui concerne la ou les finalité(s) de l'annuaire public des médecins, la Commission nationale considère qu'un annuaire des professionnels de la médecine est en principe mis en place pour informer les personnes sur les médecins qui sont autorisés à exercer légalement et renseigne encore sur leur spécialité et leurs coordonnées afin qu'ils puissent être contactés. La publication sur Internet assure la possibilité de tenir cette liste toujours à jour.

Il serait possible d'envisager que l'annuaire public soit considéré aussi comme un outil pouvant contribuer à l'efficacité des sanctions les plus graves que sont l'interdiction et la suspension d'exercer.

La Commission nationale relève que la publication systématique, notamment sur Internet, des sanctions d'interdiction et de suspension d'exercer n'existe pas pour les autres professions réglementées au Grand-Duché de Luxembourg.

Ensuite, et par comparaison avec nos pays voisins, des annuaires des médecins sont consultables sur Internet. Ainsi, en Belgique, en Allemagne et en France, les annuaires publient uniquement les médecins en situation régulière d'exercice, sans mentionner les éventuelles suspensions ou interdictions d'exercer. L'article R.4127-80 du Code de la Santé Publique français énumère les indications relatives aux

médecins qui peuvent figurer dans les annuaires à usage du public et la mention d'une éventuelle interdiction ou suspension d'exercice n'y figure pas.

La Commission nationale est d'avis que la finalité accessoire relative à l'amélioration de l'efficacité des sanctions - dans l'hypothèse où elle était recherchée par les auteurs de l'avant-projet de loi soumis à examen - ne peut pas justifier la publication sur Internet de ces informations compte tenu de l'atteinte disproportionnée portée aux droits fondamentaux des médecins sanctionnés, du fait du caractère infamant d'une telle mesure.

Eu égard à ces considérations, la Commission nationale estime que le projet d'annuaire a pour finalité essentielle d'informer le public sur les médecins pouvant légalement exercer au Grand-Duché de Luxembourg et qu'il suffirait pour cela d'indiquer uniquement les données des médecins qui peuvent légalement exercer leur activité, sans autre précision. Les données relatives aux médecins faisant l'objet d'une interdiction ou d'une suspension d'exercice ne seraient dès lors pas disponibles sur l'annuaire public tant que dure la sanction. Une note sur le site Internet pourrait, par exemple, préciser que si une personne ne retrouve pas les coordonnées d'un médecin, elle a la possibilité de demander aux autorités nationales compétentes, les raisons pour lesquelles ce médecin précis n'y figure pas et signaler, le cas échéant, son exercice professionnel illégal.

Des mesures devraient être prises pour garantir la mise à jour régulière de l'annuaire public en question.

Avis relatif à l'avant-projet de règlement grand-ducal déterminant les procédés à suivre pour constater la mort en vue d'un prélèvement

Délibération n°402/2008 du 12 décembre 2008

Faisant suite à la demande lui adressée par l'intermédiaire de Monsieur Raymond MOUSTY, Premier Conseiller de Gouvernement auprès du Ministère de la Santé, en date du 19 septembre 2008, la Commission nationale pour la protection des données entend présenter ci-après ses réflexions et commentaires au sujet de l'avant-projet de règlement grand-ducal « *déterminant les procédures à suivre pour constater la mort en vue d'un prélèvement* », et plus particulièrement sur son article 4 ayant trait aux données à caractère personnel.

Cet article prévoit en effet qu'en vue d'une transplantation d'organes ou autres substances corporelles, le numéro d'identité et les données médicales du donneur pourront être communiquées « *au service national de coordination dont question à l'article 15 de la loi du 25 novembre 1982 réglant le prélèvement de substances d'origine humaine, à la banque européenne d'organes la plus représentative avec laquelle il collabore, ainsi qu'à l'équipe médicale ayant en charge le ou les receveur(s) potentiel(s)* ».

Il se pose, tout d'abord, le problème de la communication du numéro d'identité du donneur. La Commission nationale relève que, conformément à ce qu'elle précisait dans son courrier du 3 juin 2008 adressé au Ministère de la Santé, l'article 5 de la loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales pose deux conditions cumulatives à l'utilisation dudit numéro d'identification à savoir qu'un règlement grand-ducal détermine les actes, documents, fichiers qui utiliseront le numéro et, deuxièmement, que son utilisation soit limitée à un usage administratif interne ou aux relations avec le titulaire du numéro.

Or, et sans qu'il soit nécessaire de se prononcer sur la première condition, l'avant- projet de règlement grand-ducal sous examen ne satisfait pas à la condition qui limite l'utilisation du numéro d'identification à l'usage administratif interne ou aux relations avec son titulaire.

Par conséquent, et en l'état actuel du droit, il ne serait pas possible de transmettre le numéro d'identité du donneur aux intervenants à la transplantation énumérés dans le texte sous examen.

Il est vrai que le projet de loi n°5950 relatif à l'identification des personnes physiques, au registre national des personnes physiques et à la carte d'identité élargit la liste des personnes pouvant utiliser le numéro d'identification. Ainsi, l'article 3 paragraphe (3) du projet de loi précité prévoit limitativement les intervenants du secteur de la santé qui peuvent utiliser le numéro d'identification nationale mais il précise encore que son utilisation est réservée à l'usage administratif interne ou aux relations avec son titulaire.

Il est dans l'intention des auteurs du projet de loi précitée que « *l'usage de ce numéro doit (…) se limiter à un usage interne pour gérer les dossiers des patients, respectivement aux relations avec le patient. Le but de cette possibilité d'utilisation de ce numéro est de faciliter les relations avec les organismes de sécurité sociale qui ont un besoin évident de pouvoir identifier sans équivoque leurs assurés* » (travaux parlementaires n°5950/0, page 15).

De plus, les hypothèses supplémentaires de communication du numéro de matricule national prévues au paragraphe 4 dudit article 3 ne semblent pas non plus donner de solution.

Il nous paraît dès lors que ni le service national de coordination dont question à l'article 15 de la loi du 25 novembre 1982 réglant le prélèvement de substances d'origine humaine ni les banques européennes d'organes ne peuvent être rangés dans les différentes catégories prévues à l'article 3 du projet de loi n°5950 précité.

Il s'en suit que ni l'état actuel du droit ni le projet de loi n°5950 tel que déposé ne fournissent de base légale appropriée pour la transmission du numéro d'identification national.

En tout état de cause, la transmission de ce numéro soulève d'autres problématiques plus épineuses encore lorsqu'elle s'opère en dehors du Luxembourg (par exemple, Eurotransplant).

Ensuite, il convient d'analyser la transmission des données médicales. Ces dernières sont des catégories particulières de données au sens de l'article 6 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement de données à caractère personnel (ci-après : la loi du 2 août 2002). L'article 7 paragraphe (4) de la même loi précise encore que ces données « *peuvent être communiquées à des tiers (…) d'après les modalités et suivant les conditions à déterminer par règlement grand-ducal* ».

A supposer que l'avant-projet de règlement grand-ducal sous examen soit pris en vertu de l'article 7 paragraphe (4) de la loi, encore faudrait-il que le texte ne se limite pas seulement à poser le principe de la transmission des données, mais qu'il arrête également les modalités et les conditions de cette transmission, conformément aux exigences de l'article précité.

Par ailleurs, la Commission nationale estime que le texte sous examen doit également satisfaire aux dispositions des articles 6 et 9 de la loi du 25 novembre 1982 réglant le prélèvement de substances d'origine humaine aux termes desquels, d'une part, les prélèvements sont possibles seulement si le défunt n'a pas fait connaître son refus par écrit de son vivant et, d'autre part, le médecin est tenu de vérifier toute éventuelle opposition.

La Commission nationale considère que la transmission des données médicales est accessoire à la transplantation d'organes.

Par conséquent, et afin de ne pas se heurter aux principes de la loi précitée du 25 novembre 1982, le texte sous examen devrait mentionner que la transmission des données médicales n'est possible que dans l'hypothèse où le défunt ne s'y est pas opposé de son vivant par écrit ; il devrait encore préciser que le médecin doit vérifier cette possible opposition.

La Commission nationale recommande encore que le règlement grand-ducal appelé à abroger celui du 2 octobre 1992 règlementant l'utilisation des données médicales nominatives dans les traitements informatiques et qui est en cours d'élaboration au sein du Ministère de la Santé, contienne une disposition reprenant explicitement l'exception au principe du consentement en matière de prélèvement d'organes. Il pourrait ainsi faire une référence explicite à l'article 4 du texte sous examen pour parer à tout éventuel conflit de textes.

La Commission aimerait encore formuler quelques observations sur les destinataires des données médicales cités à l'article 4 du texte sous examen.

L'article 15 de la loi du 25 novembre 1982 réglant le prélèvement de substances d'origine humaine prévoit un service national de coordination uniquement pour le prélèvement des reins. Il se pose alors la question du champ de compétence et de la mission confiée à ce service.

Avis sur l'enregistrement d'appels téléphoniques d'urgence en vertu de l'article 4 paragraphe (3) de la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

Madame la Directrice,

Par votre courrier du 11 septembre 2008, l'Institut Luxembourgeois de Régulation demande à notre Commission nationale de lui faire connaître son avis à l'égard de la demande d'inscription des numéros d'appels d'urgence du service SOS-Seniors de la Ville de Luxembourg.

Si les numéros en question (numéro de téléphone général 457575 et numéros d'appel formés automatiquement par les équipements mis à disposition des personnes âgées et vulnérables lors du déclenchement du bouton d'urgence) étaient inscrits par l'Institut Luxembourgeois de Régulation sur la liste prévue à cette fin par l'article 4 paragraphe (3) lettre c de la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, l'enregistrement du contenu des communications et des données de trafic deviendrait licite. En principe ces données doivent rester confidentielles aux vœux de l'article 2 de la loi du 11 août 1982 sur la protection de la vie privée et de l'article 4 des paragraphes (1) et (2) de la prédite loi du 30 mai 2005, sauf exception expressément prévue par une loi.

Les exceptions au secret des communications (portant sur leur contenu et les données de trafic) doivent à notre avis être interprétées de façon restrictive. Si le consentement des parties à la conversation téléphonique ou communication électronique constitue bien une telle exception, encore faut-il que ce cas réponde aux critères légaux, c.à.d. qu'il ait été exprimé librement et de façon éclairée. D'après nos informations, la Ville de Luxembourg se propose de recueillir le consentement général des abonnés à son service SOS-Seniors dans le cadre des conditions générales contractuelles.

Pour pallier à un caractère spécial du consentement des personnes concernées qui fait défaut, il serait prévu en outre d'avertir les personnes entrant en communication avec les services communaux sur les numéros visés dans la demande à travers une bande sonore préenregistrée qui diffuserait automatiquement une brève annonce au début de chaque conversation.

Notre Commission nationale s'est félicitée de ces mesures et précautions envisagées par la Ville de Luxembourg lors d'une entrevue avec les responsables.

Toutefois avons-nous estimé que le cas de figure exposé pourrait être considéré comme faisant partie de ceux réglés à la lettre (c) du paragraphe (3) de l'article 4 de la loi du 30 mai 2005, alors que le motif invoqué pour justifier l'enregistrement systématique des appels à destination du / des numéro(s) en question consiste dans la nécessité de réécoute en vue de garantir la possibilité d'apporter des secours dans les meilleures conditions et dans la nécessité éventuelle de vérifier et prouver que les suites données étaient promptes et appropriées.

Ces motifs peuvent à notre avis être considérés comme rentrant dans les prévisions du législateur au regard des dispositions de l'article 4 § (3) invoqué.

Toutefois ledit texte légal ne rend-il légitime l'enregistrement du message et des données de trafic qu'à une double condition :

- il faut qu'il s'agisse d'un numéro d'appel d'urgence (destiné à alerter les secours) et
- que ledit numéro figure parmi ceux déterminés par votre Institut dans le but de permettre la réécoute lors de problèmes de compréhension ou d'ambiguïté.

Nous partageons votre avis que dans l'état actuel de la demande, le numéro 457575 ne répond pas

aux conditions de la loi parce qu'il donne accès à des services multiples et que son usage n'est pas strictement limité aux cas d'urgence.

Nous ne nous sentons en revanche pas en mesure de prendre position à l'égard de l'argument suivant lequel les numéros 460613 et 460614 devraient être exclus de la liste de numéros d'urgence à déterminer par votre Institut aux vœux de ladite disposition légale alors que les critères (il existe une relation contractuelle avec les personnes qui appellent, la communication est formée automatiquement suite au déclenchement manuel d'un bouton de téléalarme) que vous mentionnez ne figurent pas en tant que tels dans la loi.

Le législateur n'a entendu à notre avis restreindre son champ d'application qu'aux seuls numéros destinés à recevoir des appels formés en vue du déclenchement d'actions de secours à apporter par les services et organismes publics.

Il vous appartient sans doute, en application des pouvoirs que le législateur vous a délégués en la matière, de déterminer davantage les critères et de préciser les conditions qui doivent être remplies pour que vous acceptiez de porter un numéro d'appel donné sur la liste des numéros d'urgence visé par la disposition légale en question.

Décision type concernant la surveillance informatique (courrier électronique, utilisation de l'internet et du réseau informatique)

La société … S.A., établie et ayant son siège à L-…, …., inscrite au registre de commerce et des sociétés de Luxembourg sous le numéro B … (ci-après désignée « la requérante ») a introduit par courrier du …, une demande d'autorisation sur base de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après en abrégé « la loi »), enregistrée sous les références ….

La Commission nationale pour la protection des données (ci-après « la Commission nationale ») se déclare compétente pour examiner la demande d'autorisation lui présentée sur base des articles 3, 11 nouveau, 14 et 32 paragraphe (3), lettre (d) de la loi et de l'article L.261-1 paragraphe (1) du Code du Travail et reçoit la demande en la forme pour être conforme aux dispositions de l'article 14 paragraphe (2) de la loi.

Le traitement de données à caractère personnel en matière de surveillance du courrier électronique, de l'utilisation d'Internet et du réseau informatique tombe dans le champ d'application de diverses dispositions légales qu'il convient de rappeler brièvement avant de statuer sur le fond de la demande, notamment :

- la Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après dénommée « Directive cadre ») ;

- la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (ci-après dénommée «Directive vie privée et communications électroniques ») ;

- l'article 8, alinéa (1) de la Convention européenne des Droits de l'Homme ;

- l'article 7 de la Charte des droits fondamentaux de l'Union européenne ;

- l'article 28 de la Constitution ;

- la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après dénommée « la loi ») ;

- la loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques (ci-après dénommée « la loi du 30 mai 2005 ») ;

- la loi du 11 août 1982 concernant la protection de la vie privée (ci-après dénommée « la loi du 11 août 1982 ») ;

- l'article 460 du Code pénal ;

- le Code du travail et notamment ses articles L.261-1, L.261-2 et L.423-1.

1. Caractéristiques du traitement

1.1. Description du traitement envisagé

La requérante envisage de mettre en place un traitement de données à caractère personnel en vue de contrôler l'utilisation par ses employés du courrier électronique, de l'utilisation d'Internet et des réseaux informatiques.

Elle entend, dans un premier stade, recueillir des données statistiques (par exemple, le volume du trafic e-mail ou Internet, ou le volume des informations stockées sur chaque poste de travail) établies au moyen d'outils d'analyse spécifiques.

Dans une seconde étape, et dans l'hypothèse où un abus ou une anomalie est constaté, elle envisage un

contrôle ponctuel plus poussé qui pourrait avoir lieu sur une base individualisée.

En ce qui concerne plus particulièrement le courrier électronique, il est prévu d'utiliser des outils logiciels spécifiques pour analyser le trafic d'un point de vue statistique et pour mettre en évidence l'intensité du trafic, les points de saturation et les éventuels comportements anormaux ou attentatoires à la sécurité de l'infrastructure informatique de la requérante.

En ce qui concerne Internet, il est prévu d'effectuer la surveillance au moyen de logiciels spécifiques installés sur des serveurs proxy de la requérante. Des outils logiciels spécifiques seront utilisés pour analyser le trafic d'un point de vue statistique et mettre en évidence l'intensité du trafic, les points de saturation et les éventuels comportements anormaux ou attentatoires à la sécurité de l'infrastructure informatique de la requérante.

Pour l'utilisation des systèmes informatiques, la Commission nationale considère qu'on peut distinguer entre trois types de surveillance envisageables:

1) par l'accès direct aux fichiers et aux documents
2) par la consultation des fichiers de journalisation
3) par le recours à des logiciels de surveillance

En l'espèce, la requérante entend, dans certains cas, avoir accès aux documents et fichiers. De plus, elle a recours à des logiciels, notamment pour faire des recherches sur base de mots-clefs et pour déterminer le volume stocké sur chaque poste de travail.

1.2. Responsable du traitement et/ou sous-traitant

La requérante s'est désignée elle-même comme responsable du traitement.

1.3. Les personnes concernées

Les personnes concernées sont les employés de la requérante disposant d'un ordinateur et/ou d'un accès Internet et/ou d'un accès au courrier électronique.

1.4. Origine des données

Les données relatives au trafic du courrier électronique et de l'utilisation d'Internet sont collectées systématiquement par les infrastructures techniques y dédiées (infrastructure informatique, serveur web et serveur e-mail) lors de l'utilisation de ces infrastructures par les employés.

Les données stockées sur l'infrastructure informatique de la requérante et notamment sur le disque dur des ordinateurs sont constituées au fur et à mesure que les personnes concernées utilisent leur ordinateur.

1.5. Catégories de destinataires

Les destinataires des données sont :

- les membres de la direction de la requérante ;
- le responsable de la sécurité de l'information ; et
- pour des raisons techniques liées à la maintenance, le responsable informatique et les administrateurs système qui assurent la maintenance du système.

La Commission nationale tient à préciser que les données peuvent également être communiquées aux autorités publiques et judiciaires compétentes pour constater ou pour poursuivre des infractions pénales.

2. Légitimité du traitement

La loi définit la surveillance comme toute activité qui, opérée au moyen d'instruments techniques, consiste en l'observation, la collecte ou l'enregistrement de manière non occasionnelle des données à caractère personnel d'une ou de plusieurs personnes, relatives à des comportements, des mouvements, des communications ou à l'utilisation d'appareils électroniques et informatisés (article 2 (p) de la loi).

L'article 11 de la loi prévoit un régime spécial pour la surveillance sur le lieu de travail. Cet article stipule que « le traitement à des fins de surveillance sur le lieu de travail ne peut être mis en œuvre par l'employeur, s'il est le responsable du traitement, que dans les conditions visées à l'article L. 261-1 du Code du Travail. »

En l'espèce, les personnes concernées par le traitement à des fins de surveillance sont des travailleurs de la requérante.

Dans ces conditions, il y a lieu d'examiner la légitimité au regard de l'article 11 (« traitement à des fins de surveillance sur le lieu de travail ») de la loi.

2.1. Au regard des travailleurs de la requérante

Le régime de l'article 11 s'applique dès qu'il existe un lien de subordination entre le responsable du traitement et les personnes surveillées (travailleurs permanents et intérimaires).

Le régime doit être réputé d'application aux pratiques de surveillance envisagées par le responsable du traitement dans le secteur privé ainsi que dans le secteur public.

Le législateur a voulu prévoir une protection spéciale en définissant de manière restrictive les cas où la surveillance est autorisée. Il appert que le législateur a exclu le consentement du travailleur comme cause de légitimité (*document parlementaire n° 4735, p.99 et Projet de loi, document parlementaire n° 5554, p. 35*).

La requérante devra donc pouvoir se prévaloir d'un critère de légitimation prévue à l'article L.261-1 du Code du Travail.

Elle entend invoquer vis-à-vis de ses travailleurs comme cas d'ouverture légitimant la surveillance sur le lieu de travail l'article L.261-1 paragraphe (1) point 2. indiquant comme finalité « pour les besoins de protection des biens de l'entreprise ».

Selon la demande, le traitement serait nécessaire pour garantir :

i. la protection des intérêts économiques, commerciaux et financiers de la requérante auxquels est attaché un caractère de confidentialité ainsi que la lutte contre les pratiques contraires (notamment, la concurrence déloyale, la divulgation de données confidentielles, la violation du secret bancaire, de secrets d'affaire ou de droits de propriété intellectuelle de tiers, l'atteinte à l'image de marque)

ii. la continuité des activités de la requérante et la gestion régulière des affaires en cours, notamment en cas d'absence (congés ou maladie) des personnes concernées ;

iii. la sécurité et/ou le bon fonctionnement des systèmes informatiques de la requérante, y compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'entreprise (notamment contre les phénomènes de saturation ou d'engorgement, la propagation de virus, etc.).

Il s'ensuit que la demande d'autorisation de la requérante doit être analysée par la Commission nationale à la lumière des dispositions expresses de l'article L. 261-1 paragraphe (1) du Code du Travail ainsi que de la « ratio legis » ayant conduit à son adoption.

2.1.1. Quant à la notion de protection des biens

En ce qui concerne la notion de protection des biens, les documents parlementaires précisent que «… relèvent également de la protection des biens de l'entreprise les moyens de surveillance destinés à s'assurer que des virus ne pénètrent pas le réseau d'ordinateurs, que des fichiers professionnels ne soient pas détruits, que le réseau ne soit pas encombré. (cf. document parlementaire n° 4735/13, p. 21).La Commission nationale considère que « la protection des biens » vise les biens meubles et immeubles de l'entreprise, mais que cela ne comprend pas la protection d'intérêts économiques de l'entreprise autres que ceux liés à des biens meubles ou immeubles clairement identifiables. Il ne suffit pas d'invoquer un risque de préjudice financier ou un coût injustifié ou un manque à gagner.

Les travaux parlementaires indiquent que la sécurité et/ou le bon fonctionnement technique des systèmes informatiques de l'entreprise, ainsi que la protection physique des installations de l'entreprise (par ex. phénomènes d'engorgement, propagation de virus, spoofing, etc.) peuvent être inclus.

Sont également visés des biens incorporels comme les droits de propriété intellectuelle, les secrets d'affaires et de fabrication ainsi que les informations auxquelles est attaché un caractère de confidentialité.

La Commission nationale fait remarquer que d'autres finalités comme le contrôle du respect du code éthique de l'entreprise (notamment la prévention des comportements illicites et contraires aux bonnes

mœurs, la consultation de sites pornographiques, pédophiles et racistes, etc.) et le contrôle du respect de la charte informatique (visant par exemple à faire respecter les principes et règles en vigueur dans l'entreprise relatifs à l'usage d'Internet et de la correspondance électronique) ne tombent pas forcément sous la notion de « protection des biens de l'entreprise ».

La Commission nationale a déjà eu l'occasion d'attirer l'attention du gouvernement sur cette situation qui découle de l'optique du législateur de 2002 focalisée sur les mesures de vidéosurveillance.

Elle relève que la version initiale du projet de la loi n° 5181 envisageait d'ajouter à l'article 11 de la loi un critère de légitimation supplémentaire et spécifique « *pour détecter les actes susceptibles d'engager la responsabilité de l'employeur quel que soit son statut, public ou privé* » mais cet amendement a été retiré, de sorte que la loi n'a pas été complétée sur ce point.

De plus, dans son avis du 5 décembre 2005 relatif au projet de loi n°5554 portant modification de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, la Commission nationale a suggéré d'introduire des critères de légitimation supplémentaires pour qu'un traitement à des fin de surveillance soit possible « *lorsqu'une telle mesure est nécessaire :*

- pour assurer la prévention, la recherche et la détection d'actes illicites ou susceptibles d'engager la responsabilité de l'employeur, ou
- pour la protection des intérêts économiques, commerciaux ou financiers de l'employeur, ou
- *pour des besoins de formation des travailleurs ou pour l'évaluation et l'amélioration de l'organisation du travail, ou …* ».

Le législateur n'a cependant pas adopté de disposition nouvelle relative à ces critères de légitimation lors du vote du projet de loi.

2.1.2. Analyse des différentes finalités invoquées par la requérante

En ce qui concerne la finalité sub. (i) invoquée par la requérante, la Commission nationale estime que la protection contre des violations du secret bancaire et des divulgations de données confidentielles rentre dans le critère de légitimation de la protection des biens de l'entreprise prévu par l'article L.261-1 paragraphe (1) point 2. du Code du Travail.

La notion de biens de l'entreprise couvre également les droits intellectuels. La prévention de téléchargements illicites d'œuvres protégées à partir de l'Internet ne relève cependant pas de la protection des biens de l'entreprise. De telles pratiques peuvent certes engager la responsabilité de l'entreprise. Cependant, comme il vient d'être expliqué, la prévention d'actes susceptibles d'engager la responsabilité de l'employeur n'est pas prévue à titre de critère de légitimation.

La protection des biens de l'entreprise couvre seulement des actes de concurrence déloyale se faisant au moyen d'une atteinte à des informations de l'entreprise auxquelles est attaché un caractère de confidentialité.

La Commission nationale estime que la protection de l'image de marque n'est pas couverte non plus par la notion de « biens de l'entreprise ».

En ce qui concerne la finalité invoquée sub. (ii) poursuivie par la requérante (« continuité des activités de la requérante et la gestion régulière des affaires en cours »), il est renvoyé aux développements exposés aux points 3.1.1. et 3.1.3. de la présente délibération.

La finalité invoquée sub.(iii) cadre avec le critère de légitimation de la protection des biens de l'entreprise prévu par l'article L.261-1 paragraphe (1) point 2. du Code du Travail.

3. Conditions de licéité du traitement

La Commission nationale rappelle que tout traitement à des fins de surveillance (que ce soit le régime général visé à l'article 10 de la loi ou le régime particulier prévu à l'article 11 de la loi) doit, pour être licite être effectué conformément aux dispositions de l'article 4 de la loi (cfr. Document parlementaire 4735/13, p. 17).

L'article 4, paragraphe 1er de la loi stipule ce qui suit :

« le responsable du traitement doit s'assurer que les données qu'il traite le sont loyalement et licitement, et notamment que ces données sont ;

(a) Collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités ;

(b) Adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement ;

(c) Exactes et, si nécessaire, mises à jour ; toute mesure raisonnable doit être prise pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées ;

(d) Conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées… ».

Ci-après la demande de la requérante sera examinée par rapport au critère de licéité et au principe de la confidentialité des communications et du secret de la correspondance.

3.1. La licéité du traitement au regard des principes du secret de la correspondance et de la confidentialité des communications

3.1.1. Le contrôle du courriel

La Commission nationale relève qu'il y a lieu de distinguer deux catégories de courriers électroniques, les courriels personnels et les courriels professionnels, les deux catégories étant soumises au secret des correspondances.

En ce qui concerne les courriels à caractère professionnel, la Commission nationale estime que le responsable du traitement est lui-même à considérer comme destinataire ou expéditeur du courriel professionnel et que ce dernier peut dès lors procéder à un contrôle.

En raisonnant par analogie à la jurisprudence rendue en matière de courrier postal, la Commission nationale retient la présomption réfutable que les courriels échangés sur le lieu de travail sont de nature professionnelle.

Les courriels qui contiennent une indication marquant leur caractère privé et personnel ainsi que ceux dont cette nature résulte manifestement des circonstances doivent être réputés privés et personnels et ne peuvent pas être contrôlés.

En effet, le responsable du traitement est tenu de ne pas violer le secret des correspondances privées. Il ne peut donc pas ouvrir des courriers électroniques personnels des collaborateurs conformément à la loi du 11 août 1982 et la loi du 30 mai 2005.

A ce sujet, il convient de souligner que la Cour de cassation française a relevé que « *l'employeur ne peut dès lors sans violation de cette liberté fondamentale* [le droit au respect de l'intimité de la vie privée *prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur* » (chambre sociale, 2 octobre 2001). L'éventuelle interdiction par l'employeur d'une utilisation privée de la messagerie électronique ne confère donc pas pour autant à tous les courriels personnels la qualité de courriels professionnels.

Dans l'hypothèse où tous les courriels (personnels et professionnels) sont mélangés dans la boîte de réception de la messagerie électronique de l'employé, il sera difficile d'avoir accès aux messages de l'entreprise sans risquer de violer à cette occasion la confidentialité des messages à caractère personnel.

Pour cette raison, la Commission nationale recommande d'ailleurs soit de faire mettre en place pour leurs collaborateurs une double boîte de messagerie permettant de distinguer les messages personnels et les messages professionnels, soit d'inviter ces derniers à classer les messages reçus dans un dossier identifié comme « personnel » lorsqu'ils présentent un tel caractère.

En outre, les collaborateurs devraient être invités à marquer clairement la nature privée et personnelle dans l'objet des messages en question et à signaler à leurs correspondants d'adopter la même pratique.

En ce qui concerne la consultation des courriels pendant l'absence du collaborateur ayant comme but la poursuite des activités du responsable du traitement, la Commission se rallie aux suggestions du « *Guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique sur le lieu de travail* »[12] du Préposé fédéral (suisse) à la protection des données et à la transparence qui recommande à ce sujet :

« *Lors des absences prévisibles (telles que vacances, congés* […]*), les messages entrants peuvent être gérés de trois manières principales:*

- *définition d'une réponse automatique d'absence du bureau envoyée à l'expéditeur avec indication des personnes à contacter en cas d'urgence;*
- *définition d'une règle qui transfère au suppléant* [de la personne absente] *tous les messages entrants; cette solution a pour inconvénient toutefois que les messages de nature privée non marqués comme tels sont eux aussi transmis au suppléant;*
- *désignation d'un suppléant et définition d'un droit d'accès personnalisé (droit de lire et, si nécessaire, de traiter les messages entrants d'ordre professionnel); le suppléant n'a pas d'accès aux messages privés signalés comme tels; ce type de mesures permet de protéger la sphère privée du collaborateur absent; les expéditeurs de messages privés doivent être conscients du fait que leurs messages sont lus par le suppléant si rien ne permet de déterminer qu'il s'agit de messages privés.*

Pour les absences non prévisibles (maladie ou accident), chaque collaborateur devrait avoir un suppléant prédéfini ayant entre autres accès à son courrier électronique. »

Pour ce qui est de l'hypothèse du collaborateur quittant l'entreprise, la Commission nationale prend également à son compte les suggestions suivantes dudit guide :

« *Un employé qui va quitter l'entreprise doit avant son départ transférer à qui de droit les dossiers en cours (y compris les messages électroniques). Il certifie en outre par une déclaration qu'il a remis à l'entreprise tous les documents de nature professionnelle. On doit lui offrir la possibilité de copier les messages électroniques et autres documents de nature privée sur un support privé, puis de les effacer des serveurs de l'entreprise.*

A la fin du dernier jour de travail au plus tard, son compte de courrier électronique (comme d'ailleurs ses autres comptes informatiques) doit être bloqué et sa boîte à lettres (comme du reste ses autres supports de données personnelles) effacée; cette règle s'applique également en cas de décès. Il serait bon que l'employeur s'engage par écrit à le faire. Les personnes qui enverront un message à l'adresse bloquée seront automatiquement informées du fait que cette adresse n'existe plus. La réponse automatique pourra en outre indiquer une adresse alternative. »

Les données relatives aux courriels par les collaborateurs consultés dans ces circonstances (absence, départ du collaborateur) ne devront pas être utilisées par l'employeur à l'égard du collaborateur pour l'évaluation de celui-ci, à des fins disciplinaires ou dans des litiges de quelque nature que ce soit.

