Commission Nationale pour la Protection des Données

Rapport Annuel 2009

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 notifi és ;
- 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 aux mesures réglementaires ou administratives concernant le traitement de données personnelles;
- 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'orientations thématiques.

Table des matières

ANNEXES :

Avis et décisions

Participations aux travaux européens

1 Avant-propos

Veiller à l'application des lois qui protègent la vie privée et les données à caractère personnel des citoyens, telle est la mission de la Commission nationale pour la protection des données.

Ainsi, 2009 a été une année d'activité intense, marquée notamment par le rôle de chef de file de la Commission nationale dans l'examen conjoint par les autorités de plusieurs pays européens de la charte « BCR » du groupe eBay. Ces « Binding Corporate Rules » garantissent que la protection dont bénéficient les utilisateurs et employés de l'entreprise multinationale dans les États de l'Union européenne continue à s'appliquer lorsque les données les concernant sont transférées en dehors de ces pays. Nous avons pu faire aboutir la procédure d'adoption dans un temps record à la satisfaction du groupe et de nos confrères en Europe.

La Commission nationale a par ailleurs pris position sur un certain nombre de dossiers importants comme l'« identifiant unique » et l'accès de la police à des fichiers d'administrations publiques. Son avis de 2007 sur l'article 28 de la loi sur le bail à usage d'habitation est redevenu actuel en 2009 avec la réalisation de l'enquête de la Ville de Luxembourg en matière de logement.

Au cours de l'année, elle a continué d'accompagner les projets ayant un impact sur la protection de la vie privée des citoyens : « chèque-service accueil », e-Government, e-Santé, e-Go, coopérations entre administrations, Integrated Biobank of Luxembourg (IBBL), …

L'année 2009 a aussi été marquée par les investigations dans le secteur des télécommunications, un secteur « sensible » dans lequel la confidentialité des informations communiquées doit être rigoureusement respectée.

Dans le cadre de sa mission d'information et de guidance, la Commission nationale a participé à plusieurs événements visant à sensibiliser les citoyens et surtout les jeunes aux enjeux de la protection des données, un sujet qui lui tient tout particulièrement à cœur.

Tout au long de l'année, le site web de la Commission nationale s'est efforcé de constituer une source privilégiée d'informations concernant les sujets qui ont dominés l'actualité comme la vidéosurveillance dans les lieux publics, « Google Street View », le dossier « SWIFT » ou encore Facebook et les réseaux sociaux.

Comme tous les ans, la Commission nationale a activement participé aux travaux européens. Plusieurs documents ont pu être publiés grâce aux coopérations au niveau européen et international avec notamment un avis sur les réseaux sociaux en ligne et une réponse conjointe à la consultation lancée par la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel (« L'avenir de la protection de la vie privée »).

Le thème de la protection des données personnelles est de plus en plus présent dans notre quotidien : la surveillance sur le lieu de travail, les relations avec les autorités publiques, l'utilisation des réseaux sociaux sur Internet, la géolocalisation etc. Tous ces actes impliquent la collecte de données et d'informations personnelles et alimentent des fichiers de plus en plus grands. C'est le rôle de la Commission nationale d'encadrer et de limiter cette collecte.

Ce rôle est d'autant plus important dans un monde où les technologies se développent de plus en plus rapidement. Des nouveaux sites, aussi innovants soient-ils, voient le jour sur la toile quotidiennement. La plupart d'entre eux fonctionnent selon le même principe : ils proposent leurs produits ou services gratuitement et assurent leurs revenus par la publicité. Les données et les besoins des utilisateurs sont analysés afin de leur proposer des publicités de plus en plus ciblées. Les citoyens, souvent sans en avoir conscience, délivrent en masse des informations sur leurs coordonnées, leur famille, leur personnalité, leurs activités et leurs intérêts.

La question à laquelle il faudra répondre dans les prochaines années est celle de savoir comment il est possible de rendre compatible le recours à ces technologies de plus en plus incontournables avec la maîtrise pour l'utilisateur de ses données personnelles. Il s'agit là d'un grand défi pour tous ceux qui ont à cœur de préserver le respect de la sphère privée. En 2010 et pendant les années suivantes, les collaborateurs de la Commission nationale, renforcés par trois nouveaux juristes assermentés en 2009, devront faire face à ce défi posé par les nouvelles technologies et la mondialisation.

***

Luxembourg, le 31 août 2010

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

2 Les activités en 2009

Plusieurs domaines d'activités ont marqué le travail de la Commission nationale au courant de l'année 2009 :

- Le conseil et la guidance des acteurs publics et privés ;
- La supervision du respect de la loi avec notamment la régularisation et l'encadrement d'un nombre important de traitements « sensibles » soumis à autorisation préalable ;
- Les initiatives d'information et de communication, traduites par la poursuite des efforts de sensibilisation, et ce aussi bien du grand public que des milieux professionnels et publics ;
- Les activités internationales et en particulier 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 et renforcé sa politique de dialogue et de concertation avec les instances publiques et privées. À côté de son rôle plus général qui est de conseiller les pouvoirs publics au sujet de l'application des principes de la protection des données, la Commission nationale a également mis son empreinte sur des projets plus spécifiques touchant un secteur précis ou sur des projets concrets poursuivis par un département ministériel.

Pour le suivi de différents dossiers, elle était en contact avec divers ministères, administrations et organismes publics. Citons le Ministère de la Santé avec lequel la Commission nationale était en rapport à propos de l' « Integrated Biobank of Luxembourg (IBBL) » et de la mise en œuvre du plan national « e-santé ». D'autres ministères ont eu des conseils de la part de la Commission nationale, notamment le Ministère de la Famille et de l'Intégration concernant les « chèques-service-accueil » ou encore le Ministère de l'Éducation nationale et de la Formation professionnelle quant au service « eRestauration » (restauration scolaire - Restopolis).

Elle est régulièrement intervenue, comme les années précédentes, dans les travaux du Comité National d'Éthique de Recherche (CNER) et du Comité National pour la Simplification Administrative en faveur des Entreprises (CNSAE), et a fourni de multiples recommandations au cours de ces travaux.

Le nombre de réunions avec les acteurs du secteur public (54 contre 52 l'année précédente) s'est ainsi maintenu à un niveau élevé. En parallèle, les rencontres avec le secteur privé ont augmenté par rapport à l'année 2008 (52 contre 42 l'année précédente). Ces entrevues avec les représentations d'importantes entreprises privées nationales et multinationales et leurs organisations représentatives (du secteur financier notamment) traduisent l'accent mis sur les efforts de promotion des bonnes pratiques et d'une guidance constructive.

2.1.2 Demandes de renseignements

Les demandes de renseignements adressées à la Commission nationale se chiffrent à 1711 pour l'année 2009 contre 1892 requêtes enregistrées en 2008. Le nombre total reste donc à un niveau élevé mais stable, avec environ 1400 demandes de renseignements par téléphone.

Dans un souci d'optimisation continue des délais et de la qualité des réponses, la Commission nationale s'efforce d'améliorer constamment le traitement des demandes de renseignements, en particulier en ce qui concerne la rapidité et la précision des réponses données.

2.2 Supervision de l'application de la loi

2.2.1 Formalités préalables

2.2.1.1 Notifications préalables et autorisations

Généralités

Avant qu'un traitement de données ne puisse être mis en œuvre, il doit être notifié à la Commission nationale. L'utilité de cette formalité déclarative consiste d'une part à assurer à l'autorité compétente une vision des réalités sur le terrain, d'autre part à permettre au public de consulter la liste des traitements déclarés, dans un but de transparence. Les traitements déclarés

peuvent être consultés dans le registre public sur le site Internet de la Commission nationale (à l'adresse www.cnpd.lu).

Il y a toutefois deux cas où le principe de la notification préalable ne s'applique pas :

- soit que le traitement est particulièrement sensible et nécessite des garanties supplémentaires (définies par la loi même : autorisation préalable par la Commission nationale ou par règlement grand-ducal),
- soit que le traitement ne doit pas être notifié (du fait que le traitement est « anodin » ou qu'il est couvert par d'autres garanties).

Dans les deux cas, les traitements en question sont expressément et limitativement énumérés par la loi modifiée du 2 août 2002 sur la protection des données.

Les formalités préalables en chiffres

En 2009, on peut constater que le nombre des demandes d'autorisation préalables et des notifications préalables est resté plus ou moins stable par rapport à l'année précédente. 542 demandes d'autorisation ont été reçues en 2009 contre 606 en 2008. La plupart des demandes d'autorisation émanent d'organismes ou de particuliers souhaitant installer des systèmes de vidéosurveillance. Toutefois, le nombre de demandes concernant la surveillance de l'utilisation de l'outil informatique ou encore celle des trajets en voiture de service (géolocalisation) a également augmenté en 2009. Quant aux notifications préalables, leur nombre est passé de 385 à 345.

Le nombre des engagements formels de conformité a, quant à lui, baissé. Les élections sociales de 2008 sont une des raisons de cette baisse. À cette occasion, nombre d'organismes avaient introduit ou renouvelé leur engagement formel de conformité par rapport à la décision unique prise par la Commission nationale à cet effet en vue d'alléger la charge administrative des entreprises. 942 engagements formels avaient été reçus en 2008. Une année plus tard, 227 organismes se sont encore conformés à la décision unique de la Commission nationale.

Aux 542 demandes d'autorisation « individuelles » introduites en 2009, il faut encore ajouter 70 engagements formels de conformité introduits par rapport à des autorisations générales conditionnelles. Ces « autorisations uniques » sont conférées par la Commission nationale pour certains traitements fréquents ayant une même finalité, portant sur des catégories de données identiques et ayant les mêmes destinataires (en l'occurrence, la surveillance électronique des horaires de travail ainsi que le contrôle électronique et non-biométrique des accès). Le nombre d'engagements formels a toutefois également baissé par rapport à l'année 2008, quand la Commission nationale en avait reçu 220.

Au total, on peut donc constater que le nombre de démarches de formalités préalables imposées aux organismes souhaitant traiter des données à caractère personnel a diminué par rapport à l'année précédente et est passé de 2.153 à 1.184 traitements déclarés / régularisés en 2009.

Le retard dans la prise en charge des notifications a été rattrapé et l'examen des demandes d'autorisation a pu être optimisé. Toutefois, le résidu n'est pas encore tout à fait absorbé. Il faut souligner qu'une standardisation dans l'examen des dossiers est souvent difficile à réaliser, car les critères de licéité, de légitimité, de finalité, de nécessité et de proportionnalité doivent être appréciés au cas par cas et en fonction des circonstances et du contexte particulier de chaque demande. La Commission nationale ne cesse d'adapter au mieux son mode de fonctionnement dans le double but d'accélérer le traitement des formalités préalables et de simplifier les démarches administratives pour les responsables de traitements de données.

Le nombre total de traitements de données déclarés à la Commission nationale, figurant dans le registre public (consultable en ligne sur le site Internet www.cnpd.lu), dépasse désormais les 13.000.

Le nombre total de dossiers introduits depuis 2003 s'établit à 15.234 avec 4.772 déclarants / responsables ayant procédé à des formalités préalables (contre 4.357 fin 2008).

2.2.1.2 Dispositifs d'alerte professionnelle

Les dispositifs d'alerte professionnelle dits « whistleblowing » mises en place au sein des entreprises sont de plus en plus fréquents. Dans certains secteurs, ils correspondent à une exigence légale ou réglementaire. Tel est en particulier le cas des sociétés cotées en bourse aux États-Unis (en application de la célèbre loi « Sarbanes-Oxley »). Ils permettent aux employés de signaler le comportement de leurs collègues de travail, supposé contraire à la loi ou aux règles établies par l'entreprise. La Commission nationale a publié une note de synthèse des règles à respecter par les entreprises luxembourgeoises souhaitant procéder à un tel traitement de données. Les conditions et restrictions avancées par la CNPD s'inspirent largement des recommandations émises par le Groupe « Article 29 » dans son avis n° 1/2006 du 1er février 2006 (document de travail WP 117).

Une demande d'autorisation préalable n'est pas requise mais la mise en place d'un tel dispositif doit être déclarée à la Commission nationale par une notification sur base de l'article 12 de la loi modifiée du 2 août 2002.