3.1.2. Le contrôle de l'utilisation de l'Internet

Conformément à l'article 5 de la Directive vie privée et communications électroniques et à l'article 4 de la loi du 30 mai 2005, l'utilisation d'Internet est couverte par le principe de confidentialité des communications. Dans ce contexte, l'accès Internet des collaborateurs est censé être donné pour des raisons professionnelles. La jurisprudence retient ainsi dans le même ordre d'idée que « *les connexions établies par un salarié sur des sites Internet pendant son temps de travail grâce à l'outil informatique mis*

12 http://www.edoeb.admin.ch/dokumentation/00445/00472/00532/index.html?lang=fr

à sa disposition par son employeur pour l'exécution de son travail sont présumées avoir un caractère professionnel » (Cour de cassation française, chambre sociale, 9 juillet 2008).

L'employeur ne peut toutefois contrôler l'utilisation d'Internet que si les personnes concernées ont été informées clairement et préalablement dudit contrôle par le biais d'une charte, d'une police ou d'une clause contractuelle qui contient les informations prévues par la présente délibération et sous réserve du principe de proportionnalité (point 4 de la présente délibération).

3.1.3. Le contrôle des supports informatiques et des fichiers de journalisation

L'accès à des informations conservées sur les supports de stockage peut, dans certaines hypothèses, avoir une incidence sur le droit à la vie privée ainsi qu'à la confidentialité de la communication. Tel est le cas par exemple si des courriels privés sont conservés dans un ficher privé.

Selon la jurisprudence, « *les dossiers et fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel* ». (Cour de cassation française, chambre sociale, 18 octobre 2006).

En appliquant le principe de confidentialité des communications et le droit à la vie privée, on doit attribuer aux documents conservés dans un dossier personnel une protection similaire à celle attribuée aux documents qui font partie des communications privées. Ainsi, le responsable du traitement ne peut accéder aux dossiers ou fichiers identifiés comme privés sans la présence de la personne concernée. Par ailleurs, le collaborateur doit avoir la possibilité de s'opposer à l'ouverture des fichiers privés et doit être informé de cette possibilité au moment du contrôle.

La requérante envisage de procéder, en présence du salarié, à des « vérifications ponctuelles » des fichiers privés dans un certain nombre d'hypothèses. La Commission nationale rend la requérante attentive au fait que si l'ouverture ponctuelle d'un document ou d'un fichier privé se fait en présence du salarié, il faut encore que le droit d'opposition du salarié soit respecté.

La Commission nationale note que le demandeur fait également état de « recherches sur base de mots-clés ». A ce sujet, la Commission rend la requérante attentive au fait que de telles recherches ne saurait être effectuées pour le contenu de fichiers ou de documents privés.

Par analogie avec les principes exposés au point 3.2.1. en matière de courriels, la consultation des supports de stockage en l'absence du collaborateur afin d'assurer la continuité dans la poursuite des activités du responsable du traitement doit se faire dans le respect de la vie privée du collaborateur.

La Commission nationale recommande que l'employeur prenne des mesures destinées à assurer que les documents électroniques de l'entreprise soient accessibles pendant l'absence du collaborateur sans qu'il ne soit nécessaire d'ouvrir les dossiers personnels du collaborateur.

Elle recommande encore qu'à la fin de son emploi ou de ses prestations de services, la personne concernée soit habilitée à obtenir une copie des documents conservés dans son fichier privé. Au départ de la personne concernée, le responsable du traitement doit garantir qu'elle ait la possibilité d'effacer les dossiers personnels de l'outil informatique, le cas échéant en présence d'un représentant de l'employeur. A ce sujet, il convient de rappeler les suggestions du « *Guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique sur le lieu de travail* »[13] précité:

« *Un employé qui va quitter l'entreprise doit avant son départ transférer à qui de droit les dossiers en cours* […]. *Il certifie en outre par une déclaration qu'il a remis à l'entreprise tous les documents de nature professionnelle. On doit lui offrir la possibilité de copier les* […] *documents de nature privée sur un support privé, puis de les effacer des serveurs de l'entreprise.*»

13 http://www.edoeb.admin.ch/dokumentation/00445/00472/00532/index.html?lang=fr

3.2. Proportionnalité du contrôle

Le principe de proportionnalité requiert que la méthode de surveillance soit pondérée en fonction des risques concrets que le responsable veut prévenir. Un contrôle général a priori de toutes les données de communication, ainsi qu'un enregistrement de toutes ces données dans un but de surveillance, est considéré comme disproportionné.

Un contrôle général de l'utilisation de l'e-mail et d'Internet et de l'infrastructure informatique de toutes les personnes concernées est donc exclu en vertu du principe de proportionnalité.

Sauf exception légale, la surveillance permanente des personnes concernées est réputée disproportionnée. Même en cas d'interdiction totale de l'utilisation des outils informatiques à titre privé, le responsable du traitement n'a en principe pas le droit de contrôler l'usage de manière continue. Un tel contrôle constitue une ingérence radicale et non proportionnée pour les collaborateurs. La jurisprudence reconnait que les travailleurs doivent bénéficier également sur leur lieu de travail et pendant les heures de travail payées par l'employeur d'une sphère résiduelle de vie privée les protégeant contre une surveillance excessive de la part de l'employeur. Ainsi, la Cour de cassation française a jugé que « *le salarié a droit, même au temps et au lieu de travail, au respect de l'intimé de sa vie privée; que celle-ci implique en particulier le secret des correspondances* » (chambre sociale, 2 octobre 2001).

Le principe de proportionnalité exige que les mesures se limitent à une surveillance ponctuelle et le respect d'une graduation dans l'intensification de la surveillance (« progressive Kontrollverdichtung ») qui doit être justifié chaque fois par des indices et soupçons préalablement détectés. Ces vérifications ne peuvent être intensifiées graduellement qu'à l'égard des personnes concernées contre lesquelles les vérifications ponctuelles ont dégagé des indices d'abus ou de comportements irréguliers portant atteinte aux biens de l'entreprise tels qu'envisagés au point 2.1. (Légitimité) de la présente délibération.

La personne compétente pour effectuer les analyses non individualisées devra être clairement informée de ses responsabilités et en particulier de l'interdiction de faire des analyses individualisées à la première phase de la surveillance. Si les mesures dépassent une surveillance non individualisée, la Commission nationale recommande au responsable du traitement de demander au responsable informatique / administrateur réseau l'avis de la personne responsable de la protection des données dans l'entreprise ou d'un collaborateur ayant été formé à cet effet.

3.2.1. Contrôle du courrier électronique

En ce qui concerne le courrier électronique, la Commission nationale considère que la prise de connaissance systématique du contenu des courriers électroniques par l'employeur doit être qualifiée d'excessive et serait contraire aux dispositions légales susmentionnées.

La Commission nationale recommande que le responsable du traitement ait d'abord recours aux moyens préventifs comme des logiciels permettant de cibler les courriels suspects, tels que les logiciels qui identifient l'expédition de courriels en chaîne ou qui isolent et/ou bloquent ceux dont la taille est excessive et qui peuvent provoquer un engorgement ou un ralentissement du réseau.

Le contrôle du courrier électronique doit se faire dans une première phase sur base des données de trafic et de journalisation comme le volume, la fréquence, la taille, le format de leurs pièces jointes. Ces informations sont de préférence d'abord contrôlées sans identifier la personne concernée. Si des irrégularités sont constatées, le responsable du traitement peut dans une seconde phase passer à l'identification des personnes concernées.

Ce n'est qu'au moment où des irrégularités sont constatées que le contenu des courriels professionnels peut être contrôlé.

3.2.2. Contrôle de l'utilisation d'Internet

En ce qui concerne la surveillance des sites Internet consultés par la personne concernée, les données faisant l'objet du traitement sont des données de trafic et de journalisation (adresse des sites consultés). Ces données constituent des données à caractère personnel à partir du moment où l'employeur est en mesure d'établir un lien entre les adresses des sites consultés et un collaborateur particulier.

Le contrôle doit se faire d'abord de façon non individualisée, par exemple au moyen d'une liste d'adresses de sites consultés de façon globale sur une certaine période, sans que soient identifiés dans un premier temps les auteurs des consultations. Il pourra sur cette base repérer une durée anormalement élevée de consultation d'Internet ou la mention d'adresses de sites suspects et prendre les mesures de contrôle appropriées (en passant seulement à ce second stade à une surveillance individualisée).

La Commission nationale recommande la mise en place de moyens de protection préventive du réseau comme par exemple, l'installation d'un logiciel bloquant l'accès à certains sites. Le blocage de l'accès à certains sites pourrait également être effectué de façon automatique par un logiciel spécifique sur la base de mots-clés déterminés.

3.2.3. Contrôle des supports informatiques et des fichiers de journalisation

Pour autant que les enregistrements des fichiers de journalisation et des supports informatiques qui contiennent des données à caractère personnel soient exposés à une surveillance de la part du responsable du traitement, celle-ci devrait être considérée comme excessive si elle prenait la forme d'une analyse individualisée (collaborateur individuel identifié) sans graduation dans le rythme et l'envergure des données contrôlées.

De plus, la présence (avec la possibilité de s'opposer à l'ouverture des documents) de la personne concernée est requise pour que le responsable du traitement puisse prendre connaissance du contenu des fichiers dénommés comme privés (ou s'avérant de toute évidence comme étant étrangers à l'activité professionnelle).

3.2.4. Durée de conservation des données issues de la surveillance

Conformément à l'article 4, paragraphe 1, lettre (d) de la loi, les données traitées ne peuvent être conservées sous une forme permettant l'identification des personnes concernées que pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées.

Le stockage des données issues de la surveillance pendant un délai défini doit se faire conformément aux dispositions relatives à la confidentialité et à la sécurisation des traitements. Plus particulièrement, l'accès à ces données ne peut être autorisé que par le responsable du traitement et ce conformément aux conditions et pour les finalités strictes prévues pour l'exécution d'un contrôle.

Une durée limitée de conservation de données constitue une garantie supplémentaire afin d'éviter d'éventuels détournements de finalité.

La Commission nationale considère qu'un délai de conservation des données issues de la surveillance de 6 mois est suffisant en l'espèce au regard des finalités poursuivies.

Dans l'hypothèse d'une anomalie ou d'un incident, les données peuvent toutefois être conservées au-delà du délai susmentionné dans le cadre de la transmission des données aux autorités judiciaires compétentes. Dans un cas pareil, les données peuvent être conservées selon les prescriptions légales ou toute obligation de conservation légale.

Les limites de conservation susmentionnées ne s'appliquent pas aux documents commerciaux et comptables qui peuvent être conservés jusqu'à l'expiration des délais de prescription applicables.

4. Mesures d'information

Il résulte de l'article 26 de la loi du 2002, ainsi de l'article L. 261-1 paragraphe 2 du Code de Travail que la personne concernée doit être adéquatement informée des mesures de surveillance la concernant. La loi prévoit deux niveaux dans cette obligation d'information, à savoir l'information individuelle d'une part et l'information collective d'autre part (cette dernière obligation s'applique seulement vis-à-vis des travailleurs de la requérante et non par rapport aux collaborateurs externes).

L'obligation d'information du responsable du traitement devra notamment porter sur :

- la description de la manière dont les systèmes de communication du demandeur peuvent

être utilisés à des fins privées par les personnes concernées (par exemple, les limites concernant les périodes et la durée d'utilisation) et dans quelle mesure l'utilisation du courrier électronique, d'Internet et du réseau informatique (par exemple, stockage des informations sur le disque dur) est autorisée ou tolérée ;

- l'information concernant la manière dont les données issues de la surveillance sont collectées et utilisées et qui est autorisé à utiliser ces données et dans quelles circonstances ;
- les finalités et les modalités du contrôle (c'est-à-dire, les raisons et les objectifs du contrôle, nature des données collectées, étendue et circonstances des contrôles, les destinataires des données) ;
- l'information concernant la durée de conservation des données issues de la surveillance ;
- les décisions pouvant être prises par le responsable du traitement à l'encontre de la personne concernée sur la base du traitement des données collectées à l'occasion d'un contrôle ;
- l'information sur le rôle des représentants des travailleurs tant dans la mise en œuvre de la politique de surveillance que dans les enquêtes relatives aux infractions présumées ;
- les modalités du droit d'accès de la personne concernée aux données à caractère personnel la concernant ;
- l'information des systèmes installés pour empêcher l'accès à certains sites ou pour détecter une éventuelle utilisation abusive.

Conformément aux dispositions de l'article L.261-1 paragraphe (1) deuxième alinéa du Code du travail et sans préjudice au droit à l'information de la personne concernée (y compris les travailleurs) visé à l'article 26 de la loi, « *sont informés préalablement par l'employeur : la personne concernée, ainsi que pour les personnes tombant sous l'empire de la législation sur le contrat du droit privé : le comité mixte ou, à défaut, la délégation du personnel ou, à défaut encore, l'inspection du travail et des mines ; pour les personnes tombant sous l'empire d'un régime statutaire : les organismes de représentation du personnel tels que prévus par les lois et règlements afférents* ».

5. Droit d'accès

L'article 28 de la loi confère à la personne concernée le droit d'accès aux données à caractère personnel la concernant.

Le droit de rectification n'est pas absolu et est soumis à la condition que les données sont incomplètes ou inexactes. Toutefois, la personne concernée a le droit d'obtenir l'effacement des données dont le traitement n'est pas conforme à loi.

6. Pays tiers à destination desquels des transferts de données sont envisagés

Aucun transfert de données vers un pays tiers (hors Union Européenne) n'assurant pas un niveau de protection adéquate n'est envisagé.

7. Mesures de sécurité prévues aux articles 22 et 23 de la loi

7.1. Généralités

Des mesures de sécurité organisationnelles et techniques suffisantes doivent être prises, conformément aux articles 22 et 23 de la loi, afin d'assurer la protection des données traitées contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute forme de traitement illicite.

L'ensemble des mesures prises pour assurer la sécurité du traitement en application des articles 22 et 23 de la loi doit conférer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger, le tout en fonction

du risque d'atteinte à la vie privée, ainsi que de l'état de l'art et des coûts liés à la mise en œuvre dudit traitement. Ces mesures doivent également viser à prévenir tout autre risque d'atteinte aux données tel que leur vol, leur effacement, etc. ainsi que tout risque d'utilisation pour d'autres finalités.

Lorsque le responsable du traitement s'adjoint les services d'un sous-traitant pour la mise en œuvre du traitement, un contrat ou un acte juridique écrit conforme aux dispositions de l'article 22, paragraphe (3) doit être signé.

7.2. Le rôle des administrateurs systèmes / réseaux informatiques

Les administrateurs qui doivent veiller à assurer le fonctionnement normal et la sécurité des réseaux et systèmes informatiques sont conduits par leurs fonctions mêmes à avoir accès à l'ensemble des informations relatives aux utilisateurs (messagerie, connexions à Internet, fichiers «logs» ou de journalisation, etc.) y compris celles qui sont enregistrées sur le disque dur du poste de travail.

La Commission nationale prend à son compte les remarques et exigences suivantes de la Commission Nationale de l'Informatique et des Libertés française (CNIL)[14] :

« *En tout état de cause, l'accès aux données enregistrées par les employés dans leur environnement informatique - qui sont parfois de nature personnelle - ne peut être justifié que dans les cas où le bon fonctionnement des systèmes informatiques ne pourrait être assuré par d'autres moyens moins intrusifs.*

De plus, aucune exploitation à des fins autres que celles liées au bon fonctionnement et à la sécurité des applications des informations dont les administrateurs de réseaux et systèmes peuvent avoir connaissance dans l'exercice de leurs fonctions ne saurait être opérée, d'initiative ou sur ordre hiérarchique.

De même, les administrateurs de réseaux et systèmes, généralement tenus au secret professionnel ou à une obligation de discrétion professionnelle, ne doivent pas divulguer des informations qu'ils auraient été amenés à connaître dans le cadre de leurs fonctions, et en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des utilisateurs et ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt de l'entreprise. Ils ne sauraient non plus être contraints de le faire, sauf disposition législative particulière en ce sens. »

7.3. Précisions relatives aux fichiers de journalisation

Les fichiers de journalisation des connexions destinés à identifier et enregistrer toutes les connexions ou tentatives de connexion à un système automatisé d'informations constituent des mesures favorisant la sécurité et la confidentialité des données à caractère personnel, lesquelles ne doivent pas être accessibles à des tiers non autorisés ni utilisées à des fins étrangères à celles qui justifient leur traitement. Ils n'ont pas pour vocation première le contrôle des utilisateurs.

« *La finalité de ces fichiers de journalisation, qui peuvent également être associés à des traitements d'information dépourvus de tout caractère nominatif mais revêtent un caractère sensible pour l'entreprise ou l'administration concernée, consiste à garantir une utilisation normale des ressources des systèmes d'information et, le cas échéant, à identifier les usages contraires aux règles de confidentialité ou de sécurité des données définies par l'entreprise.* » (CNIL)[15]

Le recours à des fichiers de journalisations, en tant que tel, n'est pas à considérer comme un traitement à des fins de surveillance au sens de la loi.

En revanche, la mise en œuvre d'un logiciel d'analyse des différents journaux (applicatifs et systèmes) permettant de collecter des informations individuelles poste par poste pour contrôler l'activité des utilisateurs, doit être considéré comme un traitement à des fins de surveillance avec toutes les conséquences que cela comporte telles que la nécessité d'une autorisation de

14 http://www.cnil.fr/fileadmin/documents/approfondir/rapports/Rcybersurveillance-2004-VD.pdf

15 http://www.cnil.fr/fileadmin/documents/approfondir/rapports/Rcybersurveillance-2004-VD.pdf

la Commission nationale, la limitation des mesures au critère de légitimation de la protection des biens et la proportionnalité des contrôles éventuels.

La Commission nationale se rallie également aux conclusions suivantes de la CNIL :

« *Dans tous les cas de figure, les utilisateurs doivent être informés de la mise en place des systèmes de journalisation et de la durée pendant laquelle les données de connexion permettant d'identifier le poste ou l'utilisateur s'étant connecté sont conservées ou sauvegardés. Cette information, qui réalise l'obligation légale à laquelle est tenu le responsable du traitement, est de nature à prévenir tout risque et participe de l'exigence de loyauté dans l'entreprise ou l'administration.*

Une durée de conservation de l'ordre de 6 mois ne paraît pas excessive au regard de la finalité des fichiers de journalisation. »

Compte tenu des développements qui précèdent, la Commission nationale, réunissant ses trois membres effectifs et délibérant à l'unanimité des voix :

délivre l'autorisation sollicitée en matière de surveillance des installations informatiques utilisées ainsi que de leurs communications électroniques ;

autorise la requérante à recourir aux mesures envisagées de surveillance des installations informatiques utilisées ainsi que de leurs communications électroniques, selon les modalités précisées dans sa demande du …, sous réserve de respecter les conditions de la présente délibération et notamment de respecter les restrictions et conditions suivantes :

- les données issues de la surveillance ne peuvent pas être conservées au-delà d'une période de 6 mois à compter de leur collecte.
- les communications électroniques personnelles et les fichiers privés et personnels (caractérisés comme personnels ou s'avérant de toute évidence comme étant étrangers à l'activité professionnelle) ne doivent pas être contrôlés.
- les travailleurs susceptibles d'être exposés à la surveillance de leur utilisation des outils informatiques et communications électroniques doivent en être préalablement informés par l'employeur conformément à l'article 26 de la loi modifiée du 2 août 2002 et à l'article L.261-1 paragraphe 2 du Code du Travail.
- le traitement doit être strictement limité aux finalités admises au point 2.1.2. (Analyse des différentes finalités invoquées par la requérante) de la présente délibération ;
- la surveillance devra être mise en œuvre dans le respect du principe de proportionnalité, ce qui implique (i) l'absence de contrôle général et continu ; (ii) le suivi d'une procédure dite d'une graduation dans l'intensification de la surveillance (« progressive Kontrollverdichtung ») impliquant que le contrôle :
    - o s'effectue sur base des données de trafic et de journalisation et seulement dans un deuxième temps sur les données de contenu ;
    - o est fait en premier lieu de façon non individualisée, l'identification de la personne concernée présupposant la constatation préalable d'indices d'abus ou de comportements irréguliers portant atteinte à la sécurité des données et/ou au bon fonctionnement technique des systèmes informatiques et réseaux de l'entreprise ou à des droits protégés parmi ceux explicités au point 2. 1. (Légitimité) de la présente délibération ;
    - o doit se fonder sur des indices objectifs, spécifiques et ne doit pas déboucher sur une prise de connaissance préalable et systématique de toutes les données de trafic et de journalisation concernant chaque personne concernée. Une procédure d'individualisation est notamment requise là où les communications électroniques et les fichiers des personnes concernées suspectes sont distingués de ceux des personnes concernées non-suspectes.

- une information doit être prévue afin d'avertir la personne concernée de la constatation d'un usage abusif sur base des données de trafic et de journalisation.
- plus généralement, les données recueillies doivent être traitées loyalement et ne doivent être utilisées que pour les finalités sur lesquelles est fondée la présente autorisation.

Participation aux travaux européens

Documents adoptés par le groupe de travail «Article 29» en 2008

Document	Date d'adoption	Référence
Avis 3/2008 sur le projet de norme internationale de protection de la vie privée du code mondial antidopage	01.08.2008	**WP 156**
Document de travail sur les questions fréquemment posées (FAQ) concernant les règles d'entreprise contraignantes.	10.12.2008	**WP 155 rev. 03**
Document de travail établissant un cadre pour la structure des règles d'entreprise contraignantes	24.06.2008	**WP 154**
Document de travail établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes	24.06.2008	**WP 153**
Mandat du sous-groupe «Enforcement» de procéder à la 2e enquête commune	17.07.2008	**WP 152**
Avis 2/2007 concernant l'information des passagers au sujet du transfert de données des dossiers passagers (Passenger Name Record – PNR) aux autorités américaines, Adopté le 15 février 2007 et révisé et mis à jour le 24 juin 2008	24.06.2008	**WP 151**
Avis 2/2008 sur la révision de la directive 2002/58/CE concernant la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques»)	15.05.2008	**WP 150**
Letter to Commission Barrot enclosing the joint comments of the Article 29 Working Party and the Working Party on Police and Justice on the Communications from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, namely: «Preparing the next steps in border management in the European Union», COM (2008) 69 final, "Examining the creation of a European Border Surveillance System (EUROSUR)" COM (2008) 68 final, and "Report on the evaluation and future development of the Frontex Agency" COM (2008) 67 final.	29.04.2008	**WP 149**
Avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche	04.04.2008	**WP 148**
Document de travail 1/2008 sur la protection des données à caractère personnel de l'enfant	18.02.2008	**WP 147**
Programme de travail 2008-2009, Groupe de travail «article 29»	18.02.2008	**WP 146**

Working Party 29 – « Programme de travail 2008-2009»

Mission du groupe de travail

Le groupe de travail a été institué par l'article 29 de la directive 95/46/CE et a pour mission (article 30, paragraphe 1):

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

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

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

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

Ces mêmes tâches doivent également être remplies dans le secteur des communications électroniques (article 15, paragraphe 3, de la directive 2002/58/CE).

Activités en 2008-2009

En 2008-2009, sans préjudice des demandes d'avis formulées par la Commission, le groupe de travail a l'intention de se concentrer sur quatre principaux thèmes stratégiques et sur quelques questions d'actualité qu'il estime utile et urgent d'aborder dans le cadre de l'évolution de la protection des données.

Le groupe de travail devra relever trois défis majeurs en 2008-2009, et notamment:

i) les moyens d'améliorer l'impact de la directive 95/46/CE et le rôle du groupe de travail ;

ii) l'impact des nouvelles technologies ;

iii) l'environnement mondial (transferts internationaux de données, respect de la vie privée à l'échelle mondiale et compétences).

Les thèmes abordés seront donc les suivants :

I. Une meilleure mise en œuvre de la directive 95/46/CE

II. La protection des données lors des transferts internationaux

III. La protection des données en rapport avec les nouvelles technologies

IV. Une efficacité accrue du groupe de travail «article 29»

V. Les questions d'actualité

Ces différents thèmes peuvent être étroitement liés à plusieurs niveaux et le groupe de travail choisira donc le meilleur moyen de les traiter. Ils sont décrits de manière plus détaillée ci-après. Les sujets présentant un plus haut degré de priorité pour le groupe de travail sont marqués d'un astérisque (*).

À intervalles réguliers, le groupe de travail examinera la mise en œuvre de ce programme de travail et il se réserve le droit, le cas échéant, de le préciser davantage ou de le mettre à jour. Il prend également en considération le fait qu'au cours de la période 2008-2009, ce programme de travail sera mis en œuvre dans le cadre de quelque dix réunions plénières et d'environ quarante réunions de sous-groupes.

I. Meilleure mise en œuvre de la directive 95/46/CE

1. Interprétation des dispositions essentielles de la directive 95/46/CE – pour contribuer au projet de communication interprétative[16]

   a. «responsable du traitement» et «sous-traitant» (*) – article 2 de la directive 95/46/CE

16 Dans des documents isolés ou dans des documents thématiques.

b. «droit applicable» (*) – article 4 de la directive 95/46/CE

c. «restriction de la finalité» (*) – article 6 de la directive 95/46/CE

d. «raisons du traitement», et notamment le «consentement indubitable» et les «intérêts légitimes» - article 7 de la directive 95/46/CE

2. Instruments d'une mise en œuvre efficace (voir aussi IV)

a. Exécution (*)

b. Expériences nationales - délégués à la protection des données (*)

3. Nouveaux défis

a. Impact du traité modificatif (*)

b. Impact des évolutions technologiques (voir aussi III) et notamment des outils technologiques permettant de garantir la protection

II. La protection des données lors des transferts internationaux

1. Instruments spéciaux

a. Règles d'entreprise contraignantes (BCR) (*)

b. Sphère de sécurité

2. Respect de la vie privée à l'échelle mondiale et compétences

a. Favoriser l'adéquation (*)

b. Normes internationales (meilleure collaboration avec les différents organes normatifs – collaboration active avec ceux qui mettent au point des normes favorisant la prise en compte dès le départ des aspects liés au respect de la vie privée)

c. Droit applicable (voir aussi 1.b)

III. La protection des données en rapport avec les nouvelles technologies

1. Questions liées à l'Internet

a. Moteurs de recherche (*)

b. Réseaux sociaux en ligne (notamment pour les enfants et les adolescents) (*)

c. Établissement des profils de comportement, extraction de données (en ligne ou hors ligne) (*)

d. Radiodiffusion numérique

e. ICANN et WHOIS

2. Réexamen du cadre réglementaire des communications électroniques (*)

3. Gestion de l'identité

4. Administration en ligne

5. Biométrie (utilisation privée et publique – l'accent étant mis sur une application nouvelle ou spécifique de la biométrie) (*)

6. Informatique diffuse (ou ubiquité numérique)

a. Identification par radiofréquence (RFID) (*)

b. Intelligence ambiante

c. Systèmes de télépéage (*)

IV. Accroître l'efficacité du groupe de travail «article 29»

1. Le rôle du groupe de travail «article 29» (principes directeurs ou normes directrices pour l'élaboration des avis et la clarification du processus – objectif, priorités, public cible) (*)

2. Amélioration de l'efficacité :

a. Évaluation des documents du groupe de travail en tant qu'instruments pertinents permettant d'uniformiser les pratiques nationales (au niveau du groupe de travail «article 29») (*)

b. Échange des meilleures pratiques en matière de contrôle, y compris les expériences récentes en matière de désignation de délégués à la protection des données (au niveau national) (*)

3. Exécution Identifier les domaines, les secteurs ou les questions suscitant le plus de problèmes (sur la base des informations reçues des autorités chargées de la protection des données) et arrêter des actions communes pertinentes (*)

V. Questions d'actualité

1. Réutilisation des données à des fins de sûreté, et notamment les données relatives aux passagers aériens (données PNR) en Europe (*)
2. Données médicales (dossiers santé en ligne)
3. Archives et vie privée
4. Enfants et vie privée (voir aussi III.1.b) (*)
5. Mise en place d'un cadre pour les audits en matière de respect de la vie privée, destiné aux secteurs privé et public (*outil leur permettant d'évaluer eux-mêmes si les données qu'ils détiennent sont toujours nécessaires, proportionnées, exactes, à jour, etc*.)
6. Aspects financiers

   a) SWIFT/SEPA

   b) Éventuellement VISA/Mastercard
7. Marketing direct
8. Enquête préalable (*)

Working Party 29 – « Document de travail 1/2008 sur la protection des données à caractère personnel de l'enfant »

I – Introduction

1) – Contexte

Le présent avis porte sur la protection des informations concernant les enfants. Il est essentiellement destiné aux personnes qui gèrent les données à caractère personnel des enfants. Dans les écoles, il s'agit plus particulièrement des enseignants et des autorités scolaires. Il s'adresse également aux autorités nationales de contrôle de la protection des données, qui sont chargées de surveiller le traitement de ce type de données.

Ce document doit être envisagé dans le contexte de l'initiative générale de la Commission européenne décrite dans sa communication « Vers une stratégie européenne sur les droits de l'enfant ». En contribuant à cet objectif général, il cherche à renforcer le droit fondamental des enfants à la protection des données à caractère personnel.