Ces règles visent à limiter le rôle que les entreprises peuvent attribuer à un tel dispositif d'alerte et les circonstances susceptibles d'en faire un traitement de données à caractère personnel déloyal, car opéré à l'insu des personnes concernées et visant l'instauration d'un climat de suspicion et de délation généralisé au moyen du whistleblowing. Celui-ci doit être conçu comme un mécanisme additionnel et subsidiaire pour rapporter des dysfonctionnements internes via un support spécifique et non en tant que dispositif se substituant aux procédures régissant les rapports hiérarchiques et de relations de travail au sein de l'entreprise. Les dispositifs d'alerte professionnelle ne doivent pas remplacer les auditeurs internes ou le contrôle de qualité du personnel. La balance des intérêts entre proportionnalité, subsidiarité et fiabilité des faits dénoncés est une nécessité fondamentale. Finalement, les recommandations émises à l'attention des entreprises peuvent être résumées en quatre points :

- La nécessité de restreindre le dispositif d'alerte aux domaines comptable, bancaire, du contrôle des comptes, et de la lutte contre la corruption ;
- Le fait de décourager les dénonciations anonymes en assurant, dans la mesure du possible, l'identification des auteurs d'alerte ;
- La mise en place d'une organisation spécifique pour recueillir et traiter les alertes. Les personnes chargées du dispositif d'alerte doivent être formées et astreintes à une obligation de confidentialité quant aux données dont elles prennent connaissance ;
- L'information de la personne concernée dès que les preuves ont été préservées, afin de lui permettre d'exercer ses droits d'opposition, d'accès et de rectification.

L'orientation suivie en la matière est similaire à celle appliquée par nos collègues français et belges.

2.2.1.3 Les chargés de la protection des données

Suite à la modification de la loi en 2007, les organisations, entreprises, administrations, associations et institutions ont désormais la possibilité de désigner une personne salariée comme chargé de la protection des données. Jusque là cette fonction était réservée à des personnes externes. Le responsable de traitement est alors dispensé du devoir de notifier ses traitements auprès de la Commission nationale. La désignation ne dispense pas pour autant ce dernier d'introduire des demandes pour des traitements soumis à autorisation préalable. Le chargé, de son côté, a la mission de surveiller la conformité des traitements de données mis en œuvre et doit tenir à jour un registre qu'il communique à la CNPD tous les quatre mois. En 2009, le nombre de chargés de la protection des données désignés a connu un léger tassement.

Les personnes pressenties à remplir cette fonction doivent au préalable obtenir l'agrément de la Commission nationale et font, par après, l'objet d'une désignation par le responsable du traitement. Dans un effort de simplification des démarches administratives, la Commission nationale a élaboré un nouveau formulaire permettant d'introduire simultanément la demande d'agrément et la désignation d'une personne salariée. Chaque année, le chargé doit en outre parfaire ses connaissances en matière de protection des données et en référer à la Commission nationale.

Lors du séminaire annuel de l'association française AFCPD (Association française des correspondants à la protection des données à caractère personnel), le Président de la Commission nationale a eu l'occasion de présenter l'expérience luxembourgeoise des chargés internes désignés par des entreprises, organisations et organismes publics luxembourgeois. Plus d'une demi-douzaine de chargés de la protection des données luxembourgeois ont d'ailleurs participé à cette conférence avec participation internationale à laquelle ont assisté plus de 150 délégués de la protection des données.

Dans le contexte de l'application aux grandes et moyennes organisations et entreprises du principe d' « accountability » tel que commenté par le groupe « Article 29 » dans son avis du 13 juillet 2010 (WP 173), le rôle de ces correspondants internes « Protection des Données » est appelé à prendre de l'importance.

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

La libre circulation des données à caractère personnel dans les 27 pays membres de l'Union européenne est assurée par les dispositions de la Directive 95/46/CE du 24 octobre 1995, pour autant que ces dernières soient rigoureusement respectées. Ladite directive a instauré une sorte de « sphère de sécurité » en matière de protection des données, sachant que tous les pays de l'Espace économique européen (l'Union européenne, l'Islande, le Liechtenstein et la Norvège) ont transposé la directive en droit national. Les législations de ces pays garantissent ainsi un même niveau élevé de protection des personnes concernées.

L'article 25 de la directive prévoit que le transfert vers un pays tiers ne peut en principe avoir lieu que si ce dernier assure un niveau de protection adéquat équivalent à celui instauré par la directive. Dès que des données à caractère personnel sont appelées à sortir de la « sphère de sécurité » européenne, il est indispensable que le destinataire des données exportées offre des garanties suffisantes en matière de protection de la vie privée et des libertés et droits fondamentaux des personnes. Ces garanties peuvent résulter de clauses contractuelles appropriées. Par contre, le caractère adéquat de la législation d'un pays non-membre de l'Union européenne est apprécié par la Commission européenne, qui a établi une liste avec les pays offrant un niveau de protection adéquat. Aux États-Unis d'Amérique, seules les entreprises ayant volontairement adhéré aux accords « Safe Harbor » (négociés entre le « Department of Commerce » et l'Union européenne) peuvent librement recevoir des données personnelles à partir de l'Europe.

Ainsi, l'examen préalable par la Commission nationale est-il obligatoire pour un transfert de données du Luxembourg vers un pays tiers n'assurant pas un niveau de protection adéquat si le responsable de traitement ne peut invoquer une des dérogations légales (consentement de la personne concernée, nécessité pour l'exécution d'un contrat conclu dans l'intérêt de la personne concernée, intérêt public important,…) prévues à l'article 19 (1) de la loi modifiée du 2 août 2002. Il est ainsi garanti que les données exportées bénéficient chez leur destinataire en dehors de l'Union européenne des mêmes garanties que dans la « sphère de sécurité » instaurée par la directive dans les 27 États membres.

En 2009, la Commission nationale a été saisie de 17 demandes d'autorisation ayant pour objet des transferts de données vers des pays sans protection adéquate, chiffre resté stable depuis 2007.

2.2.1.5 Approbation de règles contraignantes d'entreprise

Les « règles contraignantes d'entreprise » (en anglais : Binding Corporate Rules - BCRs) constituent une alternative à la conclusion de contrats bilatéraux (basés sur des clauses contractuelles types élaborées par la Commission européenne) pour rendre possible des transferts de données vers des pays hors Union européenne n'assurant pas un niveau de protection adéquat. De telles règles, adoptées (volontairement) par la maison-mère d'un groupe d'entreprises multinationale, constituent des garanties suffisantes exigées par la directive et évitent aux entités de ce dernier de devoir conclure une multitude de contrats pour chaque type de flux de données et pour chaque entité concernée. Contrairement aux contrats basés sur les clauses contractuelles types qui sont des instruments juridiques fixes et immuables, les BCRs sont rédigées

par les entreprises elles-mêmes selon leurs besoins et constituent souvent pour les multinationales un moyen plus flexible et plus adapté à la culture d'entreprise et dès lors plus « viable ».

Il s'agit en quelque sorte d'une « charte de la protection des données à caractère personnel » dont un groupe d'entreprises peut se doter et dont il rend le respect obligatoire pour chaque membre du groupe. Par ce biais, des garanties suffisantes en matière de protection des données sont offertes pour transférer des données à caractère personnel d'une entité établie dans un État membre de l'Union européenne vers d'autres entités d'un même groupe établies dans des pays n'offrant pas un niveau de protection adéquat. De telles règles contraignantes doivent prévoir la gestion des plaintes liées au traitement de données personnelles et, le cas échéant, l'indemnisation des personnes concernées ayant subi un préjudice suite à une violation des principes de la protection des données par une entité située hors Union européenne.

En juin 2003, le Groupe des autorités européennes de protection des données (« Groupe Article 29 » ou « G29 ») a publié un premier document de travail introduisant le concept des BCRs. Ses efforts sont dirigés vers les groupes multinationaux du monde industriel et commercial pour lesquels plusieurs documents de référence et pratiques supplémentaires ont été publiés entre 2004 et 2009. Ces documents précisent le contenu obligatoire des BCRs pour être reconnues comme apportant les garanties suffisantes en termes de protection des libertés et droits fondamentaux des personnes concernées et guident les multinationales en leur proposant une sorte de modèle afin d'établir la structure de base des règles à élaborer. Un recueil de questions fréquemment posées (« FAQ ») complète les documents élaborés par le G29.

Des réunions régulières du sous-groupe « BCRs » du Groupe Article 29 à Bruxelles ont permis aux autorités nationales d'échanger leurs expériences et en même temps de concrétiser le concept des règles contraignantes d'entreprise. Grâce aux compétences acquises en général et dans ce sous-groupe, les autorités européennes de la protection des données ont réussi à réduire la durée de la phase d'approbation, notamment grâce à des déclarations de reconnaissance mutuelle des décisions des autorités nationales.

Les collaborateurs de la Commission nationale se sont largement investis dans ce groupe de travail, convaincus que les règles contraignantes d'entreprise constituent une simplification importante et un outil à la fois pratique, concret et efficace pour instaurer une « culture de la protection des données » au sein des multinationales. Elle a 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.

En 2009, la Commission nationale s'est vue reconnaître, en application de la procédure de coopération entre commissaires des différents États membres, le rôle de chef de file pour la validation des BCRs du groupe eBay (développé au chapitre 3.1 du présent rapport). Elle a également été impliquée dans l'analyse de deux chartes soumises à l'examen et à l'approbation des différentes autorités de protection de données des États membres.

L'économie luxembourgeoise comprend un nombre relativement important d'entreprises ayant une activité internationale ou du moins qui ont des relations commerciales avec des entreprises situées en dehors de l'Union européenne. La participation active de la CNPD dans le sous-groupe « BCRs » du G29, ainsi que son implication dans des procédures de coopération européennes pour l'approbation de BCRs a apporté sans doute une augmentation du « know-how » en la matière au fil des dernières années. La Commission nationale est persuadée que sa gestion efficace du dossier eBay s'inscrit favorablement dans la promotion du Luxembourg comme site d'activité pour des entreprises faisant appel à des technologies informatiques avancées ou étant actives dans le commerce en ligne.

2.2.2 Demandes de vérification de licéité et plaintes

Le nombre de plaintes et demandes de vérification de licéité a connu une nette augmentation avec 133 dossiers en 2009 contre 63 en 2008.

Le traitement des réclamations par les personnes concernées et des demandes relatives à leurs droits est une des missions de la Commission nationale. Si une demande d'accès aux données, d'effacement ou de rectification, adressée directement à l'administration,

l'entreprise, l'association, le professionnel ou l'indépendant est restée sans suite (ou si une telle réclamation s'avère difficile, voire impossible compte tenu des circonstances), les citoyens peuvent s'adresser à la Commission nationale.

Un certain nombre de demandes tendaient à obtenir le soutien de la Commission nationale pour imposer le droit d'accès aux données des administrés ou clients, respectivement l'effacement des données après la fin des relations.

De plus, l'installation illégale de systèmes de vidéosurveillance a donné lieu à des objections de la part de salariés estimant que leur patron n'a pas le droit de les filmer ou encore de locataires s'opposant aux prises de vue des escaliers et des couloirs par leurs propriétaires.

À côté des exemples mentionnés ci-dessus, d'autres types de traitements de données ont provoqué des objections de citoyens ou d'organisations, à savoir la communication non autorisée de données à des tiers, l'utilisation de données à des fins de prospection ou de marketing direct ou encore l'installation illégale de systèmes de géolocalisation sur le lieu de travail.

Dans des situations semblables, la Commission nationale peut même être amenée à prendre des sanctions administratives en vue d'interdire un traitement de données. En cas de non-respect de la loi, elle est également susceptible d'ordonner la suppression de données et de saisir le procureur d'État. Des peines pourront être prononcées en cas d'infraction.

2.2.3 Contrôles et investigations

La loi modifiée du 2 août 2002 attribue à la Commission nationale un pouvoir d'investigation grâce auquel elle peut recueillir toutes les informations nécessaires à l'accomplissement de sa mission de contrôle. Pour cette raison, elle dispose d'un accès direct aux locaux autres que les locaux où a lieu le traitement ainsi qu'aux données faisant l'objet du traitement, et procède aux vérifications utiles.

Les investigations de la Commission nationale sont menées en vue de vérifier le respect des obligations légales suite à des plaintes ou des demandes de vérification de licéité d'un traitement.

Il est à relever que la Commission nationale a procédé à des actions d'investigation aussi bien dans le cadre d'initiatives coordonnées au niveau européen par le Groupe « Article 29 » que de sa propre initiative. Ces dernières sont, soit liées à un dossier de plainte ou de vérification ponctuelle de licéité, soit à une initiative *in tempo non suspecto* menée à des fins dissuasives et pédagogiques et rendue publique (Exemple : secteur des télécommunications mobiles). En général, la Commission nationale se concentre tous les deux ans sur un chantier d'investigation de taille, dans un domaine déterminé, qui donne lieu à des traitements de données d'envergure ou particulièrement sensibles.

2.3 Information du public

2.3.1 Actions de sensibilisation du public

Dans le cadre de sa mission d'information et de guidance, la Commission nationale a mené un certain nombre d'actions visant à sensibiliser le grand public à la protection de la vie privée et des données personnelles et à informer les organisations, entreprises et organismes publics des droits reconnus aux personnes dont les données sont traitées.