Ce sujet n'est pas totalement nouveau pour le groupe de travail « Article 29 », qui a déjà adopté plusieurs avis relatifs à cette question. Ses avis sur le code de conduite « FEDMA » (avis 3/2003), sur l'utilisation des données de localisation (avis 5/2005) et sur les visas et les éléments d'identification biométrique (avis 3/2007) contiennent certains principes ou recommandations concernant la protection des données relatives aux enfants.

Le présent document a pour objectif de synthétiser cette question de manière structurée, en définissant les principes fondamentaux applicables (partie II) et en les illustrant par des références aux données scolaires (partie III).

Le domaine des données scolaires a été sélectionné car c'est l'un des plus importants secteurs de la vie des enfants et il représente une part significative de leurs activités quotidiennes.

Son importance tient également au caractère sensible de la plupart des données traitées dans les établissements scolaires.

2) – Objectif et champ d'application

L'objectif du présent document est d'analyser les principes généraux relatifs à la protection des données relatives aux enfants et d'expliquer leur pertinence dans un domaine sensible particulier, celui des données scolaires.

Ce faisant, il vise à identifier les questions importantes pour la protection des données relatives aux enfants en général et à donner des orientations aux personnes travaillant dans ce domaine.

Selon les critères définis dans les principaux instruments internationaux applicables dans ce domaine, un enfant est une personne de moins de 18 ans, à moins qu'il ou elle n'ait acquis la majorité légale avant cet âge.

Un enfant est un être humain dans toute l'acception du terme. À ce titre, il doit jouir de l'ensemble des droits d'une personne, y compris le droit à la protection de ses données à caractère personnel. Cependant, la situation de l'enfant est particulière et doit être envisagée sous deux perspectives, statique d'une part et dynamique d'autre part.

D'un point de vue statique, l'enfant est une personne qui n'a pas encore atteint la maturité physique et psychologique. D'un point de vue dynamique, l'enfant est dans la phase de développement physique et intellectuel qui fera de lui un adulte. Les droits de l'enfant et leur exercice, y compris le droit à la protection des données, doivent être exprimés de manière à tenir compte de ces deux perspectives.

Le présent avis est fondé sur la conviction que l'éducation et la responsabilité sont essentielles à la protection des données de l'enfant. Il examine les grands principes applicables dans ce domaine. La plupart se rapporte aux droits de l'enfant, mais sera envisagée dans le contexte de la protection des données.

Ces principes sont tous énoncés dans les principaux instruments internationaux en vigueur, dont certains se rapportent aux droits fondamentaux de l'homme

mais comprennent également des règles spécifiques aux enfants. Les plus importants sont les suivants :

- Déclaration universelle des droits de l'homme du 10 décembre 1948 – articles 25 et 26, paragraphe 3
- Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950 – article 8
- Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000 – article 24[17]

Les autres instruments qui se rapportent directement aux droits de l'enfant sont les suivants :

- Déclaration de Genève des droits de l'enfant de 1923
- Convention des Nations unies relative aux droits de l'enfant du 20 novembre 1989
- Convention européenne sur l'exercice des droits des enfants, Conseil de l'Europe, n.º 160, du 25 janvier 1996[18]

Il va de soi que la perspective générale de la protection des données à caractère personnel doit être systématiquement considérée telle qu'elle est consacrée dans les directives sur la protection des données (directive 95/46/CE du 24.10.1995 et directive 2002/58/CE du 12.7.2002) et, partiellement, dans d'autres instruments.[19]

II – Principes fondamentaux

A – Remarques générales

1) – Intérêt supérieur de l'enfant

Le principe juridique de base est celui de l'intérêt supérieur de l'enfant.[20]

Ce principe repose sur le raisonnement qu'une personne n'ayant pas encore atteint la maturité physique et psychologique a besoin d'une protection plus importante que les autres. Son objectif est d'améliorer les conditions pour l'enfant et de renforcer son droit au développement de sa propre personnalité. Ce principe doit être respecté par toutes les entités, publiques ou privées, qui prennent des décisions relatives aux enfants. Il s'applique également aux parents et aux autres représentants de l'enfant, lorsque leurs intérêts respectifs sont comparés ou lorsque l'enfant est représenté. Les représentants de l'enfant doivent appliquer ce principe en règle générale mais, en cas de conflit entre les intérêts de l'enfant et ceux de ses représentants, la décision revient au tribunal ou, le cas échéant, aux autorités chargées de la protection des données (DPA).

2) – Protection et soins nécessaires au bien-être des enfants

Le principe de l'intérêt supérieur de l'enfant exige une appréciation adéquate de sa situation. Cela implique la reconnaissance de deux éléments. Premièrement, l'immaturité de l'enfant le rend vulnérable, ce qui

17 Et aussi :
- Déclaration d'Helsinki, juin 1964, Pr. I-11,
- Pacte international relatif aux droits économiques, sociaux et culturels du 16 décembre 1966 –art. 10, paragraphe 3,
- Pacte international relatif aux droits civils et politiques du 16 décembre 1966 – arts. 16 et 24,
- Protocole facultatif du 16 décembre 1966.

18 Et aussi :
- Déclaration des Nations unies des droits de l'enfant du 20 novembre 1959.
- Recommandations de l'Assemblée parlementaire du Conseil de l'Europe sur différents aspects de la protection des enfants (n. 1071, 1074, 1121, 1286, 1551).
- Recommandations du Comité des ministres du Conseil de l'Europe sur la participation des enfants à la vie familiale, R (98)8, et la protection des données médicales, R (97), 5.
- Convention du Conseil de l'Europe sur les relations personnelles concernant les enfants, n.192, du 15 mai 2003.

19 - Lignes directrices de l'OCDE du 23 septembre 1980,
- Convention 108 du Conseil de l'Europe du 28 janvier 1981 et protocole additionnel du 8 novembre 2001,
- Principes directeurs des Nations unies du 14 décembre 1990.

20 Inscrit dans la Convention des Nations unies relative aux droits de l'enfant (article 3), puis réaffirmé par la Convention 192 du Conseil de l'Europe (article 6) et la Charte des droits fondamentaux de l'Union européenne (article 24, paragraphe 2).

doit être compensé par une protection et des soins appropriés. Deuxièmement, l'enfant ne peut jouir de son droit au développement qu'avec l'assistance ou la protection d'autres entités et/ou personnes.[21]

Cette protection incombe à la famille, à la société et à l'État.

L'on doit admettre que, pour garantir aux enfants le niveau de soins dont ils ont besoin, leurs données à caractère personnel devront parfois être traitées très largement et par plusieurs personnes. C'est principalement le cas dans les domaines sociaux : l'éducation, la sécurité sociale, la santé, etc. Ce n'est toutefois pas incompatible avec la protection adéquate et renforcée des données dans ces secteurs, même s'il convient d'être prudent lorsque l'on partage des données concernant les enfants. Ce partage peut faire perdre de vue le principe de finalité (limitation de la finalité) et créer le risque que des profils soient créés sans tenir compte du principe de proportionnalité.

3) – Droit au respect de la vie privée

En tant qu'être humain, l'enfant a droit au respect de sa vie privée.

L'article 16 de la Convention des Nations unies relative aux droits de l'enfant prévoit que nul enfant ne fera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.[22]

Toute personne, y compris les représentants de l'enfant, est tenue de respecter ce droit.

4) – Représentation

Les enfants ont besoin de représentants légaux pour exercer la plupart de leurs droits. Cela ne signifie pas pour autant que le statut de représentant prime de manière absolue ou inconditionnelle sur celui de l'enfant. En effet, l'intérêt supérieur de l'enfant peut parfois lui conférer des droits relatifs à la protection des données susceptibles de dépasser les souhaits de ses parents ou représentants. De même, l'obligation de représentation n'implique pas que l'enfant ne doit pas être consulté, à partir d'un certain âge, sur les sujets le concernant.

Si le représentant d'un enfant consent au traitement des données concernant celui-ci, l'enfant pourra, à sa majorité, revenir sur ce consentement. En revanche, s'il souhaite la poursuite du traitement de ses données, il doit donner son consentement explicite, si nécessaire.

Par exemple, si un représentant a donné son consentement explicite à la participation de son enfant à une étude clinique, le responsable du traitement des données devra s'assurer, à la majorité de la personne concernée, d'avoir une base valable pour poursuivre le traitement des données à caractère personnel de celle-ci. Le responsable doit en particulier obtenir le consentement explicite de la personne concernée afin de poursuivre l'étude, car des données sensibles sont en jeu.

À ce sujet, il convient de rappeler que le droit à la protection des données appartient à l'enfant et non à ses représentants, qui ne font que l'exercer.

5) – Intérêts concurrents : respect de la vie privée et intérêt supérieur de l'enfant

Le principe de l'intérêt supérieur peut jouer un double rôle. A priori, ce principe exige que la vie privée de l'enfant soit protégée le mieux possible, en donnant le plus large effet possible au droit à la protection des données de l'enfant. Cependant, dans certaines situations, l'intérêt supérieur de l'enfant et son droit au respect de la vie privée entrent en conflit. Dans ce cas, le principe de l'intérêt supérieur peut prévaloir sur le droit à la protection des données.

21 Le droit à la protection est si fondamental qu'il est inscrit dans la Déclaration universelle des droits de l'homme (article 25) et a été confirmé dans le Pacte international relatif aux droits civils et politiques (article 24), dans le Pacte international relatif aux droits économiques, sociaux et culturels (article 10, paragraphe 3) et, plus récemment, dans la Charte des droits fondamentaux de l'Union européenne (article 24).

22 6 Ce droit est une confirmation du droit général au respect de la vie privée, inscrit à l'article 12 de la Déclaration universelle, à l'article 17 du Pacte international relatif aux droits civils et politiques et à l'article 8 de la Convention européenne de sauvegarde des droits de l'homme.

C'est notamment le cas dans le domaine médical où, par exemple, les services d'aide sociale à la jeunesse peuvent exiger des informations pertinentes dans les affaires de négligence ou d'abus. De même, un enseignant peut révéler des données à caractère personnel à un assistant social afin de protéger un enfant physiquement ou psychologiquement.

Dans des cas extrêmes, le principe de l'intérêt supérieur peut également entrer en conflit avec l'obligation d'obtenir le consentement des représentants. Dans ce cas, l'intérêt supérieur de l'enfant doit également être privilégié, par exemple lorsque son intégrité mentale ou physique est en jeu.

6) – Adaptation au degré de maturité de l'enfant

Dans la mesure où l'enfant est une personne en développement, l'exercice de ses droits, y compris ceux relatifs à la protection des données, doit être adapté à son niveau de développement physique et psychologique. Non seulement les enfants sont en développement, mais ils ont droit à ce développement.[23] Les systèmes juridiques gèrent ce processus différemment d'un État à l'autre mais, dans toute société, les enfants devraient être traités en fonction de leur degré de maturité.[24]

Quant au consentement, il peut s'agir d'une simple consultation de l'enfant, d'un consentement parallèle de l'enfant et du représentant, voire du seul consentement de l'enfant, en fonction de son degré de maturité.

7) – Droit d'être consulté

Les enfants acquièrent progressivement la capacité de contribuer aux décisions qui les concernent. En grandissant, ils doivent être consultés plus régulièrement sur l'exercice de leurs droits, y compris ceux relatifs à la protection des données.[25]

Ce devoir de consultation consiste à prendre en compte les opinions de l'enfant, sans nécessairement s'y conformer.[26] Le droit d'être consulté s'applique à différents domaines, comme la géolocalisation, l'usage des images de l'enfant, etc.

B – Dans la perspective de la protection des données

1) – Champ d'application du cadre juridique existant en matière de protection des données

Les directives relatives à la protection des données, à savoir les directives 95/46/CE et 2002/58/CE, ne mentionnent pas explicitement le droit au respect de la vie privée des mineurs. Ces instruments juridiques s'appliquent à toute personne physique mais aucune disposition particulière n'est prévue concernant les questions spécifiques aux enfants. Cela ne signifie pas pour autant que les enfants n'ont pas droit au respect de la vie privée et qu'ils ne relèvent pas desdites directives. D'après la formulation des directives, elles s'appliquent à toute « personne physique » et comprennent par conséquent les enfants.

Eu égard au champ d'application personnel et matériel limité de la directive, un certain nombre de questions relatives à la protection de la vie privée des enfants dans le cadre de la directive subsiste. En effet, la plupart des dispositions ne tient pas directement compte des particularités de la vie des enfants. Le degré de maturité individuelle d'un enfant, ainsi que l'obligation de représentation pour les actes juridiques, posent des problèmes.

La nécessité de protéger les données de l'enfant doit prendre en compte deux aspects importants : d'une part, les différents degrés de maturité déterminant quand l'enfant peut commencer à gérer ses données à caractère personnel et, d'autre part, la mesure dans

23 Convention des Nations unies relative aux droits de l'enfant – articles 27 et 29.

24 Certains systèmes juridiques appliquent ce principe général en distinguant les périodes suivantes : avant 12 ans, entre 12 et 16 ans, et de 16 à 18 ans.

25 Convention des Nations unies relative aux droits de l'enfant (article 12), Charte des droits fondamentaux de l'Union européenne (article 24, paragraphe 1), Convention sur les relations personnelles concernant les enfants (article 6).

26 Ce critère est clairement indiqué dans la Recommandation du Comité des ministres du Conseil de l'Europe relative à la protection des données médicales – Rec. nº R (97) 5 du 13 février 1997, paragraphes 5.5 et 6.3.

laquelle les représentants ont le droit de représenter le mineur lorsque la révélation des données à caractère personnel risque de porter préjudice à l'intérêt supérieur de l'enfant.

Le point suivant traitera de la meilleure manière d'appliquer les règles existantes de la directive pour garantir la protection adéquate et efficace de la vie privée des enfants.

2) – Principes de la directive 95/46/CE

a) Qualité des données

Les principes généraux relatifs à la qualité des données prévus dans la directive 95/46/CE doivent être adaptés de manière adéquate aux enfants.

Cela signifie :

a.1) Loyauté

L'obligation de traiter les données à caractère personnel conformément au principe de loyauté (article 6, point a)) doit être interprétée strictement lorsqu'un enfant est concerné. Dans la mesure où un enfant n'est pas encore complètement mûr, les responsables du traitement doivent en avoir conscience et agir en toute bonne foi lors du traitement de ses données.

a.2) Proportionnalité et pertinence des données

Le principe fixé à l'article 6, point c), de la directive 95/46/CE dispose que seules les données adéquates, pertinentes et non excessives peuvent être collectées et traitées.

En appliquant les principes de l'article 6, point c), les responsables du traitement doivent accorder une attention particulière à la situation de l'enfant car ils doivent toujours respecter son intérêt supérieur.

Aux termes de l'article 6, point d), de la directive 95/46/CE, les données doivent être « exactes et, si nécessaire, mises à jour ; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées ».

L'enfant étant en évolution constante, les responsables du traitement des données devront être particulièrement attentifs à l'obligation de mise à jour des données à caractère personnel.

a.3) Conservation des données

À cet égard, il convient de garder à l'esprit le « *droit à l'oubli* » qui protège toute personne concernée, et *particulièrement* les enfants. L'article 6, point e), de la directive doit être appliqué en conséquence.

Dans la mesure où les enfants sont en développement, leurs données changent et peuvent être rapidement dépassées et non pertinentes pour l'objectif initial de la collecte de données. Dans ce cas, les données ne devraient pas être conservées.

b) Légitimité

La directive 95/46/CE fixe les principes fondamentaux de la protection des données que les États membres doivent respecter et mettre en œuvre. S'agissant du droit au respect de la vie privée des enfants, les articles 7 et 8 revêtent une importance majeure car ils fixent les critères légitimant le traitement des données.

Avant tout, le traitement est autorisé si la personne concernée a donné son consentement sans ambiguïté. La définition du terme « consentement » est précisée à l'article 2, point h), de la directive.

En d'autres termes, le consentement doit être éclairé et libre. Le consentement n'est cependant pas obligatoire dans tous les cas. En effet, le traitement peut être légitime si d'autres exigences légales sont remplies conformément à l'article 7, points b) à f). Ainsi, le traitement peut être autorisé lors de la signature d'un contrat.

Si les représentants portent atteinte à la vie privée de l'enfant en vendant ou en publiant ses données, la question se pose alors de savoir comment protéger le droit au respect de la vie privée si l'enfant concerné n'est pas conscient de ces atteintes. Les enfants ont besoin d'un tuteur légal mais, dans un cas comme celui-ci, ne peuvent exercer leurs droits. Si les enfants sont suffisamment mûrs pour déceler une atteinte à leur droit au respect de la vie privée, ils ont le droit d'être entendus par les autorités compétentes, y

compris les autorités chargées de la protection des données.

Concernant les autres conditions de l'article 7 de la directive qui légitiment le traitement des données, les principes de l'intérêt supérieur de l'enfant et de la représentation doivent également être respectés. Ainsi, à partir d'un certain âge, les enfants ont la capacité juridique de s'engager contractuellement, par exemple dans le domaine de l'emploi. Or, ces contrats ne sont valables qu'avec le consentement des représentants. Préalablement à la conclusion d'un contrat ou pendant son exécution, l'autre partie peut vouloir collecter des données sur l'enfant en tant qu'employé.

Les représentants facilitent le traitement des données en donnant leur consentement. Les parents ou les tuteurs doivent prendre les décisions en se fondant sur l'intérêt supérieur de l'enfant. Ils doivent prendre en considération la menace que peut constituer la révélation des données pour la vie privée de l'enfant et ses intérêts vitaux, par exemple en ne révélant pas ses données médicales. Il existe d'autres domaines dans lesquels même les enfants sont autorisés à prendre des décisions indépendamment de leurs représentants.

En ce qui concerne la condition précisée à l'article 7, point e), il convient de noter que le principe de l'intérêt supérieur de l'enfant peut également être considéré comme un intérêt public. Cela peut être le cas lorsque les services d'aide sociale à la jeunesse ont besoin des données à caractère personnel d'un enfant pour s'occuper de lui. Les dispositions de la directive s'appliquent alors directement à ces circonstances.

Cependant, la question se pose de savoir si les enfants habilités à conclure, dans certains cas, des actes juridiques sans le consentement de leurs représentants (dans les cas où ils jouissent de droits partiels) peuvent également donner un consentement valable au traitement de leurs données.

Selon les réglementations locales en vigueur, cela peut être le cas du mariage, de l'emploi, des questions religieuses, etc. Dans d'autres cas, le consentement de l'enfant peut être valable, à condition que le représentant ne s'y oppose pas. Il est également clair que le degré de maturité physique et psychologique de l'enfant doit être pris en compte et qu'à partir d'un certain âge, il est en mesure de prendre des décisions le concernant. Cela peut être important dans le cas où le représentant est en désaccord avec l'enfant, mais où celui-ci est suffisamment mûr pour prendre des décisions dans son propre intérêt, pour des questions d'ordre médical ou sexuel par exemple. Les cas où l'intérêt supérieur de l'enfant limite ou même prévaut sur le principe de représentation ne doivent pas être négligés et devraient être approfondis.

Le motif le plus large autorisant le traitement des données concerne l'intérêt légitime poursuivi par le responsable du traitement ou par un tiers (article 7, point f)), à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée. En évaluant la situation, il faut particulièrement prendre en compte le statut de l'enfant dont les données font l'objet d'un traitement, en gardant à l'esprit son intérêt supérieur.

c) Sécurité des données

L'article 17 de la directive 95/46/CE dispose « *Les États membres prévoient que le responsable du traitement doit mettre en oeuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés* » et précise que :

« *Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en oeuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger* ».

Les responsables du traitement et les sous-traitants doivent être conscients que les données relatives aux enfants exigent un niveau élevé de protection.

d) Droits de la personne concernée

d.1) Droit d'être informée

Il convient de noter que l'exigence de consentement dans le cadre de la directive est indissociable de l'obligation d'informer de manière adéquate la personne concernée (articles 10, 11 et 14).

Le groupe de travail a déjà abordé l'obligation d'information dans plusieurs documents. L'avis sur les « Dispositions davantage harmonisées en matière d'informations » (WP 100) et la « Recommandation concernant certaines exigences minimales pour la collecte en ligne de données à caractère personnel dans l'Union européenne » (WP 43) devraient particulièrement être pris en compte, dans la mesure où ces documents fournissent des orientations claires à ce sujet.

Pour informer les enfants, priorité doit être donnée aux messages structurés, rédigés dans un langage simple, concis et pédagogique facilement compréhensible. Un message court doit contenir les informations de base à fournir lors de la collecte des données à caractère personnel soit auprès de la personne concernée soit auprès d'un tiers (articles 10 et 11). Ce message doit être accompagné d'informations plus détaillées, éventuellement accessibles grâce à un lien hypertexte, où tous les détails pertinents sont fournis. Comme le groupe de travail l'avait souligné dans sa recommandation sur le traitement en ligne de données, il est essentiel de publier les informations à l'endroit et au moment appropriés, c'est-à-dire directement sur l'écran, préalablement à la collecte de données. Outre le fait qu'elle est exigée par la directive, cette mesure est particulièrement importante pour sensibiliser les enfants aux risques et dangers potentiels des activités en ligne. En effet, on peut affirmer que, dans l'environnement virtuel, contrairement au monde réel, il s'agit de la seule occasion pour l'enfant d'être informé de ces dangers.

d.2) Droit d'accès

Le droit d'accès est, en principe, exercé par le représentant de l'enfant, mais toujours dans l'intérêt de ce dernier. En fonction du degré de maturité de l'enfant, ce droit peut être exercé à sa place ou avec lui. Dans certains cas, l'enfant peut aussi être autorisé à exercer seul son droit d'accès.

Lorsque des droits très personnels sont en jeu (par exemple dans le domaine de la santé), l'enfant peut même demander à son médecin de ne pas révéler ses données médicales à son représentant.

Cela peut être le cas lorsqu'un adolescent donne des informations d'ordre sexuel à un médecin ou à une ligne d'assistance téléphonique, excluant explicitement ses représentants de ces informations.

Cela peut également être le cas lorsqu'un enfant ne fait pas confiance à son représentant et contacte les services d'aide sociale à la jeunesse, par exemple s'il est toxicomane ou a des tendances suicidaires.

La question se pose de savoir si les représentants peuvent avoir accès à ces détails et si l'enfant peut s'y opposer. Pour déterminer si le droit au respect de la vie privée de l'enfant prévaut sur le droit d'accès des représentants, les intérêts de toutes les parties concernées doivent être attentivement pesés. Lors de l'évaluation, l'intérêt supérieur de l'enfant revêt une importance particulière.

Dans le cas de l'accès aux données médicales, l'appréciation du médecin peut être utile pour évaluer s'il est opportun que les représentants aient accès aux données.

Les pratiques nationales peuvent également constituer des exemples utiles : au Royaume-Uni, les adolescents de plus de 12 ans sont autorisés à exercer seuls leur droit d'accès.

Dans plusieurs pays, le droit d'accès des représentants aux données de leur fille adolescente est limité en cas d'avortement.

D'une manière générale, les critères fixant les conditions d'accès aux données ne relèvent pas uniquement de l'âge de l'enfant, mais également de son degré de maturité et d'autonomie. Par exemple, savoir qui a fourni les données, les parents ou l'enfant, peut donner une indication sur ce point.

d.3) Droit d'opposition

L'article 14, point a), dispose que la personne concernée a le droit de s'opposer au traitement de ses données, au moins dans les cas visés à l'article 7, points e) et f), pour des raisons prépondérantes et légitimes. S'agissant d'enfants, ces raisons peuvent être particulièrement prépondérantes. Il convient également de rappeler que la personne concernée est autorisée, dans tous les cas, à s'opposer au traitement de ses données à des fins de prospection (article 14, point b)).

III – À l'école

Dans cette section, le présent avis s'attachera à montrer comment les principes fondamentaux rappelés ci-dessus peuvent être précisés dans le contexte scolaire. En effet, la vie d'un enfant se déroule autant à l'école qu'au sein de sa famille. Il est donc naturel que plusieurs questions relatives à la protection des données se posent dans le cadre de la vie scolaire des enfants. De nature très diverse, ces questions soulèvent différents problèmes.

1) – Dossiers scolaires

a) Information

Les questions relatives à la protection des données des enfants (et parfois de leur famille) peuvent se poser au sujet du dossier scolaire dès l'inscription à l'école. En effet, dans certains pays, la législation autorise les autorités scolaires à demander de compléter des formulaires contenant des données à caractère personnel afin de constituer un dossier scolaire, informatisé ou conservé sur d'autres supports.

Sur ce type de formulaires, la personne concernée doit être informée de la collecte et du traitement de ses données à caractère personnel, ainsi que des éléments suivants : la finalité, les responsables du traitement et les modalités d'exercice de son droit d'accès et de rectification sur ses données. Si ses données sont communiquées à un tiers, elle doit également en être informée.

b) Proportionnalité

Les données demandées ne doivent pas être excessives. Par exemple, les données concernant les diplômes universitaires des parents, leur profession ou leur situation d'emploi ne sont pas toujours nécessaires. Les responsables des données doivent évaluer si elles sont réellement nécessaires. Il convient d'être particulièrement attentif car ces informations peuvent être à l'origine de discriminations.

c) Non-discrimination

Certaines données contenues dans ces formulaires peuvent être à l'origine de discriminations, notamment les données relatives à la race, à la situation d'immigré ou à certains handicaps.

Ces informations sont généralement collectées pour s'assurer que l'école est sensibilisée et consacre l'attention nécessaire aux élèves rencontrant des difficultés culturelles (par exemple d'ordre linguistique) ou économiques.

Les principes d'intérêt supérieur et de limitation de la finalité doivent être les critères retenus lors du traitement de ces informations.

Une approche très stricte doit être adoptée concernant l'inscription de la religion des élèves. Celle-ci n'est acceptable que lorsque la nature (école religieuse) et l'objectif administratif le justifient, et uniquement dans la mesure strictement nécessaire. Aucune déduction superflue sur la religion de l'élève ne doit être tirée lorsque les données sont uniquement nécessaires à des fins administratives (par exemple, la participation à un cours de religion ou l'indication des préférences alimentaires).

Les informations sur le patrimoine et les revenus de la famille d'un enfant peuvent également être à l'origine de discriminations, mais peuvent être traitées dans l'intérêt de l'enfant, par exemple si les représentants demandent une bourse ou une réduction des frais de scolarité.

Toutes les données susceptibles d'entraîner une discrimination doivent être protégées par des mesures de sécurité appropriées, comme le traitement dans des dossiers distincts par du personnel qualifié et attitré, soumis au secret professionnel, et d'autres mesures adéquates.

Le consentement au traitement de toutes les données susceptibles d'entraîner une discrimination doit être clair et explicite.

d) Principe de finalité

d.1) Communication des données

Dans certains cas, les autorités scolaires fournissent le nom et l'adresse de leurs élèves à des tiers, très souvent à des fins de prospection.

C'est notamment le cas lorsque les données sont transmises à des banques ou des compagnies d'assurance souhaitant attirer des élèves dans leur clientèle ou lorsque des données scolaires sont

communiquées aux élus locaux. Cela constitue une atteinte au principe de finalité, dans la mesure où les données fournies à des fins scolaires sont utilisées de manière incompatible avec ces finalités.

Conformément à l'article 6, paragraphe 1, point b), de la directive 95/46/CE, les données relatives aux enfants ne peuvent pas être traitées ultérieurement de manière incompatible avec les finalités qui justifient leur collecte.

La question ici n'est pas que les enfants soient la cible d'une prospection, ce qui relève de la protection des consommateurs. Le problème est la collecte préalable de données à caractère personnel afin d'envoyer ultérieurement des messages de prospection aux personnes concernées. Ce traitement doit toujours être soumis au consentement préalable des représentants (et de l'enfant, en fonction de son degré de maturité).

Dans tous les cas où une opération de prospection est considérée comme légitime et compatible, ce traitement doit toujours être effectué de la manière la moins intrusive possible.

Outre les conditions mentionnées ci-dessus, si des données sur les parents et/ou les élèves sont demandées par un tiers à des fins de prospection, leur transmission doit toujours être soumise à l'information et au consentement préalables des représentants (et de l'enfant, en fonction de son degré de maturité).

d.2) Accès aux données

Les données contenues dans le dossier scolaire sont soumises à une stricte confidentialité, conformément au principe général énoncé à l'article 16 de la directive 95/46/CE.

Le traitement des données d'une nature particulière est soumis à des exigences spécifiques de sécurité.

La liste ci-dessous fournit des exemples de ce type de données :

- procédures disciplinaires,
- consignation de cas de violence,
- traitement médical à l'école,
- orientation scolaire,
- enseignement spécialisé pour les personnes handicapées,
- assistance sociale pour les élèves défavorisés.

Les représentants de l'élève (et l'élève lui-même, en fonction de son degré de maturité) doivent avoir accès aux données. Cet accès doit être strictement réglementé et limité aux autorités scolaires, aux inspecteurs, au personnel de santé et aux services répressifs.

d.3) Résultats scolaires

Selon les pays, les traditions diffèrent quant à la publication des résultats scolaires. Dans certains pays, publier les résultats est une tradition établie de longue date.

Elle a pour objectif de permettre la comparaison des résultats et de faciliter les éventuelles plaintes ou recours.

Dans d'autres pays, même les résultats sont soumis à la règle générale de la confidentialité applicable aux données contenues dans le dossier scolaire. Dans ces cas, les résultats peuvent être révélés aux représentants de l'élève exerçant leur droit d'accès.

D'une manière générale, les résultats ne devraient être publiés que lorsque c'est nécessaire et seulement après avoir informé les élèves et leurs représentants des objectifs de la publication et de leur droit d'opposition.

Un problème particulier se pose avec la publication des résultats scolaires sur l'Internet, qui représente un moyen pratique de les communiquer aux personnes concernées. Les risques inhérents à ce mode de communication exigent que l'accès à ces données soit protégé par des garanties spécifiques, par exemple un site Internet sécurisé ou l'attribution de mots de passe personnels aux représentants ou à l'enfant, en fonction de son degré de maturité.