La « Journée européenne de la protection des données », initiée en 2007 par le Conseil de l'Europe avec l'appui de la Commission européenne, a été une bonne occasion de rappeler à travers toute l'Europe l'importance du respect de la vie privée et de la protection des données personnelles. L'année dernière a eu lieu la troisième édition de cette journée qui est célébrée annuellement le 28 janvier, date-anniversaire de l'ouverture à la signature en 1981 de la « Convention 108 de Strasbourg ». 41 pays ont, à ce jour, adhéré à cette Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, dont le Luxembourg était un des premiers signataires.

La Commission nationale a mis à profit cette journée pour déployer une campagne d'annonces publiées dans la presse écrite et sur Internet, accompagnée d'un communiqué de presse, qui a suscité une série d'articles de presse et d'interviews de son Président sur des questions d'actualité.

Souvent, les citoyens ne sont pas suffisamment conscients des risques inhérents aux traces et informations laissées sur Internet et que d'autres utilisateurs peuvent enregistrer, utiliser à leur insu et communiquer à des tiers, voire revendre ces informations sans leur consentement. La Commission nationale a ainsi saisi cette opportunité pour rendre attentifs les acteurs publics et privés au fait que la loi limite la collecte et la conservation des renseignements à caractère personnel.

La Commission nationale a également participé aux « Safer Internet Day » organisé par le réseau LuSI (Luxembourg Safer Internet) en février 2009. Ce programme, subventionné par la Commission européenne, a comme objectif de promouvoir un usage plus sûr de l'Internet et des moyens de communication auprès des jeunes, des parents et des éducateurs. La CNPD a contribué à ce projet avec une conférence-débat au sujet de « la protection des données sur Internet ». L'objectif était de sensibiliser les internautes aux règles s'appliquant sur « la Toile » et de les informer sur leurs droits concernant leurs données personnelles (Plus d'informations à ce sujet dans la partie 3.8. Sensibilisation aux risques sur Internet).

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

En 2009, la Commission nationale et le thème de la protection des données ont été mentionnés 128 fois par la presse nationale, contre 72 fois en 2008.

La panoplie des thèmes évoqués a été très vaste avec une large couverture de la présentation du rapport annuel de l'année 2008 et de la journée européenne de la protection des données. D'autres sujets avaient trait à la vidéosurveillance dans les lieux publics, « Google Street View » ou encore les dossiers européens, comme l'accord passé avec les États-Unis pour l'accès aux données du réseau SWIFT dans le cadre de la lutte contre le financement du terrorisme (TFTP).

En outre, la Commission nationale est ponctuellement intervenue dans les médias audiovisuels par la voie de son Président ou de celle d'un de ses membres effectifs pour expliquer sa position sur différents sujets relatifs à la protection des données.

2.3.3 Outil de communication : le site Internet

Le site Internet vise à informer, conseiller et guider l'internaute souhaitant se renseigner sur le thème de la protection des données. Accessible à travers l'adresse www.cnpd.lu, il constitue le vecteur de communication privilégié de la Commission nationale avec le public.

Une des vocations du site web est d'offrir aux citoyens et au public en général une information de base sur la protection des données et des explications sur l'étendue et les possibilités de mise en œuvre de leurs droits en la matière dans des rubriques spécifiques. Dans la partie « Actualités », la Commission nationale informe ses visiteurs de manière permanente et continue sur les sujets d'actualité en matière de protection des données sur les plans national, européen et international.

Pour les lecteurs avertis, conseillers et responsables d'entreprises, le site propose une documentation juridique approfondie et des dossiers thématiques avec des liens facilitant les recherches sur les sujets importants. En outre, le site constitue 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, le recours au site web pour effectuer les formalités administratives a pris davantage d'importance ces dernières années. Grâce au formulaire électronique, les formalités de notification peuvent être remplies quasiment en un clic. 48% des notifications ont été remplies en ligne par ce biais en 2009. Afin de simplifier encore plus l'accomplissement rapide des démarches administratives, la Commission nationale a adopté la signature électronique dans ses formulaires. Avec l'utilisation du certificat Luxtrust, il est dorénavant possible de signer directement les formulaires de notification par voie électronique au lieu et place d'une signature manuscrite sur papier.

2.3.4 Formations et conférences

En 2009, la Commission nationale a participé à 23 séances d'information et conférences contre 11 en 2008. Afin d'exposer et d'expliquer par des exemples pratiques le cadre légal de la protection des données personnelles, elle est intervenue lors de formations dédiées et de séminaires destinés à un public averti ou

aux professionnels d'un secteur déterminé. Elle a ainsi effectué des présentations sur ce sujet auprès de la CFL (Société nationale des chemins de fer luxembourgeois), de l'INAP (Institut national d'administration publique) et du Conseil de Presse. À l'occasion de la conférence européenne des ordres et organismes assimilés des praticiens de l'art dentaire, la Commission nationale a donné une présentation intitulée « La libre transmission des données et la problématique de la protection des données personnelles des praticiens ». Ces exposés et conférences publics constituent une alternative à la presse pour présenter les enjeux de la protection des données à un public plus spécialisé.

Par ailleurs, répondant à l'initiative du Commissariat aux étrangers (Ministère de la Famille), elle a assisté à un déjeuner-débat autour du thème « Mesurer les diversités tout en respectant la protection de la vie privée» avec des représentants d'organismes actifs dans le domaine de la recherche et des études statistiques et sociales ainsi que de la lutte contre les discriminations. C'était l'occasion d'échanger des expériences en matière de collecte et d'analyse de données statistiques dans le domaine social et de la population. Un point de discussion a porté sur les problèmes éventuels rencontrés quand il s'agit d'analyser les différences de conditions de vie réelles et ressenties entre résidents luxembourgeois et communautés étrangères d'origines diverses. Les représentants de la CNPD ont exposé, ensemble avec le Président de la CNIL, M. Alex Türk, les bonnes pratiques dans le cadre de la protection des données relatives à l'origine raciale et ethnique et aux croyances religieuses. Le Président en exercice du Groupe Article 29 a démontré que le respect des principes de la protection des données ne s'avère nullement incompatible avec les besoins d'une analyse plus approfondie des diversités et des facteurs susceptibles d'engendrer des discriminations ou un traitement inégalitaire.