Les modalités du droit d'accès sont différentes en fonction du degré de maturité de l'enfant. Selon toute probabilité, à l'école primaire, l'accès sera principalement exercé par les représentants, tandis qu'à l'école secondaire, les élèves pourront également accéder à leurs données.

d.4) Conservation et suppression

Le principe général selon lequel aucune donnée ne doit être conservée plus longtemps qu'il n'est nécessaire aux finalités de la collecte s'applique également dans ce contexte. Dès lors, une attention particulière doit être portée aux données des dossiers scolaires à conserver pour des raisons pédagogiques ou professionnelles, et à celles à supprimer, par exemple celles concernant les procédures et les sanctions disciplinaires.

2) – Vie scolaire

Des questions relatives à la protection des données dans le cadre de la vie scolaire se posent dans les domaines suivants.

a) Données biométriques – accès à l'école et à la cantine

Ces dernières années ont été marquées par une augmentation des contrôles d'accès aux écoles pour des raisons évidentes de sécurité. Ces contrôles d'accès impliquent la collecte, à l'entrée, de données biométriques, comme les empreintes digitales, l'iris ou le contour de la main. Or, dans certaines situations, de tels moyens sont disproportionnés par rapport à l'objectif et ont des effets excessivement intrusifs.

D'une manière générale, le principe de proportionnalité doit également être appliqué à l'utilisation de ces éléments biométriques.

Il est vivement recommandé de permettre aux représentants légaux de s'opposer facilement à l'utilisation des données biométriques de leur enfant. S'ils exercent ce droit, l'enfant devrait recevoir une carte ou un autre moyen d'accès aux locaux de l'école.

b) Télévision en circuit fermé (CCTV)

Les écoles ont de plus en plus tendance à recourir à la télévision en circuit fermé pour des raisons de sécurité. Il n'existe pas de solution recommandée convenant à tous les aspects de la vie scolaire et à tous les lieux d'une école.

Dans la mesure où la télévision en circuit fermé peut porter atteinte aux libertés individuelles, son installation dans les écoles exige une attention particulière. Elle ne sera installée que si nécessaire et s'il n'existe pas d'autres moyens moins intrusifs donnant le même résultat. La décision d'installer un système de télévision en circuit fermé doit être précédée d'une discussion approfondie entre les enseignants, les parents et les représentants des élèves, en prenant en compte les objectifs affichés de cette installation et l'adéquation des systèmes proposés.

À certains endroits, la sécurité revêt une importance primordiale. La télévision en circuit fermé se justifie alors plus facilement, par exemple à l'entrée et à la sortie des écoles, ainsi que dans d'autres lieux de passage, pas uniquement du personnel scolaire, mais également d'autres personnes visitant les locaux de l'école pour quelque raison que ce soit.

Le choix de l'emplacement des caméras de télévision en circuit fermé doit toujours être pertinent, adéquat et non excessif par rapport à la finalité du traitement. Dans certains pays, par exemple, le recours à des caméras de télévision en circuit fermé en dehors des horaires scolaires a été considéré comme adéquat au regard des principes de la protection des données.

En revanche, dans la plupart des autres endroits de l'école, le droit des élèves au respect de la vie privée (ainsi que celui des enseignants et de l'ensemble du personnel scolaire) et la liberté fondamentale d'enseignement mettent en question la nécessité d'une surveillance permanente par la télévision en circuit fermé.

C'est particulièrement le cas dans les salles de classe, où la vidéosurveillance peut entraver non seulement la liberté d'apprentissage et de parole des étudiants, mais également la liberté d'enseignement. Cela s'applique également dans les espaces de loisirs, les gymnases et les vestiaires, où la surveillance peut porter atteinte au droit au respect de la vie privée.

Ces remarques sont également fondées sur le droit de tous les enfants au développement de leur personnalité. En effet, la conception qu'ils se forgent progressivement de leur propre liberté peut être faussée s'ils supposent, dès le plus jeune âge, qu'il est normal d'être surveillé par télévision en circuit fermé. C'est d'autant plus vrai si des webcams ou des

dispositifs similaires sont utilisés pour surveiller les enfants à distance pendant les horaires scolaires.

Dans tous les cas où la télévision en circuit fermé est justifiée, les enfants, le reste de la population scolaire et les représentants doivent tous être informés de l'existence de cette surveillance, des personnes qui en sont responsables et de ses objectifs. L'information destinée aux enfants doit être appropriée à leur niveau de compréhension.

La justification et la pertinence d'un système de télévision en circuit fermé doivent être revues régulièrement par les autorités scolaires pour décider s'il doit être maintenu. Les représentants des enfants doivent en être informés.

c) État de santé

Les données sur l'état de santé des élèves sont des données sensibles. Pour cette raison, leur traitement doit respecter strictement les principes de l'article 8 de la directive. Ces données doivent être traitées uniquement par des médecins ou par les personnes qui « prennent soin » directement des élèves, comme les enseignants et les autres membres du personnel scolaire liés au secret par l'éthique du secret professionnel.

Le traitement des données de ce type dépend du consentement des représentants de l'enfant ou de ses intérêts vitaux en cas d'urgence liée à la vie scolaire ou éducative.

d) Sites Internet des écoles

De plus en plus d'écoles créent leur site Internet pour les étudiants/élèves et leur famille. Ces sites deviennent le principal outil pour les communications externes. Les écoles doivent avoir conscience que la diffusion d'informations personnelles demande un respect plus strict des principes fondamentaux de la protection des données, notamment la minimisation des données et la proportionnalité. De plus, il est recommandé de mettre en place des systèmes de contrôle d'accès afin de protéger les informations personnelles (par exemple grâce à un identifiant utilisateur et un mot de passe).

e) Photos

Les écoles sont souvent tentées de publier (dans la presse ou sur l'Internet) des photos de leurs élèves. Elles doivent être mises en garde au sujet de cette publication sur l'Internet. Il s'agira de toujours évaluer le type de photo, la pertinence de la mise en ligne et l'objectif visé. Les enfants et leurs représentants doivent être informés de la publication et le consentement préalable des représentants (ou de l'enfant, en fonction de son degré de maturité) doit être obtenu.

Des dérogations sont admissibles pour les photos collectives, notamment de manifestations scolaires si, par nature, elles ne permettent pas l'identification facile des élèves.

f) Cartes scolaires

Pour le contrôle de l'accès et la surveillance des achats : de nombreuses écoles utilisent des cartes scolaires non seulement pour contrôler l'accès à l'école, mais également pour surveiller les achats des enfants. On peut se demander si le second objectif est entièrement compatible avec le respect de la vie privée de l'enfant, particulièrement à partir d'un certain âge.

Quoi qu'il en soit, ces deux fonctions doivent être distinctes, la seconde étant susceptible de soulever des questions relatives au respect de la vie privée.

Pour la localisation des élèves[27]: une autre méthode de surveillance utilisée dans certaines écoles (par carte ou non) est la localisation des élèves par l'intermédiaire de badges IRF. Dans ce cas, la pertinence d'un tel système doit être justifiée au regard des risques spécifiques en jeu, particulièrement lorsque d'autres méthodes de surveillance existent.

g) Visiophones à l'école

Les écoles peuvent jouer un rôle déterminant dans la mise en place de mesures de précaution quant à l'usage de MMS et d'enregistrements audio et vidéo, qui impliquent des données à caractère personnel de tiers, sans que la personne concernée en soit consciente. Les écoles doivent avertir leurs étudiants que la circulation illimitée d'enregistrements vidéo

27 Cf. WP 115 (adopté le 25 novembre 2005) sur les principes relatifs à la localisation des mineurs.

ou audio et d'images numériques peut entraîner de graves violations du droit au respect de la vie privée de la personne concernée et à la protection des données à caractère personnel.

3) – Statistiques scolaires et autres études

Les données à caractère personnel ne sont généralement pas nécessaires à l'établissement de statistiques (néanmoins, cela peut exceptionnellement être le cas, par exemple pour des statistiques sur l'intégration professionnelle).

Conformément à l'article 6, point e), de la directive, les résultats statistiques ne doivent pas permettre l'identification des personnes concernées directement ou indirectement.

Les études menées utilisent souvent diverses données à caractère personnel des élèves, obtenues par des questionnaires plus ou moins détaillés. La collecte de ces données doit être autorisée par les représentants (en particulier s'il s'agit de données sensibles) et les représentants doivent être informés de l'objectif et des destinataires de l'étude.

En outre, lorsqu'il est possible d'effectuer ces études sans identifier les enfants, cette procédure doit toujours être privilégiée.

IV – Conclusion

1) La législation

Le présent avis montre que, dans la plupart des cas, les dispositions fixées dans le cadre juridique actuel protègent efficacement les données relatives aux enfants.

L'application desdites dispositions conformément au principe de l'intérêt supérieur de l'enfant est cependant une condition préalable à la bonne protection de la vie privée des enfants. À cet effet, il convient de prendre en compte la situation particulière des mineurs et celle de leurs représentants. Les directives 95/46/CE et 2002/58/CE doivent être interprétées et appliquées en conséquence.

En cas de conflit d'intérêts, la solution pourra être recherchée dans l'interprétation des directives conformément aux principes généraux de la Convention des Nations unies relative aux droits de l'enfant, à savoir l'intérêt supérieur de l'enfant, ainsi que dans les autres instruments juridiques déjà mentionnés.

Les États membres sont encouragés à aligner leur législation sur l'interprétation mentionnée ci-dessus, en prenant les mesures nécessaires. D'autre part, au niveau communautaire, des recommandations ou d'autres instruments appropriés sur ce sujet seraient souhaitables.

Comme indiqué précédemment, le présent avis aborde uniquement les principes généraux pertinents pour la protection de la vie privée et des données des enfants, et leur application au domaine essentiel de l'éducation. D'autres domaines spécifiques pourraient justifier à l'avenir des études distinctes du groupe de travail.

2) La pratique

Le présent avis expose les préoccupations et considérations générales que suscitent la protection des données et de la vie privée en ce qui concerne les enfants. Le groupe de travail a choisi le domaine de l'éducation comme première étape pour aborder cette question en raison de l'importance que revêt l'éducation dans la société. Comme on peut le constater, l'approche retenue pour protéger la vie privée des enfants est fondée sur l'éducation – assurée par la famille, l'école, les autorités chargées de la protection des données, les groupes d'enfants, etc. –, concernant l'importance de la protection des données et de la vie privée, et les conséquences de la révélation des données à caractère personnel lorsque ce n'est pas nécessaire.

Si nos sociétés veulent créer une véritable culture de la protection des données, en particulier, et de la vie privée, en général, il convient de commencer par les enfants, non seulement parce qu'ils constituent une catégorie de personnes nécessitant une protection ou parce qu'ils sont titulaires de droits à la protection, mais également parce qu'ils doivent être informés de leur devoir de respecter les données à caractère personnel des autres.

Afin d'atteindre cet objectif, l'école doit jouer un rôle central.

Les enfants et les élèves doivent être éduqués de façon à devenir des citoyens autonomes dans la société de l'information. À cet effet, il est fondamental qu'ils apprennent dès leur plus jeune âge l'importance du respect de la vie privée et de la protection des données. Ces notions leur permettront par la suite de prendre des décisions en connaissance de cause sur les informations qu'ils souhaitent divulguer, à qui et dans quelles conditions. La protection des données doit être systématiquement intégrée dans les programmes scolaires, en fonction de l'âge des élèves et de la nature des matières enseignées.

Il ne devrait jamais arriver que, pour des raisons de sécurité, les enfants soient confrontés à une surveillance excessive limitant leur autonomie. Dans ce contexte, un équilibre doit être trouvé entre la protection de l'intimité et de la vie privée des enfants, et leur sécurité.

Les législateurs, les dirigeants politiques et les organismes éducatifs doivent, dans le cadre de leurs domaines de compétence respectifs, prendre des mesures efficaces pour résoudre ces questions.

Le rôle des autorités chargées de la protection des données repose sur quatre axes : éduquer et informer, particulièrement les enfants et les autorités responsables du bien être des jeunes ; amener les décideurs politiques à prendre les bonnes décisions concernant les enfants et la vie privée ; sensibiliser les responsables du traitement des données à leurs devoirs ; exercer leurs pouvoirs à l'encontre de ceux qui enfreignent la législation ou ne respectent pas les codes de conduite ou les meilleures pratiques dans ce domaine.

Dans ce contexte, une stratégie efficace peut être la conclusion d'accords entre les autorités chargées de la protection des données, les ministères de l'éducation et les autres organismes responsables, définissant des conditions claires et concrètes de coopération mutuelle dans ce domaine afin de diffuser l'idée que la protection des données est un droit fondamental.

Il faut notamment apprendre aux enfants qu'il leur incombe d'être les principaux protecteurs de leurs données à caractère personnel. C'est là un domaine où l'efficacité de la responsabilisation peut être démontrée.

Consultation publique

Le groupe de travail « Article 29 » invite les personnes qui gèrent les données à caractère personnel des enfants, notamment les enseignants et les autorités scolaires, ainsi que les particuliers, à formuler des commentaires sur le présent document de travail.[28]

28 Vous pouvez envoyer vos commentaires sur le présent document de travail au groupe de travail « Article 29 » - Secrétariat - Commission européenne, direction générale « Justice, liberté et sécurité »
Unité C.5 – Protection des données
Bureau : LX 46 6/80
B - 1049 Bruxelles
E-mail : Amanda.JOYCE-VENNARD@ec.europa.eu et
Kalliopi.Mathioudaki-Kotsomyti@ec.europa.eu;
Fax : +32-2-299 80 94
Tous les commentaires des secteurs public et privé seront publiés sur le site internet du groupe de travail « Article 29 », à moins que les répondants n'indiquent explicitement que certaines informations doivent rester confidentielles.

Working Party 29 – « Avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche »

Adopté le 4 avril 2008

Le groupe de travail a été établi en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.
Le secrétariat est assuré par la direction C (Justice civile, droits fondamentaux et citoyenneté) de la Commission européenne, direction générale de la justice, de la liberté et de la sécurité, B-1049 Bruxelles, Belgique, bureau n° LX-46 06/80.
Site internet: http://ec.europa.eu/justice_home/fsj/privacy/index_fr.htm

Table des matières

Résumé
1. Introduction
2. Définition d'un «Moteur de Recherche» Modèle d'entreprise
3. Quel type de données?
4. Cadre juridique
   4.1 Responsables du traitement des données d'utilisateur
   4.1.1. Le droit fondamental – le respect de la vie privée
   4.1.2. Applicabilité de la directive 95/46/CE (directive sur la protection des données)
   4.1.3 Applicabilité de la directive 2002/58/CE (directive sur la vie privée et les communications électroniques) et de la directive 2006/24/CE (directive sur la conservation des données)
   4.2 Fournisseurs de contenus
   4.2.1. Liberté d'expression et droit à la vie privée
   4.2.2 Directive sur la protection des données
5. La légalité du traitement
   5.1 Finalités/motifs mentionnés par les fournisseurs de moteurs de recherche
   5.2 Analyse des finalités et raisons par le groupe de travail
   5.3 Problèmes que l'industrie doit résoudre
6. Obligation d'informer la personne concernée
7. Droits de la personne concernée
8. Conclusions
Annexe 1 Exemple de données traitées par les moteurs de recherche et terminologie
Annexe 2

Résumé

Les moteurs de recherche font désormais partie de la vie quotidienne des personnes utilisant l'Internet et les technologies de recherche d'informations. Le groupe de travail «Article 29» reconnaît l'utilité de ces moteurs de recherche et il est conscient de leur importance.

Dans le présent avis, il dresse une liste précise des responsabilités qui, en vertu de la directive sur la protection des données (95/46/CE), incombent aux fournisseurs de moteurs de recherche en qualité de responsables du traitement de données d'utilisateur. Du fait de leur rôle de fournisseurs de données de contenu (en l'occurrence, l'index des résultats de recherche), les moteurs de recherche sont eux aussi soumis à la législation européenne en matière de protection des données dans des cas bien particuliers, par exemple s'ils proposent un service de stockage dans une mémoire cache, ou s'ils sont spécialisés dans l'établissement de profils de personnes. Le principal objectif poursuivi dans le présent avis est de parvenir à un équilibre entre les besoins légitimes des fournisseurs de moteurs de recherche dans l'exercice de leur activité et la protection des données à caractère personnel des internautes.

L'avis aborde la définition des moteurs de recherche, les types de données traitées dans le cadre des services de recherche, le cadre juridique, les finalités/raisons d'un traitement légitime, l'obligation d'informer les personnes concernées, et les droits de ces personnes.

L'une des principales conclusions de l'avis est que la directive sur la protection des données s'applique généralement au traitement des données à caractère personnel par les moteurs de recherche, même lorsque le siège de ces derniers se trouve en dehors de l'EEE, et qu'il incombe aux fournisseurs de moteurs de recherche qui se trouvent dans cette situation de clarifier leur rôle dans l'EEE ainsi que l'étendue de leurs responsabilités en vertu de la directive. Il ressort clairement que la directive sur la conservation des données (2006/24/CE) ne s'applique pas aux fournisseurs de moteurs de recherche.

L'avis conclut que les données à caractère personnel ne doivent être traitées qu'à des fins légitimes. Les fournisseurs de moteurs de recherche ont l'obligation de supprimer ou de rendre les données à caractère personnel totalement anonymes dès qu'elles ne servent plus les finalités déterminées et légitimes pour lesquelles elles ont été collectées, et ils doivent à tout moment être en mesure de justifier le stockage et la durée de vie des «cookies» envoyés. Le consentement de l'utilisateur est requis pour tout projet de recoupement entre données relatives à l'utilisateur et d'enrichissement du profil de ce dernier. Les moteurs de recherche doivent respecter les demandes d'exclusion d'indexation formulées par les éditeurs de sites Internet et répondre immédiatement aux demandes des utilisateurs concernant l'actualisation/ le rafraîchissement des mémoires caches. Le groupe de travail rappelle que les moteurs de recherche sont tenus d'informer clairement les utilisateurs à l'avance de toutes les utilisations prévues de leurs données, et de respecter leur droit de consulter, de vérifier ou de corriger aisément ces données personnelles conformément à l'article 12 de la directive sur la protection des données (95/46/CE).

Le groupe de protection des personnes concernant le traitement des données à caractère personnel

établi par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995[29],

vu les articles 29 et 30, paragraphe 1, point a), et paragraphe 3, de la directive, et l'article 15, paragraphe 3, de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002,

vu l'article 255 du traité CE et le règlement (CE) n° 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission,

vu son règlement intérieur,

A ADOPTÉ LE PRÉSENT DOCUMENT :

1. Introduction

Dans la société de l'information, les fournisseurs de moteurs de recherche sur Internet jouent un rôle essentiel d'intermédiaires. Le groupe de travail reconnaît la nécessité et l'utilité des moteurs de recherche, et il est conscient de leur contribution au développement de la société de l'information. Pour les autorités indépendantes de protection des données de l'EEE, l'importance croissante des moteurs de recherche du point de vue de la protection des données se traduit par l'augmentation du nombre croissant de plaintes reçues de particuliers (personnes concernées) au sujet de violations potentielles de leur droit à la vie privée. On constate également une hausse marquée des demandes des responsables du traitement des données et de la presse au sujet de l'effet des services de recherche sur Internet sur la protection des données à caractère personnel.

Ces plaintes de personnes concernées et ces demandes des responsables du traitement des données et de la presse reflètent les deux rôles différents joués par les fournisseurs de moteurs de recherche à l'égard des données à caractère personnel.

D'une part, en tant que prestataires de services aux utilisateurs, les moteurs de recherche collectent et traitent de grandes quantités de données d'utilisateur, dont celles recueillies par des moyens techniques, tels que les «cookies». Les données collectées peuvent aller de l'adresse IP des différents utilisateurs, ou d'historiques de recherche complets, ou encore de données fournies par les utilisateurs eux-mêmes lorsqu'ils s'inscrivent en vue d'utiliser des services personnalisés. Cette collecte de données d'utilisateur soulève dès lors de nombreuses questions. Après l'affaire AOL, beaucoup de gens ont pris conscience de la sensibilité des informations personnelles contenues dans les journaux de recherches[30] (*search logs*). Le groupe de travail est d'avis que les moteurs de recherche, dans leur rôle de collecteurs de données d'utilisateur, n'ont jusqu'à présent pas suffisamment expliqué la nature et la finalité de leurs opérations aux utilisateurs de leurs services.

D'autre part, en tant que fournisseurs de contenus, les moteurs de recherche contribuent à rendre les publications sur Internet facilement accessibles aux quatre coins de la planète. Certains moteurs de recherche republient des données dans ce que l'on appelle une «mémoire cache». Or, en recherchant et en regroupant des informations courantes de divers types au sujet d'une personne, ils peuvent créer un nouveau profil, avec un risque beaucoup plus grand pour la personne concernée que si toutes les données publiées sur Internet restaient séparées les unes des autres. Les capacités de représentation et d'agrégation des moteurs de recherche peuvent nuire considérablement aux individus, tant dans leur vie personnelle qu'au sein de la société, en particulier si les données à caractère personnel qui figurent dans les résultats de recherche sont inexactes, incomplètes ou excessives.

29 JO L 281 du 23/11/1995, p. 31, http://europa.eu.int/comm/internal_market/fr/media/dataprot/index.htm

30 Au cours de l'été 2006, le prestataire de services a publié un échantillon des requêtes et des résultats de quelque 650 000 utilisateurs sur une période de trois mois. Bien qu'AOL ait remplacé les noms des utilisateurs par des numéros, des journalistes ont découvert que ces résultats permettaient souvent de remonter aux différents utilisateurs, non seulement en raison de ce que l'on appelle les «recherches par vanité» (des personnes qui recherchent des informations sur elles-mêmes), mais aussi en combinant plusieurs requêtes effectuées par un seul utilisateur.

Le 15 avril 1998, le groupe de travail international sur la protection des données dans les télécommunications[31] avait adopté une position commune sur la protection de la vie arrivée et les moteurs de recherche qui a été révisée les 6 et 7 avril 2006[32]. Le groupe de travail y a exprimé sa préoccupation face au potentiel des moteurs de recherche de permettre la création de profils de personnes physiques. Cette position commune décrivait comment les activités des moteurs de recherche pouvaient constituer une menace pour la vie privée et indiquait que tout type d'informations personnelles publié sur un site Internet pouvait être utilisé par des tiers afin d'établir un profil.

En outre, une résolution sur la protection de la vie privée et les moteurs de recherches[33] a été adoptée lors de la 28e conférence internationale des commissaires à la protection des données et à la vie privée, organisée à Londres les 2 et 3 novembre 2006. Cette résolution appelle les fournisseurs de moteurs de recherche à respecter les règles de protection de la vie privée définies dans la législation nationale de nombreux pays et dans des traités et documents de politique internationaux et à modifier leurs pratiques en conséquence. Elle aborde plusieurs préoccupations relatives aux journaux de serveurs, aux requêtes de recherche combinées et à leur stockage, et à l'établissement de profils détaillés des utilisateurs.

2. Définition d'un «moteur de recherche» et modèle d'entreprise

De manière générale, les moteurs de recherche sont des services qui aident leurs utilisateurs à trouver des informations sur Internet. On peut les distinguer selon le type de données qu'ils visent à rechercher, y compris des images et/ou des vidéos et/ou du son ou différents types de formats. Les moteurs de recherche spécifiquement destinés à établir des profils de personnes à partir de données à caractère personnel trouvées un peu partout sur Internet constituent un nouveau domaine d'expansion.

Dans le contexte de la directive sur le commerce électronique (2000/31/CE), les moteurs de recherche sont considérés comme une catégorie de service de la société de l'information[34], en l'occurrence, des outils de localisation d'informations[35]. Le groupe de travail a utilisé cette catégorisation comme point de départ.

Dans le présent avis, le groupe de travail s'intéresse principalement aux fournisseurs de moteurs de recherche qui suivent le modèle d'entreprise dominant, fondé sur la publicité.

Il s'agit de tous les grands moteurs connus, ainsi que des moteurs spécialisés tels que ceux axés sur l'établissement de profils de personnes, et les méta-moteurs de recherche qui présentent, et éventuellement regroupent, les résultats d'autres moteurs de recherche existants. Le présent avis n'aborde pas les fonctions de recherche intégrées dans les sites Internet pour effectuer des recherches dans le seul domaine dudit site.

La rentabilité de ces moteurs de recherche dépend généralement de l'efficacité de la publicité qui accompagne les résultats des recherches. Dans la plupart des cas, les recettes sont générées au moyen de la méthode du «paiement par clic». Dans ce modèle, le moteur de recherche facture la société de publicité chaque fois qu'un utilisateur clique sur un lien sponsorisé. Une bonne partie des recherches sur la précision des résultats de recherche et de la publicité est axée sur la contextualisation. Pour que les moteurs de recherche produisent les résultats souhaités et ciblent correctement les publicités afin d'optimiser leurs recettes, ils tentent de déterminer au mieux les caractéristiques et le contexte de chaque requête.

31 Le groupe de travail a été créé à l'initiative des commissaires à la protection des données de différents pays afin de renforcer la protection de la vie privée et des données dans les télécommunications et les médias.

32 http://www.datenschutz-berlin.de/doc/int/iwgdpt/search_engines_en.pdf

33 http://www.privacyconference2006.co.uk/index.asp?PageID=3

34 Les moteurs de recherche sur internet sont abordés dans la législation européenne sur les services de la société de l'information, définis à l'article 2 de la directive 2000/31/CE. Cet article fait référence à la directive 98/34/CE, qui définit la notion de service de la société de l'information.

35 Voir l'article 21.2, en relation avec le considérant 18, de la directive sur le commerce électronique (2000/31/CE).

3. Quel type de données ?

Les moteurs de recherche traitent les données les plus diverses[36]. Une liste des données en question figure en annexe.

Fichiers-journaux

Les fichiers-journaux récapitulent l'utilisation faite par chaque personne du service de moteur de recherche sont - en supposant qu'ils ne sont pas rendus anonymes – les données à caractère personnel les plus importantes traitées par les fournisseurs de moteurs de recherche. Ces données qui décrivent l'utilisation des services peuvent être divisées en différentes catégories : les journaux des requêtes (contenu des requêtes de recherche, date et heure, source (adresse IP et «cookie»), préférences de l'utilisateur et données relatives à son ordinateur), les données relatives au contenu proposé (liens et publicités résultant de chaque requête) et les données relatives aux sites visités ensuite par l'utilisateur (clics). Les moteurs de recherche peuvent aussi traiter des données opérationnelles relatives aux données d'utilisateur, des données relatives aux utilisateurs enregistrés, et des données d'autres services et sources comme le courrier électronique, la recherche dans l'ordinateur de l'utilisateur (*desktop search*) et la publicité sur les sites Internet tiers.

Adresses IP

Un fournisseur de moteur de recherche peut relier différentes requêtes et sessions de recherche émanant d'une même adresse IP[37]. Il est ainsi possible de suivre et de corréler toutes les recherches sur Internet émanant d'une adresse IP si ces recherches sont enregistrées. L'identification peut encore être améliorée en mettant en parallèle l'adresse IP avec le «cookie» d'identification unique de cet utilisateur attribué par le fournisseur de moteur de recherche, puisque ce «cookie» ne changera pas lorsque l'adresse IP sera modifiée.

L'adresse IP peut également servir à la localisation même si, pour le moment, elle est très souvent inexacte.

«Cookies»

Les témoins de connexion ou «cookies» sont fournis par le moteur de recherche et stockés sur l'ordinateur de l'utilisateur. Le contenu des «cookies» varie d'un fournisseur de moteur de recherche à l'autre. Les «cookies» attribués par les moteurs de recherche contiennent généralement des informations relatives au système d'exploitation et au navigateur de l'utilisateur, ainsi qu'un numéro d'identification unique pour chaque compte d'utilisateur. Ils permettent d'identifier l'utilisateur plus précisément que l'adresse IP. Par exemple, si l'ordinateur est partagé par plusieurs utilisateurs disposant de comptes distincts, chaque utilisateur a son propre «cookie» qui l'identifie de manière unique en tant qu'utilisateur de l'ordinateur. Lorsque l'ordinateur possède une adresse IP dynamique et variable, et que les «cookies» ne sont pas effacés à la fin de la session, ce genre de «cookies» permettent de retrouver l'utilisateur d'une adresse IP à l'autre. Ils peuvent également servir à recouper des recherches émanant d'ordinateurs nomades, par exemple les ordinateurs portables, puisqu'un utilisateur aura le même «cookie» à différents endroits. Enfin, si plusieurs ordinateurs partagent une connexion à Internet (p.ex. derrière un boîtier multiservice (*box*) ou un routeur de traduction d'adresse réseau), le «cookie» permet d'identifier chaque utilisateur sur les différents ordinateurs.

Les moteurs de recherche utilisent les «cookies» (généralement des «cookies» persistants) pour améliorer la qualité de leur service en mémorisant les préférences des utilisateurs et en cernant leurs habitudes, par exemple la manière dont ils effectuent leurs recherches. La plupart des navigateurs sont, au départ, configurés pour accepter les «cookies», mais il est possible de reconfigurer le navigateur pour qu'il les refuse tous, pour qu'il n'accepte que les «cookies»

36 Un des moyens employés par le groupe de travail «Article 29» a consisté à préparer un questionnaire relatif aux politiques de confidentialité. Le questionnaire a été envoyé à plusieurs moteurs de recherché dans les États membres ainsi qu'à plusieurs moteurs basés aux États-Unis. Le présent avis se fonde en partie sur l'analyse des réponses au questionnaire, qui figure à l'annexe 2 du présent avis.

37 Un nombre croissant de fournisseurs de services internet attribuent des adresses IP fixes aux utilisateurs.

de session, ou pour qu'il indique quand un «cookie» est envoyé. Il est cependant possible que les fonctions et certains services ne fonctionnent pas correctement si les «cookies» sont désactivés et certaines fonctions avancées impliquant la gestion de «cookies» ne sont pas toujours suffisamment faciles à configurer.

«Cookies» flash

Certaines sociétés de moteurs de recherche installent des «cookies» flash sur l'ordinateur de l'utilisateur. À l'heure actuelle, il n'est pas facile de les supprimer, en utilisant par exemple les outils de suppression installés par défaut sur le navigateur Internet. Les «cookies» flash sont utilisés, entre autres, en renfort des «cookies» normaux qui, eux, peuvent facilement être effacés par les utilisateurs, ou pour stocker des informations détaillées sur les recherches effectuées par ces derniers (par ex. toutes les requêtes Internet envoyées à un moteur de recherche).