Participant à un séminaire organisé en parallèle à l'Assemblée générale annuelle de l'association française AFCPD (Association française des correspondants à la protection des données à caractère personnel) devant plus de 150 experts de la protection des données, le Président de la Commission nationale a eu l'occasion de présenter l'expérience luxembourgeoise des chargés de la protection des données. Une demi-douzaine de chargés luxembourgeois avaient fait le voyage à Paris et se sont montrés très intéressés par les activités de l'association française et celle de ses homologues allemands GED, néerlandais et britanniques également représentés lors de cette rencontre.

Depuis 2007, la Commission nationale intervient dans le cadre de la formation « Management de la Sécurité des Systèmes d'Information » (MSSI) à l'Université du Luxembourg. Les objectifs de cette formation consistent à sensibiliser les responsables de la sécurité des systèmes d'information aux aspects de la protection des données à caractère personnel.

Outre les formations et conférences précitées, il y a lieu de relever l'intervention de la Commission nationale lors des « Rencontres Européennes de Luxembourg » à l'Abbaye de Neumünster sur le sujet « Traçage, fichage, profilage : Internet, les nouvelles technologies de l'information et de la communication et la protection de la vie privée ». Dans sa présentation, le Président de la Commission nationale a évoqué deux aspects frappants dans l'évolution de la société numérique face aux enjeux de la sauvegarde des libertés et du droit au respect de la vie privée : l'importance prise par le profilage, d'une part, et par les risques particuliers inhérents à l'Internet, d'autre part.

Enfin, la Commission nationale a participé au « Safer Internet Day » en février avec une conférence-débat sur la protection des données sur Internet. Cet événement, organisé par le réseau LuSI (Luxembourg Safer Internet) et subventionné par la Commission européenne, a comme objectif de promouvoir un usage plus sûr de l'Internet et des nouveaux moyens de communication auprès des jeunes, des parents et des éducateurs.

2.4 Avis et recommandations

La Commission nationale a émis six avis en 2009 :

- Avis relatif aux mesures à prendre par les établissements bancaires en ce qui concerne les transactions personnelles effectuées par leurs salariés (Délibération n° 21/2009 du 30 janvier 2009) ;
- Avis concernant 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 (Délibération n° 48/2009 du 10 mars 2009 / Voir partie 3.4. pour plus d'informations à ce sujet) ;

- Avis concernant l'avant-projet de règlement grand-ducal instituant le « chèque-service accueil » (Délibération n° 49/2009 du 16 janvier 2009) ;
- Avis au sujet du projet de loi n°5986 relatif à l'accès des autorités judiciaires, de la Police et de l'Inspection générale de la Police à certains traitements des données à caractère personnel mis en œuvre par 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 (Délibération n° 63/2009 du 3 avril 2009 / Voir partie 3.6. pour plus d'informations à ce sujet) ;
- Avis relatif au projet de règlement grand-ducal relatif à la coopération interadministrative entre l'Administration de l'Enregistrement et des Domaines et l'Administration des Douanes et Accises (Délibération n° 187/2009 du 19 juin 2009) ;
- Avis de la Commission nationale pour la protection des données concernant le projet de loi n°6072 portant approbation d'un certain nombre de conventions bilatérales de non-double imposition et prévoyant la procédure applicable à l'échange de renseignements sur demande en matière fiscale (Délibération n° 410/2009 du 20 novembre 2009).

L'intégralité de ces avis est reproduite dans les annexes du présent rapport.

2.5 Participation aux travaux européens

En 2009, la Commission nationale a participé comme par le passé 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 autorités nationales européennes ainsi que le Contrôleur européen à la protection des données (CEPD). Dans ce cadre, la Commission nationale a participé aux sous-groupes suivants :
  - « Technologies » ;
  - « Police et justice » ;
  - « Règles contraignantes d'entreprise » ;
  - « Flux internationaux de données » ;
- Du Comité consultatif de la Convention 108 du Conseil de l'Europe (T-PD) ;
- 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 ») ;

Ainsi, la Commission nationale, représentée par un ou par plusieurs de ses membres, a assisté à plus de 30 réunions de travail sur le plan international. Ces réunions se démarquent souvent par un niveau élevé de technicité et nécessitent par conséquent une préparation approfondie et un suivi régulier des matières traitées.

Par ailleurs, les membres de l'autorité de contrôle de l'article 17 (dont deux membres de la CNPD) ont participé en alternance aux réunions des autorités conjointes de contrôle européennes d'Europol, du système d'information « Schengen » et des autorités douanières.

De plus, la Commission nationale a été présente aux conférences suivantes sur le plan international :

- 31ème conférence internationale des commissaires à la protection des données et de la vie privée ;
- Spring Conference (Edinburgh) ;
- Data Retention Conference (Bruxelles) ;
- 5ème Assises du Correspondant Informatique et Libertés sur le thème « Délégué à la protection des données à caractère personnel : bilan comparé

et prospective» (avec la présence d'Alex Türk, Président de la CNIL et du Groupe « Article 29 », et de Gérard Lommel, Président de la CNPD).

2.5.1 Le groupe « Article 29 »

Le groupe de travail, institué par l'article 29 de la Directive 95/46/CE sur la protection des données, est un organe consultatif indépendant, dont l'objectif est d'examiner les questions relatives à la protection des données et de contribuer à l'application harmonisée de ladite directive dans les 27 États membres de l'Union européenne.

Au cours de l'exercice 2009, ce groupe a émis plusieurs avis à l'adresse de la Commission européenne et a adopté un certain nombre de documents de travail. Parmi ces problématiques, relevons celles qui ont plus particulièrement retenu l'attention du groupe.

La protection des données en rapport avec les nouvelles technologies constitue un des thèmes centraux du programme de travail du groupe. Cette préoccupation résulte en partie du développement des réseaux sociaux en ligne et de leur utilisation par les enfants et adolescents. L'avis relatif à ce sujet est développé au point 2.5.1.1 du présent rapport.

Le groupe « Article 29 » a également publié un document de travail sur la procédure d'échange d'informations avant le procès (« pre-trial discovery ») dans le cadre de procédures transfrontalières. Supposant que la Directive 95/46/CE sur la protection des données ne soit pas appliquée de la même manière dans les différents États membres en raison de la diversité des approches de la procédure civile, le groupe a adopté ce document pour rendre attentif à la manière dont doivent être traitées les demandes de transfert de données à caractère personnel vers un autre État en vue de leur utilisation dans une procédure civile.

À la demande de la Commission européenne, le groupe « Article 29 » s'est prononcé sur les propositions modifiant la Directive 2002/58/CE (transposée au Luxembourg par la loi modifiée du 30 mai 2005). Complétant les deux prises de position antérieures du groupe, cet avis a comme objectif principal d'améliorer la protection des données personnelles et la vie privée des individus dans le secteur des communications électroniques, notamment en exigeant des fournisseurs de services de communication de notifier les violations de sécurité.