4. Cadre juridique

4.1. Responsables du traitement des données d'utilisateur

4.1.1. Le droit fondamental – le respect de la vie privée

La collecte et le stockage à grande échelle des historiques de recherche des particuliers, sous une forme directement ou indirectement identifiable, relèvent de la protection prévue à l'article 8 de la Charte européenne des Droits fondamentaux.

L'historique de recherche d'une personne contient une indication des centres d'intérêts, des relations et des intentions de cette personne. Ces données sont susceptibles d'être ensuite utilisées à des fins commerciales, ainsi qu'en réponse à des requêtes, opérations de recherche aléatoire et/ou exploration de données par les autorités répressives ou encore les services de sécurité nationaux.

Selon le considérant 2 de la directive 95/46/CE, «les systèmes de traitement de données sont au service de l'homme; [qu']ils doivent, quelle que soit la nationalité ou la résidence des personnes physiques, respecter les libertés et droits fondamentaux de ces personnes, notamment la vie privée, et contribuer au progrès économique et social, au développement des échanges ainsi qu'au bien-être des individus».

Les moteurs de recherche jouent un rôle primordial en étant le premier point de contact pour accéder librement à l'information sur Internet. Ce libre accès à l'information est essentiel pour se faire une opinion personnelle dans notre démocratie. L'article 11 de la Charte européenne des Droits fondamentaux revêt dès lors une importance particulière car il prévoit que *l'information doit être accessible sans aucune surveillance de la part des autorités publiques, dans le cadre de la liberté d'expression et d'information.*

4.1.2. Applicabilité de la directive 95/46/CE (directive sur la protection des données)

Dans de précédents documents de travail, le groupe de travail «Article 29» a clarifié les règles de protection des données induites par l'enregistrement des adresses IP et l'utilisation de «cookies» dans le cadre des services de la société de l'information. Le présent avis donnera davantage d'indications sur l'application des définitions de «données à caractère personnel» et de «responsable du traitement» par les fournisseurs de moteurs de recherche. Les services de moteur de recherche peuvent être fournis sur Internet à partir de l'UE/EEE, à partir d'un lieu situé en dehors du territoire des États membres de l'UE/EEE, ou encore à partir de plusieurs endroits au sein de l'UE/EEE et à l'étranger. Les dispositions de l'article 4 seront dès lors également abordées puisque cet article porte sur l'applicabilité des droits nationaux en matière de protection des données.

Données à caractère personnel: adresses IP et «cookies»

Dans son avis (WP 136) sur le concept de données à caractère personnel, le groupe de travail a clarifié la définition de ces dernières[38]. L'historique des recherches d'une personne constitue des données à caractère personnel si la personne concernée est identifiable. Or, bien que dans la plupart des cas, les

38 WP 136, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_fr.pdf

adresses IP ne soient pas directement identifiables par les moteurs de recherche, un tiers peut parvenir à identifier la personne en question. Les fournisseurs d'accès à Internet disposent en effet des données relatives à l'adresse IP. Les autorités répressives et les services nationaux de sécurité peuvent obtenir l'accès à ces données et, dans certains États membres, des personnes privées ont également obtenu cet accès dans le cadre de procédures judiciaires civiles. Ainsi, dans la plupart des cas – y compris dans ceux impliquant une adresse IP dynamique – les données nécessaires existent pour identifier le ou les utilisateur(s) de l'adresse IP.

Dans son avis WP 136, le groupe de travail indiquait que «*… à moins que les fournisseurs d'accès Internet soient en mesure de déterminer avec une certitude absolue que les données correspondent à des utilisateurs non identifiables, par mesure de sécurité, ils devront traiter toute les informations IP comme des données à caractère personnel».* Ces considérations s'appliquent également aux opérateurs de moteurs de recherche.

<u>«Cookies»</u>

Lorsqu'un «cookie» contient un identifiant d'utilisateur unique, celui-ci est clairement une donnée à caractère personnel. L'utilisation de «cookies» persistants ou de dispositifs similaires comportant un identifiant d'utilisateur unique permet de pister les utilisateurs d'un ordinateur donné, même en cas d'utilisation d'adresses IP dynamiques[39]. Les données relatives au comportement qui sont générées par le recours à ces dispositifs permettent d'affiner encore les caractéristiques personnelles de la personne concernée. Cela va dans le sens de la logique qui sous-tend le modèle d'entreprise dominant.

<u>Responsable du traitement</u>

Un fournisseur de moteur de recherche qui traite des données d'utilisateur comprenant des adresses IP et/ou des «cookies» persistants contenant un identifiant unique relève de la définition du responsable du traitement, puisqu'il détermine effectivement les finalités et les moyens du traitement. La nature multinationale des grands fournisseurs de moteurs de recherche - dont le siège se trouve souvent en dehors de l'EEE, qui proposent leurs services dans le monde entier, et qui font intervenir différents domaines et, éventuellement, des tiers dans le traitement des données à caractère personnel - a donné lieu à un débat autour de la question de savoir qui devrait être considéré comme le responsable du traitement des données à caractère personnel.

Le groupe de travail tient à souligner la distinction entre les définitions du droit de la protection des données dans l'EEE et la question de savoir si ce droit s'applique dans une situation donnée. Un fournisseur de moteur de recherche qui traite des données à caractère personnel, telles que des journaux contenant des historiques de recherche identifiables personnellement, est considéré comme responsable du traitement de ces données à caractère personnel, indépendamment de la question de la compétence.

<u>L'article 4 de la directive sur la protection des données/ le droit applicable</u>

L'article 4 de la directive sur la protection des données aborde la question du droit applicable. Le groupe de travail a donné des indications complémentaires concernant les dispositions de cet article dans son **«Document de travail sur l'application internationale du droit de l'UE en matière de protection des données au traitement des données à caractère personnel sur Internet par des sites web établis en dehors de l'UE[40]»**. L'article 4 a deux raisons d'être. La première est d'éviter qu'il y ait des lacunes dans le système communautaire de protection des données en place et que celui-ci ne soit contourné. La seconde est d'empêcher que la même opération de traitement puisse être régie par le droit de plusieurs États membres de l'UE. En raison de la nature transnationale des flux de données produits par

39 WP 136: «À cet égard, il convient de relever que si l'identification par le nom constitue, dans la pratique, le moyen le plus répandu, un nom n'est pas toujours nécessaire pour identifier une personne, notamment lorsque d'autres «identifiants» sont utilisés pour distinguer quelqu'un. En effet, les fichiers informatiques enregistrant les données à caractère personnel attribuent habituellement un identifiant spécifique aux personnes enregistrées pour éviter toute confusion entre deux personnes se trouvant dans un même fichier.»

40 WP 56, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_fr.pdf

les moteurs de recherche, le groupe de travail s'est tout particulièrement penché sur ces deux complications.

Dans le cas d'un fournisseur de moteur de recherche établi dans un ou plusieurs États membres à partir duquel ou desquels il fournit l'ensemble de ses services, il ne fait aucun doute que le traitement des données à caractère personnel relève de la directive sur la protection des données. Il importe de noter que, dans ce cas, les règles de protection des données ne sont pas limitées aux personnes concernées se trouvant sur le territoire ou possédant la nationalité d'un des États membres.

Lorsque le fournisseur de moteur de recherche est un responsable du traitement qui n'est pas établi dans l'EEE, il existe deux cas dans lesquels le droit communautaire de la protection des données s'applique malgré tout. Premièrement, lorsque le fournisseur de moteur de recherche possède un établissement dans un État membre, tel que prévu à l'article 4, paragraphe 1, point a). Deuxièmement, lorsque le moteur de recherche recourt à des moyens situés sur le territoire d'un État membre, tel que prévu à l'article 4, paragraphe 1, point c). Dans ce second cas, le moteur de recherche, en vertu de l'article 4, paragraphe 2, doit désigner un représentant sur le territoire dudit État membre.

Établissement sur le territoire d'un État membre (EEE)

L'article 4, paragraphe 1, point a), mentionne que le droit de la protection des données d'un État membre doit être appliqué lorsque certaines opérations de traitement de données à caractère personnel sont effectuées par le responsable du traitement «dans le cadre des activités d'un établissement» de ce responsable situé sur le territoire d'un État membre. Une opération de traitement spécifique doit être prise comme point de départ. Lorsqu'il s'agit d'un moteur de recherche dont le siège est situé en dehors de l'EEE, il faut déterminer si des établissements situés sur le territoire d'un État membre participent au traitement des données d'utilisateur.

Comme le groupe de travail l'a déjà souligné dans son document de travail précédent[41], l'existence d'un «établissement» implique l'exercice effectif et réel d'une activité au titre d'accords stables et doit être établie conformément à la jurisprudence de la Cour de justice des Communautés européennes. La forme juridique de l'établissement - un bureau local, une filiale possédant la personnalité juridique ou une agence tierce - n'est pas déterminante.

Cependant, l'opération de traitement doit en outre être effectuée «dans le cadre des activités» de l'établissement. Cela signifie que l'établissement doit également jouer un rôle significatif dans l'opération de traitement en question. C'est manifestement le cas si:

- un établissement est chargé des relations avec les utilisateurs du moteur de recherche dans une juridiction donnée;
- un fournisseur de moteur de recherche établit un bureau dans un État membre (EEE) qui joue un rôle dans la vente de publicités ciblées aux habitants de cet État;
- l'établissement d'un fournisseur de moteur de recherche se conforme aux décisions des tribunaux et/ou répond aux demandes d'application de la loi des autorités compétentes d'un État membre à l'égard des données d'utilisateur.

Il incombe au fournisseur de moteur de recherche de préciser le degré de participation des établissements situés sur le territoire d'un État membre au traitement des données à caractère personnel. Si un établissement national participe au traitement des données d'utilisateur, l'article 4, paragraphe 1, point a), de la directive sur la protection des données s'applique.

Les fournisseurs de moteurs de recherche qui ne sont pas établis dans l'EEE doivent informer leurs utilisateurs des conditions dans lesquelles ils doivent respecter la directive sur la protection des données, en raison soit de la présence d'établissements soit du recours à des moyens situés sur le territoire d'un État membre.

41 WP 56, page 8, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_fr.pdf

Recours à des moyens

Les moteurs de recherche qui recourent à des moyens situés sur le territoire d'un État membre (EEE) pour traiter des données à caractère personnel sont également soumis au droit de la protection des données de cet État, qui s'appliquera encore lorsque *le responsable du traitement […] recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire dudit État membre, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la Communauté.*

En ce qui concerne la prestation de services de moteur de recherche à partir d'un lieu situé en dehors de l'UE, des centres de données situés sur le territoire d'un État membre peuvent servir au stockage et au traitement à distance de données à caractère personnel. D'autres types de moyens pourraient être l'utilisation d'ordinateurs personnels, de terminaux et de serveurs. L'utilisation de «cookies» et de logiciels similaires par un prestataire de services en ligne peut également être considérée comme un recours à des moyens situés sur le territoire d'un État membre, entraînant ainsi l'application de son droit de la protection des données. La question avait été abordée dans le document de travail susmentionné (WP56), qui mentionne que «*le PC de l'utilisateur peut être considéré comme un «equipment» au sens de l'article 4, paragraphe 1, point c de la directive 95/46/CE. Il est établi sur le territoire d'un État membre. Le responsable a décidé d'utiliser cet équipement à des fins de traitement de données à caractère personnel et, comme expliqué dans les paragraphes précédents, plusieurs opérations techniques ont lieu sans que le sujet des données (sic) ait un pouvoir de contrôle. Le responsable du traitement dispose des moyens de l'utilisateur et ces moyens ne sont pas uniquement utilisés à des fins de transit sur le territoire de la Communauté*».

Conclusion

L'effet combiné des points a) et b) de l'article, paragraphe 1, de la directive sur la protection des données fait que leurs dispositions s'appliquent à de nombreux cas de traitement de données à caractère personnel par les fournisseurs de moteurs de recherche, même si leur siège se trouve en dehors de l'EEE.

Pour déterminer le droit national applicable dans un cas donné, il convient d'analyser en détail les données factuelles de l'affaire. Le groupe de travail attend des fournisseurs de moteurs de recherche qu'ils contribuent à cette analyse donnant suffisamment de précisions sur leur rôle et leurs activités au sein de l'EEE.

Dans le cas de fournisseurs de moteurs de recherche multinationaux :

- un État membre dans lequel un fournisseur de moteur de recherche est établi doit appliquer son droit national de la protection des données au traitement, conformément à l'article 4, paragraphe 1, point a) ;
- si le fournisseur de moteur de recherche n'est établi dans aucun État membre, l'État membre doit appliquer au traitement son droit national en matière de protection des données, conformément à l'article 4, paragraphe 1, point c), si la société recourt à des moyens, automatisés ou non, sur le territoire dudit État membre[42], à des fins de traitement de données à caractère personnel (par exemple, l'utilisation d'un «cookie»).

Dans certains cas, un fournisseur de moteur de recherche multinational devra respecter plusieurs législations sur la protection des données, en raison des règles relatives au droit applicable et de la nature transnationale de ses opérations de traitement de données à caractère personnel :

42 Le groupe de travail tient compte des critères suivants pour déterminer l'applicabilité de l'article 4, paragraphe 1, point c) au sujet de l'utilisation de «cookies». Le premier est le cas où un fournisseur de moteur de recherche possède un établissement dans un État membre auquel l'article 4, paragraphe 1, point a) ne s'applique pas parce que cet établissement n'a pas d'incidence significative sur le traitement des données (comme, par exemple, un représentant de la presse). D'autres critères sont le développement et/ou la conception de services de moteur de recherche propres au pays, le fait que le prestataire de services en ligne sache effectivement qu'il traite avec des utilisateurs qui se trouvent dans ce pays, ainsi que le fait d'avoir l'avantage de posséder une part stable du marché des utilisateurs dans un État membre donné.

- un État membre doit appliquer son droit national à un moteur de recherche établi en dehors de l'EEE s'il recourt à des moyens ;
- un État membre ne peut appliquer son droit national à un moteur de recherche établi dans l'EEE, dans un autre ressort, même si le moteur de recherche recourt à des moyens. Dans ce cas, le droit national de l'État membre dans lequel le moteur de recherche est établi s'applique.

4.1.3 Applicabilité de la directive 2002/58/CE (directive sur la vie privée et les communications électroniques) et de la directive 2006/24/CE (directive sur la conservation des données)

En général, les services de moteur de recherche au sens strict ne relèvent pas du nouveau cadre réglementaire défini pour les communications électroniques, dans lequel s'inscrit la directive sur la vie privée et les communications électroniques. L'article 2, point c, de la directive cadre (2002/21/CE), qui contient certaines des définitions générales relatives au cadre réglementaire, exclut explicitement les services qui consistent à fournir des contenus ou à exercer une responsabilité éditoriale sur ces derniers:

«Service de communications électroniques»: le service normalement fourni contre rémunération consiste entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques, y compris les services de télécommunications et les services de transmission sur les réseaux utilisés pour la radiodiffusion, mais qui exclut les services consistant à fournir des contenus à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus; il ne comprend pas les services de la société de l'information tels que définis à l'article 1er de la directive 98/34/CE qui ne consistent pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques.

Dès lors, les moteurs de recherche ne relèvent pas de la définition de services de communications électroniques.

Un fournisseur de moteur de recherche peut cependant proposer un service supplémentaire qui lui relève de la définition des services de communications électroniques, comme un service de courrier électronique accessible publiquement, qui serait soumis à la directive 2002/58/CE sur la vie privée et les communications électroniques et à la directive 2006/24/CE sur la conservation des données.

L'article 5, paragraphe 2, de la directive sur la conservation des données prévoit qu'«aucune donnée révélant le contenu de la communication ne peut être conservée au titre de la présente directive». Les requêtes de recherche elles-mêmes seraient considérées comme des contenus plutôt que comme des données de trafic, et la directive ne justifierait donc pas leur conservation.

En conséquence, la référence à la directive sur la conservation des données en relation avec le stockage de journaux de serveurs générés par la fourniture d'un service de moteur de recherche n'est justifiée dans aucun cas.

Articles 5, paragraphe 3, et article 13 de la directive sur la vie privée et les communications électroniques

Certaines dispositions de la directive sur la vie privée et les communications électroniques, telles que l'article 5, paragraphe 3 («cookies» et logiciels espions), et l'article 13 (communications non sollicitées) sont des dispositions générales applicables non seulement aux services de communications électroniques, mais aussi à tout autre service lorsque ces techniques sont utilisées.

L'article 5, paragraphe 3, de la directive sur la vie privée et les communications électroniques, qui doit être lu conjointement avec son, considérant 25 de la même directive, porte sur le stockage d'informations dans l'équipement terminal des utilisateurs. Les «cookies» persistants avec des identifiants uniques permettent de suivre à la trace un ordinateur donné et d'établir un profil de l'usage qui en est fait, même en cas d'utilisation d'adresses IP dynamiques. L'article 5, paragraphe 3, et le considérant 25 de la directive sur la vie privée et les communications électroniques, mentionnent expressément que le stockage de telles informations dans l'équipement terminal des utilisateurs, c'est-à-dire les «cookies» et dispositifs similaires (en bref, les «cookies»), doit se faire conformément aux dispositions de la directive sur la

protection des données. L'article 5, paragraphe 3, de la directive sur la vie privée et les communications électroniques clarifie ainsi les obligations relatives à l'utilisation d'un «cookie» par un service de la société de l'information, qui découlent de la directive sur la protection des données.

4.2 Fournisseurs de contenus

Les moteurs de recherche traitent des informations, y compris des informations personnelles, en explorant, en analysant et en indexant l'Internet et d'autres sources qu'ils rendent explorables, et ainsi aisément accessibles. Certains services de moteurs de recherche republient également les données dans ce que l'on appelle une «mémoire cache».

4.2.1. Liberté d'expression et droit à la vie privée

Le groupe de travail est conscient du rôle particulier que jouent les moteurs de recherche dans l'environnement de l'information en ligne. Il faut parvenir à un équilibre, dans le droit communautaire en matière de protection des données et les droits des divers États membres, entre la protection du droit à la vie privée et la protection des données à caractère personnel d'une part, et la libre circulation de l'information et le droit fondamental à la liberté d'expression, d'autre part.

L'article 9 de la directive sur la protection des données vise à garantir que cet équilibre soit trouvé dans la législation des États membres en ce qui concerne les médias. En outre, la Cour de justice des CE a indiqué clairement que toute restriction de liberté d'expression qui pourrait découler de l'application des principes de protection des données doit être conforme à la législation et au principe de proportionnalité[43].

4.2.2 Directive sur la protection des données

La directive sur la protection des données (95/46/CE) ne contient pas de référence particulière au traitement des données à caractère personnel dans le cadre des services de la société de l'information fournis à titre d'intermédiaire de l'extraction de données. Le critère fixé par cette directive qui est déterminant pour l'applicabilité des règles de protection des données est la définition du responsable du traitement, notamment si une personne donnée «seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel». La question de savoir si un intermédiaire doit être considéré lui-même, ou conjointement avec d'autres, comme un responsable («*controller*») du traitement de données à caractère personnel est distincte de la question de la responsabilité de ce traitement[44].

Le principe de proportionnalité veut que, lorsqu'un fournisseur de moteur de recherche agit exclusivement en tant qu'intermédiaire, il ne soit pas considéré comme le principal responsable du traitement des données à caractère personnel effectué. Dans ce cas, les responsables principaux sont les fournisseurs d'informations[45]. Le contrôle formel, juridique et pratique exercé par le MP sur les données à caractère personnel en jeu se limite généralement à la possibilité de retirer des données de ses serveurs. En ce qui concerne le retrait de données à caractère personnel de leur index et de leurs résultats de recherche, les moteurs de recherche ont un contrôle suffisant pour être considérés comme des responsables du traitement (seuls ou conjointement avec d'autres) dans ces cas, mais l'existence réelle d'une obligation de retirer ou de bloquer des données à caractère personnel existe peut dépendre du droit

43 La Cour de justice a donné plus de précisions concernant la proportionnalité des effets des règles de protection des données, en d'autres termes, concernant la liberté d'expression, dans son arrêt rendu dans l'affaire Lindqvist contre Suède, points 88 à 90.

44 Dans certains États membres, il existe des exceptions horizontales particulières («refuges») concernant la responsabilité des moteurs de recherche («outils de localisation d'informations»). La directive sur le commerce électronique (2000/31/CE) ne contient pas de refuges pour les moteurs de recherche mais, dans certains États membres, des règles de ce type ont été appliquées. Voir le «Premier rapport sur l'application de la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»), 21.11.2003, COM/2003/0702 final.», p. 13.

45 À vrai dire, les utilisateurs du moteur de recherche pourraient également être considérés comme des responsables du traitement, mais leur rôle ne relèvera pas de la directive puisqu'il s'agit d'«activités exclusivement personnelles» (voir article 3, paragraphe 2, second tiret).

de la responsabilité civile délictuelle et des règles de responsabilité de l'État membre concerné[46].

Les propriétaires de sites Internet peuvent choisir *a priori* de n'apparaître ni dans le moteur de recherche ni dans la mémoire cache, en utilisant le fichier robots.txt ou les balises Noindex/NoArchive[47]. Il est essentiel que les fournisseurs de moteurs de recherche respectent le choix des éditeurs de sites Internet de ne pas participer à leurs services. Ce choix peut être exprimé avant la première exploration du site Internet, ou alors qu'il a déjà été exploré. Dans ce cas, les mises à jour du moteur de recherche doivent être effectuées le plus rapidement possible.

Les moteurs de recherche ne se bornent pas toujours exclusivement à un rôle d'intermédiaire. Par exemple, certains d'entre eux stockent des parties entières de contenus sur Internet - y compris les données à caractère personnel figurant dans ces contenus - sur leurs serveurs. En outre, on ne sait pas jusqu'à quel point les moteurs de recherche ciblent activement les informations personnellement identifiables dans les contenus qu'ils traitent. L'exploration, l'analyse et l'indexation peuvent en effet se faire automatiquement, sans révéler la présence de telles informations personnellement identifiables. La forme de certains types d'informations personnellement identifiables, comme les numéros de sécurité sociale, les numéros de cartes de crédit, les numéros de téléphone et les adresses électroniques, rend ces données aisément détectables. Mais il existe aussi des technologies plus sophistiquées, qui sont de plus en plus employées par les fournisseurs de moteurs de recherche, comme la reconnaissance faciale dans le cadre du traitement d'images et de la recherche d'images.

Les fournisseurs de moteurs de recherche peuvent ainsi effectuer des opérations à valeur ajoutée, liées à des caractéristiques ou à des types de données à caractère personnel, sur les informations qu'ils traitent. Dans ce cas, ils sont entièrement responsables au regard de la législation en matière de protection des données, des contenus affichés dans la liste des résultats à la suite du traitement des données à caractère personnel. Un moteur de recherche qui vend de la publicité induite par des données à caractère personnel, comme le nom d'une personne, est soumis à la même responsabilité.

La fonction de stockage dans la mémoire cache

La fonction de stockage dans la mémoire cache est une autre façon dont un fournisseur de moteur de recherche peut aller au-delà de son rôle exclusif d'intermédiaire. Le délai de conservation des contenus dans une mémoire cache devrait être limité au laps de temps nécessaire pour régler le problème d'inaccessibilité temporaire du site Internet lui-même.

Tout stockage dans la mémoire cache de données à caractère personnel figurant sur des sites Internet indexés pendant une durée dépassant celle nécessaire à la disponibilité technique, devrait être considéré comme une republication indépendante. Le groupe de travail tient les fournisseurs de ces fonctions de stockage pour responsables du respect de la législation sur la protection des données, dans leur rôle de responsables du traitement des données à caractère personnel contenues dans les publications stockées dans la mémoire cache. Dans les cas où la publication originale a été modifiée, par exemple pour supprimer des données à caractère personnel exactes, le responsable du traitement de la mémoire cache doit immédiatement répondre à toute demande de mise à jour de la copie stockée dans la mémoire cache, ou alors bloquer temporairement cette copie jusqu'à ce que le site Internet soit à nouveau visité par le moteur de recherche.

46 Dans certains États membres de l'UE, les autorités de protection des données ont spécifiquement réglementé l'obligation des fournisseurs de moteurs de recherche de retirer des données de contenu de l'index de recherche, sur la base du droit d'opposition consacré à l'article 14 de la directive sur la protection des données (95/46/CE), et de la directive sur le commerce électronique (2000/31/CE). En vertu de ces législations nationales, les moteurs de recherches sont obligés de suivre une politique de notification et de retrait similaire à celle appliquée par les hébergeurs en vue de prévenir toute responsabilité.

47 Cela peut être plus qu'une solution facultative. Les éditeurs de données à caractère personnel doivent examiner si leur base juridique autorisant la publication inclut l'indexation de ces informations par les moteurs de recherche et créer les garanties correspondantes nécessaires, notamment l'utilisation du fichier robots.txt et/ou des balises Noindex/NoArchive.

5. La légalité du traitement

Conformément à l'article 6 de la directive sur la protection des données, les données à caractère personnel doivent être traitées loyalement et licitement ; elles doivent être collectées à des fins déterminées, explicites et légitimes, et ne pas être traitées de manière incompatible avec les finalités pour lesquelles elles avaient, à l'origine, été collectées. En outre, les données traitées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et/ou pour lesquelles elles sont traitées ultérieurement. Pour que le traitement de données à caractère personnel soit licite, il doit répondre à un ou plusieurs des six motifs de traitement légitime définis à l'article 7 de ladite directive.

5.1. Finalités/motifs mentionnés par les fournisseurs de moteurs de recherche

Les fournisseurs de moteurs de recherche ont généralement mentionné les finalités et raisons suivantes pour justifier l'utilisation et le stockage de données à caractère personnel dans le cadre de leur rôle de responsables du traitement de données d'utilisateur.

Amélioration du service

De nombreux responsables du traitement utilisent des journaux de serveurs pour améliorer leurs prestations et la qualité de leurs services de recherche. L'analyse de ces journaux est, selon eux, un moyen important d'améliorer la qualité des recherches, des résultats et des publicités, et de développer des services nouveaux, même non prévus au départ.

Sécurisation du système

Les journaux de serveurs contribueraient à garantir la sécurité des services de moteur de recherche. Certains fournisseurs de moteurs de recherche ont déclaré que la conservation des journaux pouvait aider à protéger le système des attaques contre la sécurité, et qu'ils avaient besoin d'un échantillon historique suffisant de données provenant de journaux de serveurs pour détecter des constantes et d'analyser les menaces pour la sécurité.

Prévention des fraudes

Les journaux de serveurs contribueraient à protéger les systèmes et les utilisateurs des moteurs de recherche des fraudes et des abus. De nombreux fournisseurs de moteurs de recherche utilisent un mécanisme de «paiement par clic» pour les publicités qu'ils affichent. L'inconvénient, c'est qu'une société peut se voir facturer des clics indûment si un agresseur utilise un logiciel automatique pour cliquer systématiquement sur les publicités. Les fournisseurs de moteurs de recherche veillent donc à ce que ce type de comportement soit détecté et éradiqué.

Les exigences comptables sont citées parmi les finalités pour des services tels que les clics sur des liens sponsorisés, lorsqu'il existe une obligation contractuelle et comptable de conserver des données, au moins jusqu'à l'acquittement des factures et jusqu'à l'expiration du délai d'introduction d'un recours.

Publicité personnalisée

Les fournisseurs de moteurs de recherche s'efforcent de personnaliser la publicité afin d'accroître leurs recettes. La pratique actuelle consiste à tenir compte de l'historique des requêtes, de la catégorisation de l'utilisateur et de critères géographiques. Dès lors, en fonction du comportement de l'utilisateur et de son adresse IP, une publicité personnalisée peut être affichée.

Des statistiques sont établies par certains moteurs de recherche en vue de déterminer quelles catégories d'utilisateurs accèdent à quelles informations en ligne et à quel moment de l'année. Ces données peuvent servir à améliorer le service, à cibler les publicités, ainsi qu'à des fins commerciales, en vue de déterminer le coût à facturer à une société souhaitant faire la publicité de ses produits.

Répression des infractions

Certains fournisseurs affirment que les journaux sont des outils précieux pour les services répressifs, pour enquêter sur les infractions graves et les poursuivre, par exemple l'exploitation des enfants.

5.2. Analyse des finalités et raisons par le groupe de travail

En général, les fournisseurs de moteurs de recherche ne donnent pas une liste complète des finalités déterminées, explicites et légitimes pour lesquelles ils traitent des données à caractère personnel. D'une part, la définition de certaines finalités, telles que «l'amélioration du service» ou «l'offre de publicité personnalisée» est trop vaste pour offrir un cadre permettant de juger de la légitimité de la finalité. D'autre part, de nombreux fournisseurs de moteurs de recherche mentionnant plusieurs finalités différentes pour le traitement, on ne sait pas exactement dans quelle mesure les données sont retraitées pour une autre finalité incompatible avec celle pour laquelle elles avaient été collectées à l'origine.

La collecte et le traitement de données à caractère personnel peuvent être fondés sur une ou plusieurs raisons légitimes. Il en existe trois que les fournisseurs de moteurs de recherche peuvent invoquer à diverses fins.

- Consentement - Article 7, point a) de la directive sur la protection des données

La plupart des fournisseurs de moteurs de recherche proposent un accès non enregistré *et* un accès enregistré à leur service. Dans le second cas, par exemple lorsqu'un utilisateur a créé un compte d'utilisateur spécifique, le consentement[48] peut servir de raison légitime de traiter certaines catégories bien déterminées de données à caractère personnel à des fins légitimes bien déterminées, dont la conservation de données pour un laps de temps limité. Le consentement ne peut être obtenu de force auprès des utilisateurs anonymes du service, ni d'après les données à caractère personnel des utilisateurs qui n'ont pas choisi de signaler leur identité. Ces données ne peuvent pas être traitées ni stockées à d'autres fins que celle d'agir sur une requête spécifique avec une liste de résultats de recherche.

- Nécessaire à l'exécution d'un contrat - Article 7 (b) de la directive sur la protection des données

Le traitement peut également être nécessaire à l'exécution d'un contrat auquel la personne concernée est partie, ou à l'exécution de mesures précontractuelles prise à la demande de celle-ci. Les fournisseurs de moteurs de recherche peuvent utiliser cette base juridique pour collecter les données à caractère personnel qu'un utilisateur fournit spontanément lors de son inscription à un service donné, comme un compte d'utilisateur, par exemple. Ils peuvent également utiliser cette base, telle que le consentement, pour traiter certaines catégories bien déterminées de données à caractère personnel d'utilisateurs authentifiés à des fins légitimes bien déterminées.

De nombreuses sociétés Internet soutiennent qu'un utilisateur entre *de facto* dans une relation contractuelle lorsqu'il utilise les services proposés sur leur site, un formulaire de recherche par exemple. Cependant, ce postulat général ne répond pas à la limitation stricte de la nécessité, ainsi que la directive le requiert[49].

- Nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement - Article 7 (f) de la directive sur la protection des données

En vertu de l'article 7(f) de la directive, le traitement pourrait être nécessaire à la réalisation des intérêts légitimes poursuivis par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er paragraphe 1.

Amélioration du service

Plusieurs fournisseurs de moteurs de recherche stockent le contenu des requêtes des utilisateurs dans leurs journaux de serveurs. Ces informations constituent un

48 Article 2 (h) de la directive sur la protection des données: «consentement de la personne concernée: toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement».

49 Article 7 (b) de la directive: «… nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci».

outil important pour les fournisseurs de moteurs de recherche, qui leur permet d'améliorer leurs services en analysant le type de requêtes effectuées par les utilisateurs, la manière dont ils choisissent d'affiner ces requêtes et les résultats de recherche qu'ils choisissent de suivre. Le groupe de travail «Article 29» est toutefois d'avis qu'il n'est pas nécessaire que les requêtes de recherche soient attribuables à des individus identifiés pour qu'elles puissent être utilisées en vue d'améliorer les services de recherche.

Afin de mettre en rapport les diverses actions d'un utilisateur (et de découvrir ainsi si les suggestions du moteur de recherche sont utiles), il faut simplement pouvoir différencier les actions d'un utilisateur lors d'une requête de recherche de celles d'un autre utilisateur.

Il n'est pas nécessaire de pouvoir identifier ces utilisateurs. Par exemple, un moteur de recherche peut vouloir savoir que l'utilisateur X a lancé une recherche sur le terme «Woodhouse» et a ensuite également choisi de cliquer sur les résultats relatifs à la variante orthographique proposée «Wodehouse», mais n'a pas besoin de savoir qui est l'utilisateur X. L'amélioration des services ne peut dès lors pas être considérée comme une raison légitime de stocker des données qui n'ont pas été rendues anonymes.

Sécurité du système

Les moteurs de recherche peuvent juger que la nécessité de maintenir la sécurité de leur système est un intérêt légitime et une raison adéquate pour procéder au traitement de données à caractère personnel. Cependant, le stockage de toute donnée à caractère personnel pour des raisons de sécurité doit être soumis à une limitation stricte de sa finalité. Par conséquent, les données stockées pour des raisons de sécurité ne peuvent pas être utilisées pour optimiser un service, par exemple. Les fournisseurs de moteurs de recherche soutiennent que les journaux de serveurs doivent être stockés pendant un délai raisonnable (le nombre de mois diffère d'un moteur de recherche à l'autre) afin de leur permettre de détecter des modèles de comportement d'utilisateurs, et d'ainsi repérer et prévenir les attaques par déni de service et autres menaces pour la sécurité. Tous ces fournisseurs devraient être en mesure de justifier complètement le délai de conservation qu'ils adoptent à cette fin et qui dépendra de la nécessité de traiter ces données.

Prévention de la fraude

Les moteurs de recherche peuvent aussi avoir un intérêt légitime à détecter et prévenir les fraudes, comme la «fraude au clic», mais, comme pour la finalité de maintien de la sécurité, la quantité de données à caractère personnel stockées et traitées, ainsi que la durée pendant laquelle ces données sont conservées à cette fin, dépendront de la nécessité réelle ou non de ces données pour détecter et prévenir la fraude.

Comptabilité

Les exigences comptables ne peuvent justifier l'enregistrement systématique des données de moteurs de recherche ordinaires dans lesquelles l'utilisateur n'a pas cliqué sur un lien sponsorisé. Le groupe de travail - sur la base des informations reçues des fournisseurs de moteurs de recherche en réponse au questionnaire - doute sérieusement que les données à caractère personnel des utilisateurs de moteurs de recherche soient vraiment essentielles à la comptabilité. Pour obtenir une évaluation concluante, il faudrait procéder à des études plus approfondies. Quoi qu'il en soit, le groupe de travail demande aux fournisseurs de moteurs de recherche de mettre au point des mécanismes comptables qui permettent de mieux protéger la vie privée, par exemple en utilisant des données rendues anonymes.

Publicité personnalisée

Les fournisseurs de moteurs de recherche qui souhaitent proposer de la publicité personnalisée afin d'accroître leurs recettes peuvent trouver une raison au traitement légitime de certaines données à caractère personnel à l'article 7 (a) de la directive (consentement) ou à l'article 7 (b) de la directive (exécution d'un contrat), mais il est difficile de trouver une raison légitime à cette pratique pour les utilisateurs qui ne se sont pas spécifiquement inscrits en prenant connaissance de certaines informations sur la finalité du traitement. Le groupe de travail préfère clairement les données rendues anonymes.

Application de la loi et requêtes judiciaires

Les autorités chargées de faire respecter la loi peuvent parfois avoir besoin de données d'utilisateur des moteurs de recherche afin de détecter ou de prévenir des délits. Des parties privées peuvent également parfois tenter d'obtenir une ordonnance d'un tribunal demandant à un fournisseur de moteur de recherche de lui remettre des données d'utilisateur. Lorsque ces requêtes suivent des procédures judiciaires valables qui aboutissent à des ordonnances judiciaires valables, les fournisseurs de moteurs de recherche doivent bien sûr obtempérer et fournir les informations nécessaires. Cela ne doit toutefois pas être pris pour une obligation juridique ou pour une justification en vue de stocker ces données à ces fins uniquement.

En outre, de grandes quantités de données à caractère personnel qui se trouvent dans les mains des fournisseurs de moteurs de recherche peuvent encourager les autorités chargées de faire respecter la loi et d'autres à exercer leurs droits plus souvent et plus intensément, ce qui, à terme, peut entraîner une perte de confiance du consommateur.

5.3. Problèmes que l'industrie doit résoudre

Délais de conservation

Si le traitement effectué par le fournisseur de moteur de recherche est soumis au droit national, il doit répondre aux normes en matière de confidentialité et respecter les délais de conservation prévus dans la législation de cet État membre.

Si des données à caractère personnel sont stockées, le délai de conservation ne devra pas être plus long que ce qui est nécessaire aux finalités spécifiques du traitement. Par conséquent, au terme de la session de recherche, les données à caractère personnel pourraient être effacées, et un stockage prolongé doit dès lors être dûment justifié. Cependant, certaines sociétés de moteur de recherche semblent conserver des données indéfiniment, ce qui est interdit. Pour chaque finalité, un délai de conservation limité devrait être défini. En outre, l'ensemble de données à caractère personnel à conserver ne devrait pas être excessif par rapport à chaque finalité.

En pratique, les grands moteurs de recherche conservent des données relatives à leurs utilisateurs dans des formulaires identifiables personnellement pendant plus d'un an (la durée précise varie). Le groupe de travail salue les récentes réductions des délais de conservation des données à caractère personnel opérées par les grands fournisseurs de moteurs de recherche. Cependant, le fait que les sociétés leaders dans le domaine aient pu réduire leurs délais de conservation porte à croire que les délais précédents étaient plus longs que nécessaires.

Au vu des explications initiales données par les fournisseurs de moteurs de recherche au sujet des finalités possibles de la collecte de données à caractère personnel, le groupe de travail ne voit pas de raison d'étendre le délai de conservation au-delà de six mois[50].

La conservation de données à caractère personnel et le délai de conservation correspondant doivent cependant toujours être justifiés (à l'aide d'arguments concrets et pertinents) et réduits au minimum, afin d'accroître la transparence, de garantir un traitement légitime et de garantir la proportionnalité avec la finalité qui justifie cette conservation.

À cet effet, le groupe de travail invite les fournisseurs de moteurs de recherche à mettre en oeuvre le principe de «*privacy by design*» (intégration des principes de protection des données dès la phase de conception), qui contribuera à réduire encore le délai de conservation. En outre, le groupe de travail considère que réduire le délai de conservation renforcerait la confiance des utilisateurs et constituerait dès lors un avantage concurrentiel significatif.

Si les fournisseurs de moteurs de recherche conservent des données à caractère personnel plus de six mois, ils devront démontrer de manière détaillée que cela est strictement nécessaire au service.

Dans tous les cas, les fournisseurs de moteurs de recherche doivent informer les utilisateurs des politiques de conservation applicables pour tous les types de données d'utilisateur qu'ils traitent.

50 La législation nationale peut exiger que les données à caractère personnel soient effacées plus tôt.

Traitement ultérieur à différentes fins

La mesure dans laquelle les données d'utilisateur font l'objet d'une analyse ultérieure, la manière dont elles le font, et si oui ou non des profils d'utilisateur (détaillés) sont créés, dépendent du fournisseur de moteur de recherche. Le groupe de travail est conscient de la possibilité que ce type de traitement ultérieur de données d'utilisateur touche à un domaine essentiel d'innovation de la technologie des moteurs de recherche, et puisse donc avoir beaucoup d'importance pour la concurrence. La divulgation totale de l'utilisation et de l'analyse ultérieures des données d'utilisateur pourrait également entraîner une augmentation de la vulnérabilité des services de moteur de recherche à l'utilisation abusive de leurs services. Ces considérations ne peuvent toutefois pas servir d'excuse au non-respect du droit en vigueur en matière de protection des données dans les États membres. En outre, les fournisseurs de moteurs de recherche ne peuvent pas prétendre que leur but en collectant des données à caractère personnel est de développer de nouveaux services dont la nature est encore indéterminée. La loyauté veut que les personnes concernées aient connaissance de la mesure dans laquelle le moteur de recherche pourrait faire intrusion dans leur vie privée lors de l'obtention de leurs données. Cela ne sera pas possible à moins de définir plus précisément les finalités.

«Cookies»

Les «cookies» persistants qui contiennent un identifiant d'utilisateur unique sont des données à caractère personnel et sont donc soumis à la législation en vigueur en matière de protection des données. La responsabilité de leur traitement ne peut être réduite à la responsabilité qui incombe à l'utilisateur de prendre, ou de ne pas prendre, certaines précautions dans les paramètres de son navigateur. Le fournisseur de moteur de recherche décide si un «cookie» est stocké, quel «cookie» est stocké, et à quelles fins il est utilisé. Enfin, les dates d'expiration des «cookies» fixées par certains fournisseurs de moteurs de recherche semblent excessives. Plusieurs sociétés utilisent par exemple des «cookies» qui expirent après plusieurs années. Lorsqu'un «cookie» est utilisé, une durée de vie appropriée devrait être définie pour celui-ci, qui permettrait d'améliorer la navigation sur Internet et de limiter la durée du «cookie». Vu, en particulier, les paramètres par défaut des navigateurs, il est très important que les utilisateurs soient pleinement informés de l'utilisation et de l'effet des «cookies». Ces informations devraient être mises davantage en évidence et ne pas simplement figurer dans la politique de confidentialité du moteur de recherche, où elles ne sont peut-être pas immédiatement apparentes.

Anonymisation

S'il n'existe aucune raison légitime de traiter les données à caractère personnel, ou de les utiliser au-delà des finalités légitimes bien déterminées, les fournisseurs de moteurs de recherche doivent les effacer. Au lieu de les effacer, les moteurs de recherche peuvent également rendre les données anonymes, mais cette anonymisation doit être totalement irréversible pour que la directive sur la protection des données ne s'applique plus.

Même lorsque l'adresse IP et le «cookie» sont remplacés par un identifiant unique, la corrélation des requêtes de recherche stockées peut permettre d'identifier les individus. C'est la raison pour laquelle, lorsque l'anonymisation est préférée à la suppression des données, les méthodes utilisées devraient être étudiées soigneusement et exécutées jusqu'au bout. Cela peut impliquer la suppression de portions de l'historique de recherche, afin d'éviter la possibilité d'identification indirecte de l'utilisateur qui a effectué les recherches en question.

L'anonymisation des données devrait exclure toute possibilité d'identifier les individus, même en combinant les informations rendues anonymes détenues par la société de moteur de recherche avec les informations détenues par une autre partie concernée (par exemple, un fournisseur de services Internet). À l'heure actuelle, certains fournisseurs de moteurs de recherche tronquent les adresses IPv4 en supprimant l'octet final, conservant ainsi effectivement des informations sur le fournisseur de services Internet, ou le sousréseau

de l'utilisateur, mais sans identifier directement l'individu. L'activité pourrait ainsi provenir de n'importe laquelle des 254 adresses IP. Cela pourrait ne pas toujours être suffisant pour garantir l'anonymat.

Enfin, l'anonymisation ou la suppression de journaux doit également être appliquée rétroactivement et englober tous les journaux de moteur de recherche pertinents du monde.

Corrélations des données entres les services

De nombreux fournisseurs de moteurs de recherche proposent aux utilisateurs l'option de personnaliser l'utilisation qu'ils font de leurs services grâce à un compte personnel. Outre la recherche, ils proposent des services tels que le courrier électronique et/ou d'autres outils de communication comme des services de messagerie ou de discussion en ligne, et des outils conviviaux comme les blogues ou les communautés sociales. Si la gamme de services personnalisés peut varier, une caractéristique commune est le modèle d'entreprise sous-jacent, et le développement continu de nouveaux services personnalisés.

La corrélation du comportement du client entre les différents services personnalisés d'un fournisseur de moteur de recherche et, parfois, entre différentes plateformes[51], est techniquement facilitée par l'utilisation d'un compte personnel central, mais peut également être accomplie par d'autres moyens, grâce à des «cookies» ou à d'autres caractéristiques de différenciation, comme les adresses IP individuelles. Par exemple, lorsqu'un moteur de recherche propose aussi un service de recherche dans l'ordinateur de l'utilisateur («*desktop search*»), le moteur de recherche obtient des informations au sujet des (contenus des) documents qu'un utilisateur crée ou consulte. À l'aide de ces données, les requêtes de recherche peuvent être adaptées à un résultat plus précis.

Le groupe de travail pense que la corrélation des données à caractère personnel entre les services et les plateformes pour les utilisateurs authentifiés ne peut se faire légitimement qu'avec le consentement de l'utilisateur, après que celui-ci a été correctement informé.

L'enregistrement auprès d'un fournisseur de moteur de recherche afin de bénéficier d'un service de recherche plus personnalisé devrait être volontaire. Les fournisseurs de moteurs de recherche ne peuvent pas suggérer qu'il est nécessaire de créer un compte personnalisé pour utiliser leurs services en redirigeant automatiquement les utilisateurs non identifiés vers un formulaire d'inscription à un compte personnalisé, parce qu'il n'est pas nécessaire et qu'il n'y a aucune raison légitime de collecter des données à caractère personnel autres qu'avec le consentement éclairé de l'utilisateur.

La corrélation peut également être opérée pour les utilisateurs non authentifiés, grâce à l'adresse IP ou à un «cookie» unique qui peut être reconnu par l'ensemble des différents services proposés par un fournisseur de moteur de recherche. Généralement, cela se fait automatiquement, sans que l'utilisateur en ait conscience. La surveillance secrète du comportement des utilisateurs, un comportement assurément privé, tel que la visite de sites Internet, va à l'encontre des principes de traitement loyal et légitime inscrits dans la directive sur la protection des données. Les fournisseurs de moteurs de recherche devraient indiquer clairement dans quelle mesure les données sont transmises entre les services et ne procéder qu'avec le consentement des utilisateurs.

Enfin, certains fournisseurs de moteurs de recherche reconnaissent explicitement dans leur politique de confidentialité qu'ils enrichissent les données fournies par les utilisateurs avec des données provenant de tiers, d'autres sociétés qui peuvent, par exemple, joindre des informations géographiques à des séries d'adresses IP ou des sites Internet contenant des publicités vendues par le fournisseur de moteur de recherche[52]. Ce genre de corrélation peut être illicite si les personnes concernées n'en sont pas informées

51 Par exemple, dans le cas de Microsoft, entre le moteur de recherche en ligne et la console de jeu connectée à l'internet (Xbox).

au moment où leurs données personnelles sont collectées, si elles ne peuvent pas aisément accéder à leur profil personnel, et si elles n'ont pas le droit de corriger ou de supprimer certains éléments incorrects ou superflus. Si le traitement en question n'est pas nécessaire à la prestation du service (de recherche), le consentement éclairé donné librement par l'utilisateur doit être requis pour que le traitement soit licite.

6. Obligation d'informer la personne concernée

La plupart des internautes ne sont pas conscients des grandes quantités de données relatives à leurs recherches qui sont traitées, ni des finalités de leur utilisation. S'ils ne sont pas conscients de ce traitement, ils sont incapables de prendre des décisions éclairées à ce sujet.

L'obligation d'informer les personnes du traitement de leurs données à caractère personnel est un des principes fondamentaux de la directive sur la protection des données. L'article 10 stipule les informations à fournir lorsque les données sont obtenues directement de la personne concernée. Les responsables du traitement des données doivent fournir les informations suivantes à la personne concernée:

- l'identité du responsable du traitement et, le cas échéant, de son représentant ;
- les finalités du traitement auquel les données sont destinées ;
- toute information supplémentaire telle que :
- les destinataires ou les catégories de destinataires des données ;
- le fait de savoir si la réponse aux questions est obligatoire ou facultative, ainsi que les conséquences éventuelles d'un défaut de réponse ;
- l'existence d'un droit d'accès aux données la concernant, et de rectification de ces mêmes données.

En tant que responsables du traitement des données d'utilisateur, les moteurs de recherche devraient indiquer clairement aux utilisateurs quelles données sont collectées à leur sujet et à quoi elles servent. Une description succincte de l'utilisation faite des informations personnelles devrait être fournie à chaque fois qu'elles sont collectées, même lorsqu'une description plus détaillée existe ailleurs. Les utilisateurs devraient également être informés des logiciels, comme les «cookies», susceptibles d'être installés sur leur ordinateur lorsqu'ils utilisent le site Internet, et de la manière dont ils peuvent les refuser ou les supprimer. Le groupe de travail considère que ces informations sont nécessaires dans le cas des moteurs de recherche, afin de garantir un traitement loyal.

Les informations fournies par les fournisseurs de moteurs de recherche en réponse au questionnaire du groupe de travail montrent qu'il existe des différences importantes. Certains moteurs de recherche respectent les dispositions de la directive, y compris les liens vers leur politique de confidentialité, tant sur la page d'accueil que sur les pages générées lors du processus de recherche, et les informations relatives aux «cookies». Avec d'autres moteurs de recherche, il est très difficile de trouver la notice relative à leur politique de protection de la vie privée. Or, les utilisateurs doivent pouvoir y accéder facilement avant d'effectuer une recherche, y compris à partir de la page d'accueil du moteur de recherche.

52 Par exemple, dans ses Principaux éléments de la déclaration de confidentialité de Microsoft online, Microsoft déclare: «Lorsque vous vous inscrivez pour certains services Microsoft, nous vous demandons de fournir des informations personnelles. Les informations que nous collectons peuvent être associées à des informations obtenues via d'autres services Microsoft et d'autres sociétés.» URL: http://privacy.microsoft.com/fr-fr/. Et, au sujet du partage des données avec des partenaires publicitaires, Microsoft, dans sa déclaration de confidentialité complète, déclare: «Nous proposons également de la publicité et des outils d'analyse de sites internet sur des sites et des services autres que Microsoft, et nous sommes susceptibles de collecter des informations au sujet des pages consultées sur ces sites tiers également». URL: http://privacy.microsoft.com/en-us/fullnotice.aspx. Dans sa politique de confidentialité, Google déclare: «Nous regroupons parfois des informations personnelles recueillies auprès de vous et des informations provenant d'autres services Google ou de services tiers, afin de vous offrir un meilleur confort d'utilisation, y compris la possibilité de personnaliser votre contenu.» URL: http://www.google.fr/privacy.html. Dans sa politique de confidentialité, Yahoo! déclare: «Yahoo! est susceptible de combiner des informations vous concernant qui sont en notre possession à des information obtenues de nos partenaires commerciaux ou d'autres sociétés.» URL: http://info.yahoo.com/privacy/us/yahoo/details.html.

Le groupe de travail recommande que la version intégrale de la notice relative à la politique de confidentialité soit aussi complète et détaillée que possible, en mentionnant les principes fondamentaux inscrits dans la législation en matière de protection des données.

Le groupe de travail observe que nombre de ces notices montrent des insuffisances en ce qui concerne le droit d'accès ou de suppression reconnu à la personne concernée aux articles 12, 13 et 14 de la directive sur la protection des données. Ces droits sont pourtant un des aspects fondamentaux de la protection de la vie privée des personnes.

7. Droits de la personne concernée

Les moteurs de recherche devraient respecter les droits des personnes concernées de consulter et, le cas échéant, de rectifier ou d'effacer les informations détenues à leur sujet. Ces droits s'appliquent surtout aux données d'utilisateurs authentifiés stockées par les moteurs de recherche, y compris les profils personnels. Ces droits s'appliquent toutefois aussi aux utilisateurs non enregistrés, qui devraient avoir le moyen de prouver leur identité au fournisseur de moteur de recherche, par exemple en s'enregistrant afin d'avoir accès aux futures données et/ou à l'aide d'une déclaration de leur fournisseur d'accès attestant l'utilisation d'une adresse IP spécifique au cours de la période pour laquelle l'accès est demandé. Quant au contenu des données, les fournisseurs de moteurs de recherche ne sont, en général, pas considérés comme les principaux responsables en vertu de la législation européenne en matière de protection des données.

En 2000, dans son document de travail intitulé «Le respect de la vie privée sur Internet»[53], le groupe de travail expliquait déjà: «*La personnalisation des profils sera subordonnée à une information et un accord préalables des individus. Ils doivent avoir le droit d'annuler leur accord à n'importe quel moment, avec effet immédiat mais non rétroactif. Deuxièmement, les utilisateurs doivent pouvoir à n'importe quel moment avoir accès à leurs profils pour vérification. Ils doivent également avoir le droit de corriger et d'effacer les données enregistrées.*»

Lorsque cela est appliqué spécifiquement aux moteurs de recherche, les utilisateurs doivent avoir le droit d'accéder à toute donnée à caractère personnel stockée à leur sujet conformément à l'article 12 de la directive sur la protection des données (95/46/CE), y compris leurs recherches antérieures, les données collectées auprès d'autres sources et les données révélant leur comportement ou leur origine. Le groupe de travail «Article 29» considère comme essentiel que les fournisseurs de moteurs de recherche mettent à la disposition des utilisateurs les moyens nécessaires pour exercer ces droits, par exemple, au moyen d'un outil en ligne permettant aux utilisateurs enregistrés d'accéder directement à leurs données personnelles et offrant la possibilité de s'opposer au traitement de certaines d'entre elles.

D'autre part, le droit de rectifier ou d'effacer des informations s'applique également à certaines données spécifiques de la mémoire cache détenues par les fournisseurs de moteurs de recherche, une fois que ces données ne correspondent plus au contenu publié sur Internet par les responsables du traitement du (des) site(s) Internet qui publie(nt) ces informations[54]. Dans ce cas, lorsqu'ils reçoivent une demande d'une personne concernée, les fournisseurs de moteurs de recherche doivent agir rapidement pour supprimer ou corriger les informations incomplètes ou périmées. La mémoire cache peut être mise à jour par une nouvelle visite instantanée automatique de la publication originale. Les fournisseurs de moteurs de recherche devraient offrir aux utilisateurs la possibilité de demander gratuitement la suppression de ce genre de contenu de leur mémoire cache.

53 WP 37, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37fr.pdf

54 Le groupe de travail suggère que les éditeurs de pages internet mettent au point des mesures en vue d'informer automatiquement les moteurs de recherche de toute demande de suppression de données à caractère personnel reçue.

8. Conclusions

Internet a été conçu comme un réseau mondial ouvert permettant d'échanger des informations. Il est cependant nécessaire de trouver un équilibre entre cette nature ouverte et la protection des données à caractère personnel des internautes. À cet effet, il convient de bien distinguer les deux principaux rôles des fournisseurs de moteurs de recherche. Dans le premier, celui de responsables du traitement des données d'utilisateur (comme les adresses IP qu'ils collectent auprès des utilisateurs et leur historique de recherche propre), ils doivent être tenus pour entièrement responsables au titre de la directive sur la protection des données. Dans le second, celui de fournisseurs de données de contenu (comme les données de l'index), en général ils ne doivent pas être considérés comme les principaux responsables, au regard de la législation européenne protégeant les données, des données à caractère personnel qu'ils traitent. Les exceptions sont l'existence d'une mémoire cache à long terme et les opérations à valeur ajoutée effectuées sur les données à caractère personnel (comme les moteurs de recherche destinés à établir des profils de personnes physiques). Lorsqu'ils fournissent ce genre de services, les moteurs de recherche doivent être tenus pour entièrement responsables au titre de la directive sur la protection des données, et ils doivent respecter toutes les dispositions applicables en la matière.

L'article 4 de la directive sur la protection des données prévoit que ses dispositions s'appliquent au responsable du traitement possédant un établissement sur le territoire d'au moins un État membre qui participe au traitement des données à caractère personnel. Les dispositions de la directive peuvent également s'appliquer aux fournisseurs de moteurs de recherche qui ne possèdent pas d'établissement sur le territoire de la Communauté s'ils recourent, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire d'un État membre.

Eu égard à ce qui précède, et compte tenu du *modus operandi* actuel des moteurs de recherche, les conclusions suivantes peuvent être tirées:

Applicabilité des directives CE

1. La directive sur la protection des données (95/46/CE) s'applique généralement au traitement de données à caractère personnel effectué par les moteurs de recherche, même lorsque leur siège se trouve en dehors de l'EEE.

2. Les fournisseurs de moteurs de recherche basés en dehors de l'EEE devraient informer leurs utilisateurs des conditions dans lesquelles ils doivent respecter la directive sur la protection des données, que ce soit en raison de la présence d'un établissement ou du recours à des moyens situés sur le territoire d'un État membre.

3. La directive sur la conservation des données (2006/24/CE) ne s'applique pas aux moteurs de recherche sur Internet.

Obligations des fournisseurs de moteurs de recherche

4. Les moteurs de recherche ne peuvent traiter des données à caractère personnel qu'à des fins légitimes, et la quantité de données doit être pertinente et non excessive par rapport aux diverses finalités prévues.

5. Les fournisseurs de moteurs de recherche doivent effacer ou rendre les données à caractère personnel anonymes (de manière irréversible et effective) une fois qu'elles ne sont plus nécessaires à la finalité pour laquelle elles avaient été collectées. Le groupe de travail préconise que les fournisseurs de moteurs de recherche développent des programmes d'anonymisation adéquats.

6. Les délais de conservation devraient être réduits au minimum et être proportionnels à chaque finalité invoquée par les fournisseurs de moteurs de recherche. Au vu des explications initiales données par ces derniers au sujet des finalités possibles de la collecte de données à caractère personnel, le groupe de travail ne voit pas de raison de conserver ces données au-delà de six mois. La législation nationale peut cependant exiger que les données à caractère personnel soient effacées plus tôt. Si les fournisseurs de moteurs de recherche conservent ces données plus de six mois, ils doivent démontrer de manière détaillée que cela est strictement nécessaire au service. Quoi qu'il en soit, les informations relatives au délai de conservation des données choisi par les fournisseurs

de moteurs de recherche devraient être facilement accessibles sur leur page d'accueil.

7. Si les fournisseurs de moteurs de recherche collectent inévitablement certaines données à caractère personnel relatives aux utilisateurs de leurs services, comme leur adresse IP, résultant d'un trafic HTTP normal, il n'est pas nécessaire d'en collecter d'autres auprès des utilisateurs individuels pour pouvoir fournir le service ou proposer des résultats de recherche et des publicités.

8. Si les fournisseurs de moteurs de recherche utilisent des «cookies», leur durée de vie ne devrait pas être plus longue que celle manifestement nécessaire. Comme les «cookies» Internet, les «cookies» flash ne devraient être installés que si des informations transparentes sont fournies, expliquant les raisons de leur installation et comment accéder à ces informations, les modifier et les supprimer.

9. Les fournisseurs de moteurs de recherche doivent donner aux utilisateurs des informations claires et intelligibles au sujet de leur identité et de leur situation ainsi que sur les données qu'ils envisagent de collecter, de stocker ou de transmettre, et sur la finalité de cette collecte[55].

10. L'enrichissement de profils d'utilisateurs à l'aide de données qui ne proviennent pas des utilisateurs eux-mêmes doit être soumis à leur consentement.

11. Si les fournisseurs de moteurs de recherche proposent des moyens de conserver l'historique de recherche, ils doivent s'assurer d'avoir le consentement de l'utilisateur.

12. Les moteurs de recherche devraient respecter le choix des éditeurs de sites Internet de ne pas participer à leurs services, indiquant que le site ne devra être ni exploré ni indexé, ni figurer dans la mémoire cache des moteurs de recherche.

13. Lorsque les fournisseurs de moteurs de recherche proposent une mémoire cache, dans laquelle les données à caractère personnel sont disponibles plus longtemps que dans la publication originale, ils doivent respecter le droit des personnes concernées de faire retirer les données excessives ou inexactes de la mémoire cache.

14. Les fournisseurs de moteurs de recherche spécialisés dans la création d'opérations à valeur ajoutée, comme les profils de personnes physiques (appelés «moteurs de recherche de personnes») et les logiciels de reconnaissance faciale sur la base d'images, doivent avoir une raison légitime de traiter les données à caractère personnel, par exemple le consentement de la personne concernée, et respecter toutes les autres exigences de la directive sur la protection des données, telles que l'obligation de garantir la qualité des données et la loyauté du traitement.

Droits des utilisateurs

15. En vertu de l'article 12 de la directive sur la protection des données (95/46/CE), les utilisateurs de services de moteur de recherche ont le droit de consulter, de vérifier et, le cas échéant, de rectifier toutes leurs données personnelles, y compris leur profil et leur historique de recherche.

16. La corrélation croisée de données provenant de différents services qui appartiennent au fournisseur de moteur de recherche ne peut être effectuée que si l'utilisateur a donné son consentement pour ce service spécifique.