Le groupe de travail a en outre rendu un avis favorable concernant le projet de décision de la Commission européenne relatif aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants de données établis dans des pays tiers. Étant donné que de plus en plus d'entreprises transfèrent leurs données non seulement vers des sous-traitants, mais également vers des « sous-sous-traitants », voire des sous-traitants de troisième niveau, les clauses contractuelles types nécessitent une mise à jour pour faire face à la complexité de ces transferts subséquents.

Le groupe « Article 29 » a aussi été consulté par la Commission européenne pour donner son avis sur le standard international pour la protection des renseignements personnels de l'Agence mondiale antidopage (AMA). Suite au premier avis du groupe de travail publié en 2008, certaines adaptations ont été apportées au standard de l'AMA. Le groupe de travail a néanmoins regretté que toutes ses observations n'ont pas été prises en compte et passe en revue dans son second avis les points qui continuent à poser problème.

Il a encore élaboré une réponse à la consultation lancée par la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel. Pour plus de détail à ce sujet, se reporter au point 2.5.1.2 du présent rapport.

La liste complète avec les références des avis et documents de travail adoptés en 2009 par le groupe « Article 29 » et par les différents sous-groupes figure en annexe.

2.5.1.1 Le sous-groupe « Technologies »

Suite aux travaux du sous-groupe « Technologies », le groupe de travail « Article 29 » a adopté le 12 juin 2009 un avis sur les réseaux sociaux donnant des indications aux fournisseurs de tels services quant aux mesures à mettre en place afin de garantir le respect du droit communautaire.

Les réseaux sociaux ont connu au cours de ces dernières

années un essor considérable, le nombre d'utilisateurs ayant augmenté de façon exponentielle. L'intérêt pour ces sites, offrant des services innovants et permettant d'interagir, de communiquer ou de partager des informations, images ou vidéos avec d'autres internautes, ne cesse d'augmenter.

De ce fait, les échanges de données à caractère personnel sur Internet se sont multipliés. Une fois en ligne et rendues publiques, les informations communiquées peuvent être largement diffusées, indexées et analysées. En contrepartie de l'utilisation gratuite du service par les internautes, les fournisseurs des sites constituent souvent des fichiers contenant une multitude d'informations, pouvant être utilisées à des fins publicitaires ou commerciales. La publication de données personnelles peut ainsi avoir des effets indésirables tels que le vol d'identité, la perte d'emploi ou l'atteinte à l'intégrité physique.

Afin de protéger au maximum les données des utilisateurs, le groupe recommande aux réseaux sociaux d'offrir aux internautes un niveau approprié de sécurité et de proposer des paramètres par défaut respectueux de la vie privée. Plus particulièrement, il préconise que l'accès au profil d'un utilisateur devrait être limité aux contacts qu'il a sélectionnés dès l'inscription au service.

En outre, le groupe demande aux fournisseurs de réseaux sociaux d'être plus transparents quant à l'utilisation des données des utilisateurs. Une attention particulière doit aussi être accordée au traitement des données à caractère personnel des mineurs. Les utilisateurs, à leur tour, devraient éviter de mettre en ligne des photos d'autres personnes sans le consentement de celles-ci.

Le groupe de travail complète le présent avis en abordant les problématiques du traitement de données sensibles, de la publicité et de la conservation des données en relation avec les réseaux sociaux.

2.5.1.2 Le sous- groupe « Police et justice »

En collaboration avec le sous-groupe « Police et justice » (WPPJ – Working Party on Police and Justice), le groupe « Article 29 » a élaboré une réponse conjointe à la consultation lancée par la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel (« L'avenir de la protection de la vie privée »).

Cette consultation a comme objectif de recueillir des éléments de réflexion pour déterminer si le cadre juridique actuel répond aux besoins et de définir quelles mesures devraient être prises à l'avenir pour relever les défis identifiés.

Une des principales conclusions ressortant de cet avis est que les principes essentiels de la protection des données restent valables en dépit des nouvelles technologies et de la mondialisation. Les groupes constatent également qu'une amélioration du niveau de protection des données et de la vie privée serait possible grâce à une meilleure application des principes actuels de la protection des données dans la pratique.

Selon les deux groupes, il serait opportun de saisir cette occasion pour effectuer des modifications législatives. Dans le cadre d'une telle révision, il serait pertinent de préciser certains principes clés en matière de protection de données (ex : consentement, transparence) et d'intégrer de nouveaux concepts dans le cadre actuel, notamment la « prise en compte du respect de la vie privée dès la conception » et la « responsabilité ».

Une modernisation des dispositions de la Directive 95/46/CE permettrait en outre de prendre les mesures nécessaires pour réduire la charge administrative.

Enfin, les groupes recommandent d'insérer les principes fondamentaux de la protection des données dans un cadre juridique global, qui s'applique également à la coopération policière et judiciaire en matière pénale.

2.5.2 Comité consultatif de la Convention 108 du Conseil de l'Europe (T-PD)

La Commission nationale participe régulièrement aux travaux du Comité consultatif de la Convention STE N° 108 du Conseil de l'Europe sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

Dans le domaine de la protection des données, cette convention de 1981 constitue le premier instrument international juridiquement contraignant à vocation universelle. Celle-ci a largement inspiré la législation adoptée en la matière par l'Union européenne.

41 pays dont le Luxembourg ont à ce jour adhéré à cette « Convention de Strasbourg », fondée sur l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (Rome, 4 novembre 1950).

Le Comité consultatif (T-PD) est constitué de représentants des États ayant signé la Convention, d'observateurs d'autres États (membres et non membres) et d'experts scientifiques. Il émet des recommandations et publie des analyses et avis qui sont une référence pour tous les États signataires de la Convention.

Faisant suite à un rapport d'expertise présenté par les professeurs Yves Poullet et Jean-Marc Dinant du CRID de l'Université de Namur, le T-PD a élaboré une recommandation sur le profilage. La première lecture de ce projet a été adoptée en septembre 2009. Dans ce cadre, le Comité consultatif avait invité les acteurs intéressés du secteur privé, ainsi que les associations, à exposer leurs commentaires concernant la réglementation sur les activités de profilage. L'objectif est de trouver un équilibre entre la protection des données et les intérêts légitimes pouvant justifier des activités de profilage.