Fait à Bruxelles, le 4 avril 2008
Pour le groupe de travail
Le président
Alex TURK

55 Le groupe de travail recommande un modèle stratifié pour la politique de confidentialité, tel que décrit dans son avis intitulé «Dispositions davantage harmonisées en matière d'informations»
(WP 100, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_fr.pdf)

Annexe 1

Exemple de données traitées par les moteurs de recherche et terminologie

Journaux des requêtes	
Requête de recherche	Requête de recherche introduite dans le moteur de recherche, habituellement stockée dans ses journaux sous la forme de l'URL de la page proposée comme résultat de la requête.
Adresse IP	Adresse du protocole Internet de l'ordinateur de l'utilisateur pour chaque requête introduite.
Date et heure	Date et heure auxquelles une requête spécifique a été introduite.
«Cookie»	«Cookie(s)» (et/ou dispositif(s) similaire(s)) stocké(s) sur l'ordinateur de l'utilisateur, y compris tous les paramètres du «cookie» tels que sa valeur et sa date d'expiration. Sur le serveur du moteur de recherche, toutes les données relatives au «cookie», comme les informations suivantes: «le «cookie»/dispositif X a été placé sur l'ordinateur dont l'adresse IP est Y, à la date et à l'heure Z».
«Cookie» flash	ou «Local Shared Object» est un «cookie» installé au moyen de la technologie Flash. Actuellement, il ne peut pas être effacé simplement via les paramètres du navigateur, comme les «cookies» Internet traditionnels.
URL de référence	URL de la page Internet sur laquelle la requête de recherche a été introduite, qui peut être une URL tierce.
Préférences	Préférences spécifiques possibles de l'utilisateur dans les paramètres avancés du service.
Navigateur	Informations relatives au navigateur, dont le type et la version.
Système d'exploitation	Informations relatives au système d'exploitation.
Langue	Paramètres de la langue définis dans le navigateur de l'utilisateur, qui peuvent être utilisés pour déduire la préférence linguistique de l'utilisateur.
Contenu proposé	
Liens	Liens qui ont été proposés à un utilisateur à la suite d'une requête, à une date et une heure données. Les résultats des moteurs de recherche sont dynamiques. Pour pouvoir évaluer les résultats en détail, le fournisseur de moteur de recherche doit stocker des informations relatives aux liens spécifiques et à l'ordre dans lequel ils ont été présentés à une date et une heure données en réponse à une requête d'utilisateur.
Publicités	Publicités qui sont présentées à l'utilisateur à la suite d'une requête.

Navigation de l'utilisateur	
	Clics de l'utilisateur sur les résultats organiques et les publicités de la (des) page(s) de résultats. Cela inclut le classement des résultats spécifiques qui ont été suivis par l'utilisateur (le lien n° 1 a d'abord été suivi, après quoi l'utilisateur est revenu à la page des résultats et a suivi le lien n° 8).
Données opérationnelles	
	En raison de la valeur et de l'utilisation opérationnelles de certaines des données décrites ci-dessus, par exemple pour détecter des fraudes, assurer la sécurité/l'intégrité du service et établir le profil des utilisateurs, les moteurs de recherche signalent et analysent ces données de différentes manières. Par exemple, une adresse IP donnée peut être signalée comme source probable de fraude au niveau des requêtes ou des clics, un clic spécifique sur une publicité peut être signalé comme frauduleux, une requête peut être signalée comme étant liée à des sources d'information sur un certain sujet.
Données relatives aux utilisateurs enregistrés	
	Un fournisseur de moteur de recherche peut proposer aux utilisateurs de s'enregistrer afin de bénéficier de services améliorés. En général, le fournisseur traite les données du compte d'utilisateur telles que le nom d'utilisateur et son mot de passe, une adresse électronique, et toute autre donnée à caractère personnel fournie par l'utilisateur, comme ses intérêts, ses préférences, son âge et son sexe.
Données d'autres services/sources	
	La plupart des fournisseurs de moteurs de recherche proposent d'autres services, tels que le courrier électronique, la recherche sur l'ordinateur de l'utilisateur et la publicité sur des sites Internet et services tiers. Ces services génèrent des données d'utilisateur qui peuvent être mises en corrélation et utilisées pour améliorer la connaissance que les moteurs de recherche ont des utilisateurs. Les données d'utilisateur et les éventuels profils peuvent également être enrichis à l'aide de données provenant d'autres sources, comme les données de géolocalisation des adresses IP et les données démographiques.

Annexe 2

Questionnaire adresse aux moteurs de recherche au sujet de leur politique de confidentialite

1. Stockez-vous des données relatives à l'utilisation individuelle de vos services de recherche?
2. Quel type d'informations stockez/archivez-vous dans le cadre de vos services de recherche? (p. ex. journaux de serveurs, mots clés, résultats de recherche, adresses IP, «cookies», données relatives aux clics, copies instantanées de sites Internet (mémoires caches), etc.)
3. Demandez-vous le consentement (éclairé) de l'utilisateur pour stocker les données indiquées dans votre réponse à la question 2, et si oui, comment? Si non, sur quelle base juridique justifiez-vous le stockage de ces données?
4. Créez-vous des profils de comportement des utilisateurs à partir des données indiquées dans votre réponse à la question 2? Si oui, à quelles fins? Quelles données traitez-vous? Sous quel identifiant (p. ex. adresse IP, nom d'utilisateur, «cookie» d'identification) stockez-vous ces profils? Demandez-vous le consentement de l'utilisateur?
5. Si vous proposez d'autres services spécialisés en plus des services de recherche, partagez-vous les données collectées dans le cadre de vos services de recherche avec ces autres services, et/ou vice versa? Si oui, veuillez indiquer quelles données.
6. Combien de temps stockez-vous les données indiquées dans votre réponse à la question 2 et à quelles fins?
7. À quels critères recourez-vous pour déterminer la durée de stockage?
8. Lorsque vous stockez des données pour une durée déterminée à l'avance, que faites-vous une fois que ce délai arrive à expiration, et quelles procédures sont en place à ce sujet?
9. Rendez-vous les données anonymes? Si oui, comment? Cette anonymisation est-elle irréversible? Quelles informations les données rendues anonymes contiennent-elles encore?
10. Les données sont-elles accessibles au personnel, par exemple, ou sont-elles traitées sans intervention humaine?
11. Transmettez-vous des données à des tiers? Dans quels pays? Veuillez indiquer, pour les catégories suivantes, le type de données que vous êtes susceptibles de partager et avec quels pays:
    - annonceurs;
    - partenaires publicitaires;
    - services répressifs (respect des obligations juridiques de fournir des données, par exemple dans des affaires judiciaires);
    - autres (veuillez préciser).
12. Comment informez-vous les utilisateurs de la collecte, du traitement et du stockage de leurs données? Leur fournissez-vous des informations complètes concernant, par exemple, les «cookies», l'établissement de profils et d'autres outils qui contrôlent l'activité du site Internet? Si oui, veuillez joindre une copie de l'avis d'information, ainsi qu'une description de son emplacement.
13. Octroyez-vous aux utilisateurs le droit de consulter et le droit de rectifier les données ou de les modifier, de les effacer ou de les bloquer? Est-il possible de refuser la collecte ou le stockage des données de telle manière qu'aucune donnée à caractère personnel ne soit collectée, et qu'aucune trace de l'utilisateur individuel ne soit laissée sur aucun système de stockage concerné? Des coûts sont-ils facturés pour l'exercice de ces droits?
14. Appliquez-vous des mesures de sécurité au traitement des données? Lesquelles?
15. Avez-vous averti une autorité nationale de protection des données dans l'EEE? Si oui, veuillez indiquer laquelle. Si non, veuillez en donner les raisons.

Working Party 29 – « Avis 3/2008 sur le projet de norme internationale de protection de la vie privée du code mondial antidopage »

Adopté le 1er août 2008

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

établi par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995,

vu l'article 29 et l'article 30, paragraphe 1, point a), et paragraphe 3, de ladite directive, et l'article 15, paragraphe 3, de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002,

vu l'article 255 du traité CE et le règlement (CE) n° 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission,

vu son règlement intérieur,

a adopté le présent avis.

Introduction

La direction générale de l'éducation et de la culture (DG EAC) de la Commission européenne a sollicité l'avis du groupe de travail «article 29» (ci-après «le groupe de travail») sur le projet de norme internationale de protection de la vie privée, élaboré par l'Agence mondiale antidopage (AMA).

Le projet de norme doit être lu en parallèle avec le code mondial antidopage de l'AMA (ci-après «le code»), et en particulier avec son article 14.

Le code exige que les athlètes communiquent régulièrement certaines données aux organisations antidopage. Ces informations sont ensuite regroupées avec d'autres renseignements (y compris des données sensibles) dans la base ADAMS, située au Canada.

Des données relatives à leur personnel d'encadrement – tel qu'il est défini dans le code – et à d'autres catégories de personnes sont également traitées au titre des obligations prévues dans le code. Dans le cadre de ce dernier, le terme «participant» désigne l'athlète ainsi que son personnel d'encadrement.

Partie I – Introduction, dispositions du code et définitions

Point 2 – Dispositions du code

Bien que l'avis du groupe de travail porte uniquement sur le projet de norme internationale tel qu'il lui a été soumis le 7 juillet 2008, et non sur le code mondial antidopage, le groupe se doit néanmoins de souligner (lorsque le projet de norme renvoie aux dispositions du code) que certaines de ces dispositions suscitent des interrogations concernant leur compatibilité avec les normes européennes de protection des données.

Toute personne participant à la lutte contre le dopage a droit au respect de sa vie privée et à la protection de ses données personnelles. Par conséquent, l'article 14 du code pourrait être modifié comme suit: *«Les signataires conviennent des principes d'une gestion coordonnée des résultats antidopage, d'une gestion responsable, transparente et respectueuse des intérêts privés* ***de tous les individus, y compris*** *ceux présumés avoir violé des règles antidopage».*

Article 14.2 – Diffusion publique

Le groupe de travail rappelle que la divulgation et la communication de données constituent un traitement de données soumis au régime de protection des données. Il note avec satisfaction que la diffusion de décisions concernant un athlète qui n'a pas commis de violation des règles antidopage ne pourra avoir lieu qu'avec le consentement de cet athlète. Il préconise néanmoins de préciser la norme internationale afin qu'il soit clair pour les organisations antidopage que «des efforts raisonnables afin d'obtenir ce consentement» ne peuvent remplacer valablement le consentement à la diffusion de la personne concernée (voir article 14.2. 3).

Le groupe de travail s'interroge également sur la proportionnalité du processus qui consiste à divulguer publiquement, en les affichant sur Internet pendant au

moins un an, le jugement et d'autres informations sur les athlètes ou toute autre «personne» (article 14.2.4 – voir également Partie II, point 10 ci-dessous). À cet égard, le groupe de travail suggère que ces «personnes», à moins qu'elles ne soient les athlètes eux-même ou leur personnel d'encadrement, soient soumises à la présente norme. Aucune raison ne justifie que, dans ce cas, elles ne bénéficient pas de sa protection.

Article 14.5 (base de données ADAMS)

À l'exception des quelques lignes dans l'article 14.4 du code, le projet de norme ne prévoit aucune règle précise pour le traitement des informations lié à la base de données ADAMS. Ce projet s'adresse uniquement aux organisations antidopage.

Or, les dispositions de protection des données dans le cadre de la lutte contre le dopage doivent être garanties tant pour le traitement des données effectué par les organisations antidopage que pour l'utilisation de la base de données ADAMS. Le groupe de travail note que la surveillance de cette base de données relève de la compétence des autorités canadiennes de la protection des données. Il estime toutefois que la simple référence faite dans la norme à cette base de données est insuffisante.

Par conséquent, le groupe de travail recommande que la norme internationale soit modifiée pour y inclure davantage de détails sur la base de données ADAMS ou que l'AMA mette au point des procédures pour les utilisateurs de cette base. Il rappelle en outre que des précautions doivent être prises dans le cadre des transferts de données de l'UE vers le Canada pour assurer le respect de la législation de l'UE sur les garanties en matière de transferts ultérieurs.

Article 14.6

Le terme «tiers» n'est pas défini.

D'une manière générale, les objectifs spécifiques du traitement des données effectué au titre du code devraient être définis. La seule référence au traitement des données par les organisations antidopage «dans le contexte [de leurs] activités contre le dopage» n'est pas suffisante.

Point 3 – Termes et définitions

Participant

Le groupe de travail considère que la notion de «participant» telle qu'elle est définie dans le code est trop restrictive pour garantir la protection de toute personne dont les données peuvent être traitées dans le cadre de l'application du code (voir les remarques ci-dessus sur la notion de «personne» (article 14.2.4) et sur les «tiers» (article 14.6)). Le groupe de travail reconnaît que seuls les athlètes et leur personnel d'encadrement seront dans l'obligation de communiquer des renseignements à caractère personnel à l'AMA, mais un usage homogène des termes dans la norme internationale et dans le code contribuerait à éviter toute confusion.

Trois nouvelles définitions sont introduites à l'article 3.2 du projet de norme:

Informations à caractère personnel

La définition donnée inclut celle des «données à caractère personnel» de l'article 2, point a), de la directive 95/46/CE. Le groupe de travail observe qu'à l'exception du point 9 (sécurité des informations à caractère personnel), le projet de norme n'offre aucune garantie supplémentaire pour la protection des données sanitaires et judiciaires traitées dans le cadre des activités de lutte contre le dopage.

Informations à caractère personnel sensibles

Les informations à caractère personnel considérées comme sensibles correspondent à celles visées à l'article 8 de la directive 95/46/CE. Le groupe de travail renvoie ici à son commentaire sur l'article 6 de la norme concernant le traitement de données de ce type (voir ci-dessous).

Traitement

Même si la définition ne correspond pas exactement à celle de l'article 2, point b), de la directive 95/46/CE, elle est néanmoins acceptable.

Partie II– Normes pour le traitement des données à caractère personnel

Point 4 – Traitement des informations à caractère personnel conformément à la norme internationale et au droit applicable

Le groupe de travail considère que la notion de «tiers» comprend les sous-traitants au sens de l'article 2, point e), de la directive 95/46/CE. Cette supposition fonde les autres commentaires concernant cette notion (voir point 9), dont le champ d'application doit être défini avec précision.

Article 4.1

Le groupe de travail estime nécessaire de modifier l'article 4.1 afin de préciser que les tiers sont également tenus de respecter la norme, même lorsque les obligations qu'elle impose dépassent celles des législations nationales.

Le projet de norme n'opère pas de distinction entre les différentes catégories de personnes qui lui sont soumises (athlètes, personnel d'encadrement, tiers). Or, l'application du principe de proportionnalité dépendra de la catégorie à laquelle la personne appartient.(quelles données sont traitées? quelles données sont stockées?) Le projet de norme devrait donc être modifié sur ce point.

Traitement d'informations personnelles pertinentes et proportionnées

L'article 5.3, devrait spécifier quelles sont les informations à caractère personnel ou les catégories d'informations à caractère personnel qui sont nécessaires pour atteindre les objectifs énumérés aux points a), b) et c) en tenant compte des principes de nécessité et de proportionnalité. Comme il a été indiqué précédemment, la mise en oeuvre de ces principes variera en fonction de la catégorie des personnes dont les données seront traitées (athlètes, personnel d'encadrement).

L'article 5.4 du projet de norme dispose que les informations à caractère personnel ainsi traitées doivent être exactes, complètes et actualisées. La dernière phrase de ce paragraphe semble toutefois atténuer cette obligation pour les organisations antidopage. Elle semble même déplacer la responsabilité du responsable du traitement des données vers la personne concernée[56], comme semble le confirmer le commentaire. À cet égard, le groupe de travail souligne que, d'après l'article 6, point d), de la directive 95/46/CE, toutes les mesures nécessaires doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées. Cette responsabilité incombe au responsable du traitement des données, si nécessaire en réponse à une demande de rectification présentée par la personne concernée.

Point 6 – Traitement d'informations personnelles avec le consentement de la personne concernée

D'après l'article 7 de la directive 95/46/CE, tout traitement de données doit être justifié par un motif légitime valable. L'existence d'un tel fondement légitime est primordial dans les cas où sont traitées des données sanitaires.

Article 6.1

L'article 6.1 du projet de norme invite les organisations antidopage à se servir du consentement des athlètes et des membres de leur personnel d'encadrement pour légitimer leur traitement de données. Le groupe de travail estime que ce consentement n'est pas conforme aux obligations énoncées à l'article 2, point h), de la directive 95/46/CE, qui le définit comme «*toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement*». Or, le consentement

56 «(…). Bien que ceci ne signifie pas nécessairement que les organisations antidopage sont tenues de vérifier l'exactitude de toutes les informations à caractère personnel qu'elles traitent, elles sont néanmoins dans l'obligation de rectifier ou de modifier dès que possible toute information à caractère personnel qu'elles savent avec certitude être incorrecte ou inexacte.»

au traitement des données recueillies dans le contexte de l'exécution des obligations du code mondial antidopage n'est ni libre, ni informé. Les sanctions liées à un éventuel refus des participants de se soumettre aux obligations du code (communication de données facilitant la localisation des athlètes, contrôles médicaux antidopage) amènent le groupe de travail à considérer que le consentement n'est en aucun cas donné librement[57]. Le groupe de travail émet également des doutes quant au caractère informé du consentement (voir point 7 ci-dessous).

Le traitement des données ne pouvant pas être justifié par l'article 7, point a), et l'article 8, paragraphe 2, point a) de la directive 95/46/CE, il devra s'appuyer sur un autre motif légitime.

Le groupe de travail rappelle que le traitement de données relatives aux infractions n'est pas autorisé, même avec le consentement, fût-il informé, de la personne concernée (article 8, paragraphe 5, de la directive 95/46/CE).

Par conséquent, le groupe de travail préconise que l'AMA envisage d'autres motifs de traitement que ceux décrits à l'article 7 pour les données à caractère personnel et à l'article 8 pour les données à caractère personnel sensibles, de la directive 95/46/CE.

Différents accords internationaux relatifs à la lutte contre le dopage, tels que la convention internationale contre le dopage dans le sport ou la convention contre le dopage du Conseil de l'Europe, pourraient servir de fondements juridiques au traitement des données, dans la mesure où ces conventions invoqueraient une obligation juridique contraignante à laquelle les organisations antidopage sont soumises en tant que responsables du traitement, en vertu des mesures nationales d'exécution de l'article 7, point c), et de l'article 8, paragraphe 4, de la directive 95/46/CE.

Article 6.2

L'article 6.2 du projet de norme autorise l'éventuel traitement de données sensibles telles que celles préalablement définies à l'article 3.2. Conformément à la directive 95/46/CE, les données à caractère personnel sensibles incluent les données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale ou la vie sexuelle. Le groupe de travail doute très sérieusement de la pertinence du traitement de plusieurs de ces catégories d'informations, en particulier si ces données sont destinées à être introduites dans la base de données ADAMS. C'est pourquoi le groupe de travail invite l'AMA à fournir d'autres informations ou à réexaminer la pertinence de l'éventuel traitement de données de ce type et à spécifier à l'article 6.2 les données significatives destinées à être traitées dans ce cadre. Par ailleurs, la définition de l'article 3.2 inclut les caractéristiques génétiques. Le groupe de travail conteste la légitimité et la nécessité du traitement de telles informations et demande à l'AMA de s'assurer que ce traitement est nécessaire. Dans tous les cas, il recommande que le niveau de protection des données pendant leur traitement soit particulièrement élevé.

Article 6.4

Le champ d'application de l'article 6.4 devrait être étendu afin de permettre aux représentants légaux des participants d'exercer les autres droits évoqués par le projet de norme, notamment ceux décrits au point 11.

Point 7 – Assurer la bonne information des participants

Le groupe de travail attire l'attention sur les dispositions des articles 10 et 11 de la directive 95/46/CE, en particulier sur l'obligation de fournir des renseignements non seulement sur l'identité du responsable du traitement mais également sur l'identité de tous ses représentants.

L'article 7.2 mentionne que lorsque les informations à caractère personnel ne sont pas recueillies auprès du participant, ce dernier doit en être informé «le plus tôt possible». Afin de respecter les dispositions de la directive 95/46/CE à son

57 L'article 6.3 du projet de norme requiert ainsi que «les organisations antidopage informent les participants des conséquences négatives que peut entraîner leur refus de prendre part aux contrôles antidopage, y compris le «testing»».

article 11, paragraphe 1, ces informations devront être communiquées dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard lors de la première communication de données. Dans des circonstances exceptionnelles, il ne sera pas nécessaire de fournir ces informations «*lorsque, en particulier pour un traitement à finalité statistique ou de recherche historique ou scientifique, l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés ou si la législation prévoit expressément l'enregistrement ou la communication des données*». Ces limites doivent toutefois être interprétées de manière restrictive.

Le groupe de travail signale également que, dans le commentaire de l'article 7.2, l'emploi des termes «*il ou elle devrait […] avoir un accès raisonnable aux informations […]*» semble restreindre le droit à l'information des personnes concernées. Il rappelle que le droit de la personne concernée à être informée est essentiel et fait partie des obligations de transparence du traitement des données.

Point 8 – Diffusion d'informations à caractère personnel à d'autres organisations antidopage et à des tiers

Le groupe de travail souligne qu'un transfert à partir de l'Espace économique européen vers un pays tiers ne peut avoir lieu que si le pays tiers assure le niveau de protection adéquat décrit à l'article 25, paragraphe 2, de la directive 95/46/CE, ou lorsque le responsable du traitement offre des garanties suffisantes en matière de protection de la vie privée, ou encore lorsque le transfert se fonde sur l'une des exceptions ou dérogations envisagées à l'article 26, paragraphe 1, de la directive 95/46/CE.

En l'occurrence, la base de données ADAMS se situe au Canada. Aux fins de l'article 25, paragraphe 2, de la directive 95/46/CE, le Canada est considéré comme assurant un niveau de protection adéquat des données à caractère personnel transférées de la Communauté européenne aux destinataires soumis à la loi canadienne sur la protection des renseignements personnels et les documents électroniques (loi PIPEDA)[58]. Cependant, le groupe de travail ne peut déterminer si le responsable de la base de données ADAMS est l'AMA ou une autorité nationale canadienne de lutte contre le dopage, ni si le responsable est soumis à la loi PIPEDA. Il préconise que ce point soit clarifié et, si le responsable de la base de données ADAMS n'est pas soumis à la loi PIPEDA, que des mesures soient prises pour garantir un niveau de protection adéquat des informations transférées de la Communauté européenne vers la base de données ADAMS.

Le groupe de travail souligne la nécessité de respecter le «principe de finalité» et l'obligation de compatibilité du traitement ultérieur des données avec l'objectif initial pour lequel elles ont été recueillies.

En ce qui concerne l'article 8.4, le groupe de travail réitère les remarques faites au point 6 cidessus à propos de la validité du consentement. Il fait également observer que cette disposition n'autoriserait pas la publication sur Internet d'informations à caractère personnel concernant les athlètes ou d'autres personnes, comme le prévoit l'article 14.2.4 du code antidopage (voir ci-dessus point 2 – Dispositions du code).

Point 9 – Sécurité des informations à caractère personnel

À l'article 9.1, les coordonnées de la personne désignée par l'organisation antidopage devraient être immédiatement communiquées à la personne concernée (ainsi que les informations visées à l'article 7.1, et non uniquement à sa demande).

Au sujet des sous-traitants auxquels les organisations antidopage peuvent faire appel (tiers – article 9.4), le groupe de travail rappelle les règles prévues par les articles 16 et 17 de la directive 95/46/CE, en particulier l'obligation qui incombe au responsable des données

58 2002/2/CE: Décision de la Commission du 20 décembre 2001 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la loi canadienne sur la protection des renseignements personnels et les documents électroniques [notifiée sous le numéro C(2001) 4539].

de choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer.

Point 10 – Conservation des seules informations à caractère personnel nécessaires et garantie de leur destruction

Le groupe de travail se félicite de l'introduction dans cette version du projet d'une disposition relative à la durée de conservation des données et de l'obligation de les effacer une fois qu'elles ne sont plus nécessaires à la poursuite des objectifs pour lesquels elles ont été traitées. Il invite néanmoins l'AMA à définir, dans la mesure du possible et en tenant compte de l'expérience acquise dans ce domaine, une durée maximale raisonnable de conservation de ces données – ou, du moins, de certaines catégories de données – par les organisations antidopage. Le point 2, qui concerne les règles relatives à la diffusion publique énoncées à l'article 14.2.4 du code antidopage, ne devrait pas servir ici de modèle car il semble disproportionné que les informations personnelles sur les athlètes ou les autres personnes soupçonnés d'infraction aux règles antidopage doivent «au moins» être affichées sur le site Internet de l'organisation antidopage «pendant au moins un an». (voir partie I ci-dessus).

Le groupe de travail renvoie également à son avis 4/2007 sur le concept de données à caractère personnel[59] afin de comprendre ce que signifient les termes «*anonymisation* / *données anonymes*» au sens de la directive.

Point 11 – Droits des participants relatifs aux informations à caractère personnel

Le projet de norme envisage un droit d'accès pour les athlètes et leur personnel d'encadrement. Conformément à l'article 12 de la directive 95/46/CE, toute personne concernée a notamment le droit d'obtenir du responsable du traitement des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données sont communiquées.

Ces éléments ne sont pas envisagés dans le projet de norme.

Ce dernier prévoit que, dans certains cas, les organisations antidopage ne sont pas tenues de répondre aux demandes d'accès. Le groupe de travail note à ce sujet que les exceptions formulées en des termes particulièrement vagues au point 11.1 (*à moins que cette confirmation n'entre en conflit avec la capacité de l'organisation antidopage à remplir les obligations qui lui sont imposées par le code*) et au point 11.2 (*les demandes qui sont manifestement abusives ou excessives en termes d'ampleur et de fréquence, ou qui imposent une charge disproportionnée en termes de coûts ou d'efforts*) ne semblent pas, au vu de la disposition, être en conformité avec les articles 12 et 15 de la directive. Toute restriction du droit d'accès n'est autorisée que si elle est conforme aux dispositions de l'article 13 de la directive, qui autorise les États membres à prendre des mesures législatives visant à limiter la portée de cette obligation lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder les intérêts énumérés par ces dispositions.

Le groupe de travail constate avec satisfaction que, dans le cas où le droit d'accès du participant lui serait refusé, il devrait recevoir par écrit les raisons de ce refus. Il rappelle néanmoins que ce refus est autorisé uniquement dans les conditions énumérées à l'article 13 de la directive, qui doivent être interprétées de manière restrictive.

S'agissant de l'article 11.4, le groupe de travail souligne que, en application de l'article 12, point c), de la directive, le responsable des données doit notifier aux tiers auxquels les données ont été communiquées toute rectification ou tout effacement effectué en raison du caractère incomplet ou inexact des données si cela ne s'avère pas impossible ou ne suppose pas un effort disproportionné. Pour être en accord avec la

59 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_fr.pdf

législation européenne sur la protection des données, les termes «*le cas échéant*» («*where appropriate*») devraient être interprétés uniquement dans le sens de ces deux exceptions.

Dispositions complémentaires

Enfin, le groupe de travail déplore que plusieurs principes fondamentaux du régime européen de protection des données n'apparaissent pas dans le projet de norme. Il invite l'AMA à réfléchir à l'introduction de dispositions complémentaires qui permettraient de garantir les points suivants:

- l'interdiction des décisions individuelles automatisées (article 15 de la directive): cette interdiction apparaît essentielle au vu des sanctions auxquelles peut exposer le traitement des données;

- l'indépendance du contrôle de l'application par les organisations antidopage des dispositions minimales contenues dans la norme. L'article 8.3 du projet de norme indique qu'une organisation antidopage peut faire part de ses préoccupations à l'AMA concernant l'éventuel non-respect de la norme par une autre organisation. Le groupe de travail estime qu'un tel mécanisme de délation suscite des doutes quant à l'engagement de l'AMA de surveiller l'application effective de la norme et le respect de ses dispositions minimales. Par ailleurs, il remarque que le non-respect des normes n'entraîne aucune sanction contre les organisations antidopage. En somme, quelle sera l'efficacité réelle de cette norme?

- l'existence d'un droit de recours et d'un droit à la réparation du préjudice subi à la suite d'une opération de traitement incompatible avec la norme;

- le fait pour les organisations nationales antidopage d'être soumises aux législations nationales qui réglementent le traitement des informations à caractère personnel.

***

Le groupe de travail soutient l'incitative de l'AMA en faveur de l'adoption de normes minimales de protection de la vie privée et des données à caractère personnel des athlètes et des autres personnes participant à la lutte contre le dopage. Le groupe de travail «article 29» considère que la portée géographique de cette norme peut lui permettre de jouer un rôle significatif à l'égard des traitements de données qui ne sont pas soumis à la législation de l'UE ni à une législation ayant été jugée adéquate par l'UE. Dans tous les États, qu'ils aient ou non établi une protection appropriée pour le traitement des données, cette norme pourrait contribuer à sensibiliser les organisations antidopage à cette question.

Le groupe de travail se félicite qu'il soit fait référence à la directive 95/46/CE dans le préambule du projet de norme. Cependant, il ne lui est pas encore possible de donner son aval à cette dernière puisque ses conditions minimales ne semblent pas atteindre les niveaux minimaux requis par la réglementation européenne sur la protection des données. Le groupe de travail pourrait néanmoins parvenir à une telle conclusion si les remarques ci-dessus sont prises en compte et si les informations concernant la base de données ADAMS sont précisées.

Par conséquent, le groupe de travail invite l'AMA à tenir compte de ces commentaires dans le développement du projet de norme. Il accueillera favorablement toute explication de l'AMA et est disposé à rencontrer l'Agence dans ce but, si nécessaire.

Le groupe de travail n'en espère pas moins être tenu informé du suivi qui sera accordé à ces remarques et, de manière plus générale, de l'évolution des travaux de l'AMA concernant ce projet de norme.

International Working Group on Data Protection in Telecommunications Report and Guidance on Privacy in Social Network Services

"Rome Memorandum"

43rd meeting, 3-4 March 2008, Rome (Italy)

Report

Background

"A social network service focuses on the building and verifying of online social networks for communities of people who share interests and activities, or who are interested in exploring the interests and activities of others, and which necessitates the use of software. Most services are primarily web based and provide a collection of various ways for users to interact […]"[1]. Specifically, many popular sites offer means to interact with other subscribers (based on self-generates personal profiles[2]).

The advent and ever increasing popularity of social network services heralds a sea change in the way personal data of large populations of citizens all over the world become more or less publicly available. These services have become incredibly popular in the past years especially with young people. But increasingly such services are also being offered e.g. for professionals and the elderly.

The challenges posed by social network services are on the one hand yet another flavour of the fundamental changes that the introduction of the Internet in the 90s of the past century has brought with it, by – inter alia – abolishing time and space in publishing information and real-time communication, and by blurring the line between service providers (authors) on the one hand and users/consumers (readers) on the other.

At the same time, social networking services seem to be pushing at the boundaries of what societies see as a person's individual space: Personal data about individuals become publicly (and globally) available in an unprecedented way and quantity[3], especially including huge quantities of digital pictures and videos.

With respect to privacy, one of the most fundamental challenges may be seen in the fact that most of the personal information published in social network services is being published at the initiative of the users and based on their consent. While "traditional" privacy regulation is concerned with defining rules to protect citizens against unfair or unproportional processing of personal data by the public administration (including law enforcement and secret services), and businesses, there are only very few rules governing the publication of personal data at the initiative of private individuals, partly because this had not been a major issue in the "offline world", and neither on the Internet before social network services came into being. Furthermore, the processing of personal data from public sources has traditionally been privileged in data protection and privacy legislation.

At the same time, a new generation of users has arrived: The first generation that has been growing up while the Internet already existed. These "digital natives"[4] have developed their own ways of using Internet services, and of what they see to be private and what belongs to the public sphere. Furthermore they – most of them being in their teens – may be more ready to take privacy risks than the older "digital immigrants". In general, it seems that younger people are more comfortable with publishing (sometimes intimate) details of their lives on the Internet.

Legislators, Data Protection Authorities as well as social network service providers are faced with a situation that has no visible example in the past. While social network services offer a new range of opportunities for communication and real-time exchange of any kind of information, the use of such services can also lead to putting the privacy of its users (and of other citizens not even subscribed o a social network service) at risk.

Risks for Privacy and Security

The surge of social network services has only just begun. While it is possible to identify some risks associated to the provision and use of such services already now, it is very likely that we are at present only looking at the tip of the iceberg, and that new uses – and accordingly new risks – will continue to emerge in the future. Specifically, new uses for the personal data contained in user profiles will be invented by public authorities (including law enforcement and secret services[5]) and by the private sector.

The following list of risks can only represent a snapshot which may need to be revised and updated as social network services develop.

Risks associated to the use of social network services identified up to now include the following:

1. *No oblivion on the Internet:* The notion of oblivion does not exist on the Internet. Data, once published, may stay there literally forever - even when the data subject has deleted them from the "original" site, there may be copies with third parties (including archive services and the "cache" function provided by a well-known search engine provider). Additionally, some service providers refuse to speedily comply (or even to comply at all) with user requests to have data, and especially complete profiles, deleted.

2. *The misleading notion of "community":* Many service providers claim that they are bringing communication structures from the "real" world into cyberspace. A common claim is that it is safe e.g. to publish (personal) data on those platforms, as it would just resemble sharing information with friends as it used to be face-to-face. However, a closer look at some features in some services reveals that this parallel has some weaknesses, including that the notion of "friends" in cyberspace may in many cases substantially differ from the more traditional idea of friendship, and that a community may be very big[6]. If users are not openly informed about how their profile information is shared and what they can do to control how it is shared, they may by the notion of "community" as set out above be lured into thoughtlessly sharing their personal data they would not otherwise. The very name of some of these platforms (e.g. "MySpace") creates the illusion of intimacy on the web.

3. "*Free of charge" may in fact not be "for free"*, when users of many social network services in fact "pay" through secondary use of their personal profile data by the service providers, e.g. for (targeted) marketing.

4. *Traffic data collection by social network service providers*, who are technically capable of recording every single move a user makes on their site; eventually sharing of personal (traffic) data (including users' IP-addresses which can in some cases also resemble location data) with third parties (e.g. for advertising or even targeted advertising). Note that in many jurisdictions these data will also have to be disclosed to law enforcement and/or (national) secret services upon request, including maybe also foreign entities under existing rules on international cooperation.

5. *The growing need to refinance services and to make profits may further spur the collection, processing and use of user data*, when they are the only real asset of social network providers. Social network sites are not – while the term "social" may suggest otherwise – public utilities. At the same time, Web 2.0 as a whole is "growing up", and there is a shift from startups sometimes run by groups of students with less financial interests to major international players entering the market. This has partially changed the rules of the game, as many of these companies noted on national stock markets are under extreme pressure from their investors to create and maximise profits. As for many providers of social networks user profile data and the number of unique users (combined with frequency of use) is the only real asset these companies have, this may create additional risks for unproportional collection, processing and use of users' personal

data. Note that at present, many providers of social network services follow the concept of externalisation of privacy costs to users[7].

6. *Giving away more personal information than you think you do:* For example, photos may become universal biometric identifiers within a network and even across networks. Face recognition software has been dramatically improved over the past years, and will continue to reap even "better" results in the future. Note that once a name can be attached to a picture, this can also endanger the privacy and security of other, possibly pseudonymous or even anonymous user profiles (e.g. dating profiles, which normally have a picture and profile information, but not the real name of the data subject published). Additionally, the European Network and Information Security Agency points to an emerging technology called "content based image retrieval" (CBIR), which creates additional possibilities for locating users by matching identifying features of a location (e.g. a painting in a room, or a building depicted) to location data in a database[8]. Furthermore, "social graph" functionalities popular with many social network services do reveal data about the relationships between different users.

7. *Misuse of profile data by third parties*: This is probably the most important threat potential for personal data contained in user profiles of social network services. Depending on available privacy (default) settings and whether and how users use them, and as well on the technical security of a social network service, profile information, including pictures (which may depict the data subject, but also other people) are made available to – in the worst case – the entire user community. At the same time, very little protection exists at present against copying any kind of data from profiles, and using them for building personal profiles, and/or re-publishing them outside of the social network service[9].

   But even "normal" uses of (user) profile data uses can encroach upon users' informational self-determination and, for example, also severely limit their career prospects[10]: One example that has gained public attention is personnel managers of companies crawling user profiles of job applicants and/or employees, which seems to emerge as a steady feature: According to press reports, already today one third of human resources managers admit to use data from social network services for their work, e.g. to verify and/or complete data of job applicants[11]. privacy standards) are other entities likely to capitalise on these sources[12]. In addition, some social network service providers make available user data to third parties via application programming interfaces, which are then under control of these third parties[13].

8. *The Working Group is especially concerned about* further increased risks of identity theft fostered by the wide availability of personal data in user profiles[14], and by possible hijacking of profiles by unauthorised third parties.

9. *Use of a notoriously insecure infrastructure:* Much has been written over the (lack of) security of information systems and networks, including web services. Recent incidents include wellknown service providers like Facebook[15], flickr[16], MySpace[17], Orkut[18] and the German provider "StudiVZ"[19]. While service providers have taken measures to strengthen the security of their systems, there is still room for improvement. At the same time, it is likely that new security leaks will keep emerging in the future, and is unlikely that 100% security will ever be realized at all given the complexity of software applications at all levels of Internet services[20].

10. *Existing unsolved security problems of Internet services* add to risk of using social network services and may also in some cases raise the level of risk, or develop "flavours" specific to social network services. A recent position paper by the European Network and Information Security Agency (ENISA) inter alia lists SPAM, cross site scripting, viruses and worms, spear-phishing and social network-specific phishing,

infiltration of networks, profile-squatting and reputation slander through ID theft, stalking, bullying, and corporate espionage (i.e. social engineering attacks using social network services)[21]. According to ENISA, "social network aggregators" pose an additional security threat[22].

11. *The introduction of interoperability standards and application programming interfaces* (API; e.g. "open social" introduced by Google in November 2007) to make different social network services technically interoperable entails additional new risks: They allow for automatic evaluation of all social networks websites implementing this standard. The API delivers literally the entire functionality for automatic evaluation implemented in the web interface. Possible applications with potential repercussions on user privacy (and possibly also on the privacy of non-users whose data are part of a user profile) may include: Global analysis of (professional and private) user relationships, which may well cross "borders" between different networks where user act in different roles (e.g. professionally oriented vs. more leisureoriented networks). Interoperability may also further foster download and third-party re-use of profile information and photos, and creation of profiles about change histories of user profiles (including making available of information a user has deleted from his profile).

Guidance

Based on the above said, the Working Group makes the following (preliminary) recommendations to regulators, providers and users of social network services:

<u>*Regulators*</u>

1. *Introduce the option of a right to pseudonymous use – i.e. to act in a social network service under a pseudonym[23] –,* where not already part of the regulatory framework.

2. *Ensure that service providers are honest and clear about what information is required for the basic service so that users can make an informed choice whether to take up the service*, and that users can refuse any secondary uses (at least through opt-out), specifically for (targeted) marketing. Note that specific problems exist with consent of minors[24].

3. *Introduction of an obligation to data breach notification for social network services*. Users will only be able to deal especially with the growing risks of identity theft if they are notified of any data breach. At the same time, such a measure would help to get a better picture of how well companies secure user data, and provide a further incentive to further optimise their security measures.

4. *Re-thinking the current regulatory framework with respect to controllership* of (specifically third party-) personal data published on social networking sites, with a view to possibly attributing more responsibility for personal data content on social networking sites to social network service providers.

5. *Improve integration of privacy issues into the educational system.* As giving away personal data online becomes part of the daily life especially of young people, privacy and tools for informational self-protection must become part of school curricula.

<u>*Providers of social network services*</u>

Providers must have a vital self-interest in preserving security and privacy of personal data of their users. A failure to make swift progress in this field may result in loss of user confidence (which is already now considerably shaken by recent security and privacy incidents), and may well result in an economic backlash comparable to the crisis that hit the digital economy in the late 1990s.

1. *Transparent and open information of users* is one of the most important elements of any fair processing and use of personal information. While the need for such a mechanism is recognized in most national, regional and international regulatory instruments for

privacy, the present form in which many service providers inform their users may need to be revisited: At present – and in many cases in line with existing regulatory frameworks – privacy information form a part of sometimes complex and lengthy "terms and conditions" of a service provider. In addition, a privacy policy may be provided. Some service providers suggest that the percentage of users actually downloading this information is very low[25]. Even if this information is displayed on the screen when a user signs up to a service, and can also be accessed later if the user so wishes, the goal to inform users about potential consequences of their actions during the use of a service (e.g. when changing privacy settings for a collection of – say – pictures) may be better served by built-in, context-sensitive features, that would deliver the appropriate information based on user actions.

User information should specifically comprise information about the jurisdiction under which the service provider operates, about users' rights (e.g. to access, correction and deletion) with respect to their own personal data, and the business model applied for financing the service. Information must be tailored to the specific needs of the targeted audience (especially for minors) to allow them to make informed decisions.

Information of users should also refer to third party data: Providers of social network services should – on top of informing their users about the way they treat their (the users') personal data, also inform them about the do's and don'ts of how they (the users) may handle third party information contained in their profiles (e.g. when to obtain the data subjects' consent before publication, and about possible consequences of breaking the rules). Especially the huge quantities of photos in user profiles showing other people (in many cases even tagged with name and/or link to the other persons' user profile) are an issue in this context, as current practices are in many cases not in line with existing legal frameworks governing the right to control one's own image.

Candid information should also be given about remaining security risks, and possible consequences of publishing personal data in a profile, as well as about possible legal access by third parties (including also e.g. law enforcement, secret services).

2. *Introduce the creation and use of pseudonymous profiles as an option*, and encourage its use.

3. *Living up to promises made to users:* A *conditio sine qua non* for fostering and maintaining user trust is clear and unambiguous information about how their information will be treated by the service provider, specifically when it comes to sharing personal data with third parties. However, with some service providers there are at present ambiguities with respect to those promises. The most prominent example is the popular statement "we will never share your personal information with third parties" in relation to targeted advertising. While this statement may be formally correct in the eyes of the service provider, some providers fail to clearly communicate the fact that e.g. for displaying advertisements in the browser window of a user, the IP address of these users may be transmitted to another service provider delivering the content of the advertisement, in some cases based on information processed by the social network service provider from a users' profile. While the profile information itself may indeed not be transmitted to the advertisement provider, the users' IP address will[26] (if the social network provider does not e.g. use a proxy mechanism to hide the user IP address from the provider of the advertisement). The problem is that some providers of social network services erroneously assume that IP addresses are not personal data, while in most jurisdictions they in fact often are. Such ambiguities may mislead users and may spur an erosion of trust when users learn about what happens in reality, which is neither in the interest of the users, nor

in the interest of the service provider. Similar problems exist regarding the use of cookies.

4. *Privacy-friendly default settings* play a key role in protecting user privacy: It is known that only a minority of users signing up to a service will make any changes to default settings – including privacy settings. The challenge for service providers here is to choose settings that offer high degree of privacy by default without making the service unusable. At the same time, usability of setting features is key to encourage users to make their own changes. In any case, non-indexibility of profiles by search engines should be a default.

5. Improve user control over use of profile data:

   - *within the community*; e.g. allow restriction of visibility of entire profiles, and of data contained in profiles, as well as restriction of visibility in community search functions. Tagging of photos (i.e. the addition of links to an existing user profile or the naming of depicted persons) should be bound to the data subject's prior consent.

   - *create means allowing for user control over third party use of profile data* – vital to especially address risks of ID theft. However, there are at present only limited means to control information once it is published. The experience of the movie and music industries with digital rights management technologies suggests that possibilities may in this respect stay limited. Nevertheless, services providers should strengthen research activities in this domain: Existing and maybe promising approaches include research on the "semantic" or "policy-aware web[27]", encrypting user profiles, decentralise storage of user profiles (e.g. with users themselves), the use of watermarking technologies for photos, the use of graphics instead of text for displaying information, and the introduction of an expiration date to be set by users for their own profile data[28]. Service providers should also strive to discourage secondary use especially of pictures by offering a function allowing users to pseudonymise or even anonymise pictures[29]. They should also take effective measures to prevent spidering, bulk downloads (or bulk harvesting) of profile data. Specifically, user data should only crawled by (external) search engines if a user has given his explicit, prior and informed consent.

   - *Allow for user control over secondary use of profile and traffic data;* e.g. for marketing purposes, as a minimum: opt-out for general profile data, opt-in for sensitive profile data (e.g. political opinion, sexual orientation) and traffic data. Many existing legal frameworks contain binding rules on secondary uses for marketing purposes, which must be observed by providers of social network services. Consider letting users decide for themselves, which of their profile data (if any) they would like to be used for targeted marketing. In addition, the introduction of a fee should be considered as an additional option at the choice of the user for financing the service instead of use of profile data for marketing.

   - *Comply with user rights recognised in national, regional and international privacy frameworks* including the right of data subjects to have data – which may well be entire profiles – erased in a timely manner.

   - *Address the issues that may arise in cases of a takeover or merger of a social network service company*: Introduce guarantees for users that new owner will maintain present privacy (and security) standard.

6. *Appropriate complaint handling mechanisms* should be introduced (e.g. to "freeze" contested information, or pictures), where they do not already exist, for users of social networks, but also with respect to third party personal data. Timely response to data subjects is important. Measures may also include a penalty mechanism for abusive behaviour with

respect to profile data of other users and third party personal data (incl. removing users from site as appropriate).

7. *Improve and maintain security of information systems.* Use recognised best practices in planning, developing, and running social network service applications, including independent certification.

8. *Devise and/or further improve measures against illegal activities, such as spamming, and ID theft.*

9. *Offer encrypted connections for maintaining user profiles,* including secured log-in.

10. Social network providers acting in different countries or even globally should respect the privacy standards of the countries where they operate their services.

Users of social networks

1. *Be careful*. Think twice before publishing personal data (specifically name, address, or telephone number) in a social network profile. Think also about whether you would like to be confronted with information or pictures in a job application situation. Maintain your profile information. Learn from CEOs of big companies: These people know about the value of their personal information and control it. This is why you will not find a lot of personal information about them on the web.

2. *Think twice before using your real name in a profile*. Use a pseudonym instead. Note that even then you have only limited control over who can identify you, as third parties may be able to lift a pseudonym, especially based on pictures. Think of using different pseudonyms on different platforms.

3. *Respect the privacy of others*. Be especially careful with publishing personal information about others (including pictures or even tagged pictures), without that other person's consent. Note that illegal publication especially of pictures is a crime in many jurisdictions.

4. *Be informed*: Who operates the service? Under which jurisdiction? Is there an adequate regulatory framework for protecting privacy? Is there an independent oversight mechanism (like a Privacy Commissioner) that you can turn to in case of problems? Which guarantees does the service provider give with respect to handling your personal data? Has the service been certified by independent and trustworthy entities for good quality of privacy, and security? Use the web to educate yourself about other people's experience with the privacy and security practices of a service provider you do not know. Use existing information material from providers of social network services, but also from independent sources like Data Protection Agencies [30], and security companies[31].

5. *Use privacy friendly settings*. Restrict availability of information as much as possible, especially with respect to indexing by search engines.

6. *Use different identification data* (e.g. login and password) than those you use on other websites you visit (e.g. for your e-mail or bank account).

7. *Use opportunities to control* how a service provider uses your personal (profile and traffic) data. E.g. opt out of use for targeted marketing.

8. *Pay attention to the activity of your children in the Internet*, especially on social network websites.

Closing remark

The Working Party calls upon Consumer and Privacy Protection Organisations to take appropriate measures to raise awareness with regulators, service providers, the general public, and notably young people[32] about privacy risks regarding the use of social networks and responsible behaviour with respect to one' own personal data, as well as those of others.

The Working Group will closely monitor future developments with respect to the protection of privacy in social network services and revise and update this Guidance as necessary.

Notes

1. Quoted from Wikipedia at http://en.wikipedia.org/wiki/Social_network_service [viewed on 5 February 2008]

2. This report does not cover chat, blogging, and ranking sites.

3. A German researcher recently identified in a selection of popular social network services about 120 single personal attributes contained in user profiles in social network services, like for example age, home address, favourite movies, books, music etc., and also including political opinions and even sexual preferences. Cf. „Berliner Morgenpost" of 23 January 2008, S. 9: „Mehr Informationen als die Stasi"; http://www.morgenpost.de/content/2008/01/23/wissenschaft/942868.html (in German language)

4. A term attributed to Marc Prensky, a US speaker, writer, consultant, and game designer in education and learning. Cf. e.g. http://www.ascd.org/authors/ed_lead/el200512_prensky.html [viewed on 5 February 2008]

5. Already now, secret services from the United States (namely the "Open Source Center", a service attached to the US "Director of National Intelligence") seem to be using data from what is called "open sources", which seem to include inter alia YouTube, but also social media like Myspace, and blogs; cf. http://www.fas.org/blog/secrecy/2008/02/open_source_intelligence_advan.html [accessed 7 February 2008]

6. 6 While some service providers have tried to create limited areas within their services to give users more control over how they share their (personal) information, others make such information or parts thereof available to a bigger audience, which can in some cases be the entire community – and thus millions of perfect strangers: "it stays between us", yes, but "us" may well be 50 million+.

7. Cf. the statement of John Lawford from the Canadian Public Interest Advocacy Center in a speech given 3 October 2007 at the OECD-Canada Technology Foresight Forum "Confidence, privacy and security"; cf. http://www.stenotran.com/oecd/2007-10-03-Session4b.pdf [accessed 6 February 2008], p. 35

8. Cf. ENISA Position Paper No.1: "Security Issues and Recommendations for Online Social Networks", October 2007, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

9. Note that some social network services allow search engines to crawl user content, and that search engine services have emerged recently specialising in offering personal profiles drawn together from different sources. On the other hand, service providers seem to have at present little or no control over the actions of spiders on their websites who do not respect the "robots.txt" protocol.

10. "APRIL 26--A Pennsylvania woman claims that her teaching career has been derailed by college administrators who unfairly disciplined her over a MySpace photo that shows her wearing a pirate hat and drinking from a plastic cup. In a federal lawsuit, […] charges that Millersville University brass accused her of promoting underage drinking after they discovered her MySpace photo, which was captioned «Drunken Pirate». Quoted from http://www.thesmokinggun.com/archive/years/2007/0426072pirate1.html [accessed 11 February 2008]. Cf. also The Guardian, January 11, 2008: "Would-be students checked on Facebook"; http://education.guardian.co.uk/universityaccess/story/0,,2238962,00.html

11. Cf. e.g. "Employers Use «Facebook» and «MySpace» to Weed Out Applicants"; http://www.wtlv.com/tech/news/news-article.aspx?storyid=64453 [accessed 12 February 2008]. Finland seems to be the only country so far to ban such practices.

12. Other examples to emerge in the future may well include use by immigration authorities when travelling abroad.

13. Cf. e.g. "Facebook API Unilaterally Opts Users Into New Services", by Ryan Singel, 25 May 2007, http://blog.wired.com/27bstroke6/2007/05/facebook_api_un.html; cf. also Chris Soghoian: "Exclusive: The next Facebook privacy scandal", 23 January 2008, http://www.cnet.com/8301-13739_1-9854409-46.html?tag=blog.1 [accessed 12 February 2008]

14. Cf. as a telling example for instance the recent "Natalie"- and "frog-" experiments conducted by the Security company Sophos; cf. "Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves. Research highlights dangers of irresponsible behaviour on social networking sites", August 2007; http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html and "Der Fall 'Natalie'. Online Communities zunehmend IT-Sicherheits-Risiko. Experten warnen vor massivem Anstieg von Datendiebstahl und - missbrauch auf Social Network Websites", 21 January 2008 (in German language)

15. Cf. "Secret Crush Facebook App Installing Adware, Security Firm Charges", Wired of 3 January 2008, http://blog.wired.com/27bstroke6/2008/01/secret-crush-fa.html

16. Cf. "Phantom Photos: My photos have been replaced with those of another"; http://flickr.com/help/forum/33657/

17. Cf. e.g. the December 2006 "MySpace XSS QuickTime Worm"; http://www.websense.com/securitylabs/alerts/alert.php?AlertID=708

18. Cf. PC World: "Worm Hits Google's Orkut" of 19 December 2007, http://www.pcworld.com/article/id,140653-c,worms/article.html , and SC Magazine US: "Google's Orkut hit by self-propagating trojan" of 26. February 10 -

19. 2008, http://www.scmagazineus.com/Googles-Orkut-hit-by-self-propagating-trojan/article/107312/ [both accessed 3 March 2008] Cf. e.g. „Datenleck beim StudiVZ? [Update]"; http://www.heise.de/newsticker/meldung/81373/ (in German language)

20. In addition, the steep growth of information stored electronically every year is in itself seen as a security risk: At the last RSA Europe Security Conference in London in 2007, RSA president Art Coviello was cited saying that alone in 2006 176 exabytes of data had been generated worldwide, and that such a huge amount of data was in his view unmanageable, and could not be secured effectively; cf. the German Computer Magazine "iX", December 2007, p. 22 "Trübe Aussichten: Große Datenmengen verhindern Datensicherheit" (in German language); http://www.heise.de/kiosk/archiv/ix/2007/12/022/

21. Cf. ENISA Position Paper No.1: "Security Issues and Recommendations for Online Social Networks", October 2007, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

22. Cf. ENISA Position Paper No.1 (footnote 21 supra), p. 12

23. "Pseudonymous use" in this context means the right to act in a social network service under a pseudonym without having to reveal one's "true" identity to other users of the service, or to the general public, if the user wishes so. Depending on circumstances, this may well include having to reveal one's true identity vis-à-vis the provider of the social network when registering.

24. Cf. Working Paper "Children's' Privacy On Line: The Role of Parental Consent", adopted at the 31st meeting, Auckland (New Zealand), 26/27 March 2002; http://www.datenschutzberlin.de/attachments/205/child_en.pdf?1200656702

25. A representative from facebook stated recently at an OECD conference that the percentage of users visiting a privacy policy may not be more than a quarter of a percent; cf. http://www.stenotran.com/oecd/2007-10-03- Session4b.pdf p. 33f. [accessed 6 February 2008].

26. Depending on circumstances, the advertisement provider may even be able to reconstruct some or all of the underlying profile information based on the kind of targeted advertisement that is to be displayed to a specific user.

27. Cf. e.g. Daniel J. Weitzner, Jim Hendler, Tim Berners-Lee, Dan Connolly: "Creating a Policy-Aware Web: Discretionary, Rule-based Access for the World Wide Web". To appear in: Web and Information Security, E. Ferrari and B. Thuraisingham (eds), Idea Group Inc., Hershey, PA (forthcoming); http://www.w3.org/2004/09/Policy-Aware-Web-acl.pdf, and Sören Preibusch, Bettina Hoser, Seda Gürses, and Bettina Berendt: Ubiquitous social networks – opportunities and challenges for privacy-aware user modelling; http://vasarely.wiwi.hu-berlin.de/DM.UM07/Proceedings/05-Preibusch.pdf [both accessed 12 February 2008].

28. Cf. e.g. The Royal Academy of Engineering: Dilemmas of Privacy and Surveillance. Challenges of Technological Change. March 2007, at 7.2.1, p. 40

29. Cf. ENISA Position Paper No.1: "Security Issues and Recommendations for Online Social Networks", October 2007, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf, p.23

30. Cf. e.g. the brochure "when online gets out of line" jointly published by facebook and the Information and Privacy Commissioner of Ontario, Canada, at http://www.ipc.on.ca/images/Resources/up-facebook_ipc.pdf, the US Federal Trade Commission: "Social Networking Sites: A Parent's Guide" at http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec13.shtm and "Social Networking Sites: Safety Tips for Tweens and Teens" at http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec14.shtm

31. Cf. e.g. the model privacy settings proposed by Sophos for facebook; http://www.sophos.com/security/bestpractice/ facebook.html

32. Cf. e.g. the campaign „dubestemmer" launched by the Norwegian Data Protection Authority; http://www.dubestemmer.no/english.php, the "DADUS"-Project of the Portuguese Data Protection Authority; http://dadus.cnpd.pt, and the initiatives cited in footnote 30 above

International Working Group on Data Protection in Telecommunications Recommendation on the Implementation and Application of the Council of Europe Convention No. 185 on Cybercrime (a.k.a. "Budapest Convention")

43r[d] meeting, 3 – 4 March 2008, Rome (Italy)

Whereas the Budapest Convention of 2001 on cybercrime is a major international co-operation tool with a view to harmonizing criminal offences, investigation procedures, and judicial and police assistance;

Considering that several provisions of the Convention and the relevant Protocol as undersigned in 2003 impact directly on the processing of personal data, and that it is important for data protection principles to be taken into consideration in ratifying and implementing those provisions;

Considering that the provisions of the Convention do not apply exclusively to cybercrime, but also to the collection of evidence in electronic format for whatever type of offence, whether committed by means of a computer system or not; considering that certain decisions made at domestic level in ratifying the Convention produce effects on international co-operation as well, especially with regard to mutual assistance procedures;

Considering that some criticalities in this sector have already been pointed out in the preparatory work to the Convention, inter alia by this Working Group , and by the Article 29 Working Party (Opinion no. 4/2001 rendered on 22 March 2001);

Considering that several countries have undersigned the Convention, and twenty-two of them have already ratified it;

RECOMMENDS

That special attention be paid to all the implications for the processing of personal data and the safeguards applying to citizens' rights in any instruments ratifying the Convention and the relevant Protocol, or in connection with the concrete implementation thereof by the competent investigational bodies, in particular with a view to the following:

1. ***(Proportionality)*** The principle of proportionality, as set out in several articles of the Convention, should be abided by in all criminal investigation activities performed by the competent law enforcement bodies (e.g. inspections, searches, seizure, custody, urgent inquiries, search for evidence) whenever the evidence is to be gathered on and/or by means of electronic tools;

   Cf. "Common Position on data protection aspects in the Draft Convention on cyber-crime of the Council of Europe" (Berlin, 13/14.09.2000); http://www.datenschutz-berlin.de/attachments/218/cy_en.pdf

2. ***(Safeguards for Third Parties' Rights)*** Whenever the said investigations activities are carried out, their impact on the rights vested in third parties that are alien to the facts investigated upon should always be assessed with the utmost care;

3. ***(Corporate Liability for Employees' Criminal Offences)*** As regards implementation of the provisions in the Convention related to corporate liability (article 12), which envisage the liability of legal persons employing individuals that are held liable for the criminal offences established in accordance with the Convention, consideration should be given to applying the respective punishments also if the criminal offences in question are established under domestic legislation on personal data protection;

4. ***("Freezing" of Traffic Data)*** The instruments implementing the provisions set out in the Convention with regard to the expedited preservation of stored computer data and the partial disclosure of traffic data (articles 16 and 17) should be applied on the basis of the careful assessment of purpose limitation and proportionality principles as well as in accordance with a selective

approach, by also taking account of the safeguards partially laid down by the countries that envisage traffic data retention for law enforcement purposes;

5. ***(Countries' Jurisdiction in Investigating and Detecting Criminal Offences)*** In order to afford enhanced protection to cybercrime victims, ratification of the Convention and/or any subsequent regulatory amendments, especially at domestic level, should provide an opportunity for updating domestic law, in particular the provisions contained in criminal codes and/or criminal procedure codes, so as to expand the scope of national jurisdiction in prosecuting these offences, which might go unpunished if the conventional standards underlying criminal jurisdiction (type of conduct, facts, etc.) were applied.

The Working Group recognises the special importance of international co-operation in this area and reserves the right to undertake further initiatives in order to foster exchanges of information, monitoring of the appropriate application of the Convention and its Protocol, and the widest possible harmonization of regulatory approaches and implementing practices.

Le collège :
Pierre WEIMERSKIRCH, Gérard LOMMEL et Thierry LALLEMANG

L'administration et le service juridique :
Marc MOSTERT, Serge FERBER, Thomas FRERES, Marc KINTGEN,
Michel SINNER, Georges WEILAND et Christian WELTER
(de gauche à droite)

Commission Nationale
pour la Protection
des Données

41, avenue de la gare, L-1611 Luxembourg
Siège : L-4100 Esch-sur-Alzette
téléphone : +352 26 10 60 -1 - Fax : +352 26 10 60 - 29

www.cnpd.lu