Le T-PD a par ailleurs formulé des observations concernant la « proposition conjointe pour un projet de standards internationaux sur la protection de la vie privée à l'égard du traitement des données à caractère personnel » (résolution approuvée lors de la 31ème conférence internationale des commissaires à la protection des données et de la vie privée à Madrid). Dans ses commentaires, le T-PD a d'ailleurs félicité cette tentative de procéder à une mise à jour des principes applicables et a noté que la Convention 108 et son protocole ont le potentiel d'avoir une vocation universelle.

Le programme de travail du T-PD pour 2009 et les années à venir est reproduit en annexe du présent rapport. Les priorités du T-PD concernent les amendements à la Convention 108 ainsi que l'élaboration de recommandations. D'autres travaux portent sur le statut des autorités de contrôle de protection des données et sur le phénomène des réseaux sociaux en ligne.

2.5.3 Groupe de travail international sur la protection des données dans les télécommunications (Le « groupe de Berlin »)

Le « groupe de Berlin » a mis l'accent sur les problèmes relatifs aux télécommunications et médias lors de ses réunions biannuelles.

Dans un document de travail portant sur la réutilisation de comptes e-mails, le groupe s'est penché sur la question de ce qui se passe si l'utilisateur change de domaine (« *E-mail heritage: What happens when the user moves to a different domain?* »).

En quelques années, le courrier électronique est devenu un des moyens de communication les plus répandus. Simplicité, facilité d'utilisation, rapidité et gratuité ne sont que quelques raisons pour lesquelles l'e-mail est actuellement l'outil principal pour envoyer des messages privés ou professionnels.

Après fermeture ou changement d'un compte e-mail par un utilisateur, une autre personne peut se voir attribuer la même adresse. Dans une grande entreprise, par exemple, on peut imaginer qu'un employé reçoit une adresse qui auparavant appartenait à une autre personne avec le même nom. Cette situation risque également de se présenter lorsqu'un client change de fournisseur d'Internet sans avoir la possibilité de garder son adresse. Dans les cas précités, une nouvelle personne est susceptible de recevoir des messages personnels destinés à l'ancien titulaire de l'adresse e-mail.

Ce document de travail analyse donc surtout les risques en matière de vie privée qu'encourent les internautes en changeant ou résiliant leur adresse e-mail. Ne se limitant pas aux comptes e-mail, cette problématique s'étend également aux comptes de réseaux sociaux, aux services de téléphonie sur Internet et de messagerie instantanée et même aux numéros de téléphone portable. Sont concernés en particulier, les services où l'utilisateur a besoin de son adresse e-mail pour s'identifier.

Le groupe a adopté un deuxième document portant sur la protection des données en relation avec les déchets électroniques (« Recommandation on Data Protection and E-Waste »). Il préconise que les pouvoirs publics doivent prendre, en coopération avec les autorités

de protection des données, les mesures nécessaires pour prévenir l'accès non autorisé aux données à caractère personnel enregistrées sur les équipements électroniques, destinés à être détruits ou recyclés.

Finalement, un rapport traitant du sujet des systèmes de péage à grande échelle utilisant des données à caractère personnel a été adopté. Afin de protéger la vie privée des chauffeurs et propriétaires de voitures, le groupe a émis plusieurs recommandations (« *Report and Guidance on Road Pricing – Sofia Memorandum* ») concernant cette problématique.

2.5.4 Le séminaire biannuel européen « Case Handling Workshop »

Aux mois de mars et octobre 2009, la Commission nationale a participé aux rencontres biannuelles des représentants des autorités de protection des données européennes consacrées aux expériences dans le traitement de cas pratiques « Case Handling Workshop » qui ont eu lieu respectivement à Prague (République tchèque) et à Limassol (Chypre).

Lors de ces ateliers, beaucoup de sujets variés ont été abordés. Il y a lieu de relever les suivants :

- médias et vie privée ;
- traitements des données des salariés : Whistleblowing, systèmes d'accès biométriques, tests de dépistage d'alcool et de drogue, géolocalisation ;
- données traitées dans le secteur de la santé : dossier patient électronique, prescription médicale électronique ;
- Internet : responsabilité des publications sur les sites Internet, les dangers pour les jeunes, spam ;
- les droits que peuvent exercer les citoyens, en particulier le droit à l'information et le droit d'accès aux données ;
- secteur bancaire et financier : fichiers centraux sur les crédits, agence de crédit, scoring ;
- vidéosurveillance dans les lieux privés et publics.

L'importance des échanges d'expériences basées sur des plaintes et cas pratiques et la discussion des questions techniques, spécifiques à des situations particulières dans des domaines bien précis, complètent de façon heureuse les travaux plus académiques et institutionnels qui se déroulent au niveau du Groupe Article 29. Dans les années à venir, ces concertations de « brain storming » autour de cas pratiques sont appelées à prendre encore de l'ampleur.

3 Les temps forts de 2009

Les travaux de la Commission nationale ont été marqués par l'émergence d'un certain nombre de dossiers, soit dictée par le contexte institutionnel et l'actualité, soit choisie 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 Feu vert pour la charte « BCR » du groupe eBay

Une collaboration constructive entre le groupe eBay et la CNPD

Fin mai 2008, le groupe eBay s'est mis en rapport avec la Commission nationale pour la première fois au sujet de l'élaboration de « Binding Corporate Rules » (« BCRs »). Un « kickoff-meeting » avec le « Chief Privacy Officer » d'eBay, Monsieur Scott Shipman et le cabinet d'avocats Allen&Overy Luxembourg, a débouché en octobre 2008 à la soumission d'une toute première ébauche de règles contraignantes d'entreprise par le groupe. Suite à l'analyse de la charte par la CNPD, une nouvelle entrevue a eu lieu peu de temps après. Conformément aux bonnes pratiques en matière de coopération entre autorités européennes de la protection des données, ce premier « draft » a ensuite été revu par la Commission de l'Informatique et des Libertés (CNIL) en France. Après une troisième réunion début janvier 2009, le groupe a soumis une seconde version améliorée des BCRs tenant compte des commentaires de la CNPD et ceux de la CNIL.

Après une nouvelle revue du dossier par la CNPD, deux entrevues et une conférence téléphonique supplémentaire, le groupe eBay était finalement prêt, en février 2009, à introduire sa demande officielle d'approbation de ses règles contraignantes d'entreprise. Ce n'est qu'après cette période de préparation et de collaboration intensive entre eBay et la Commission nationale qu'a pu être entamée la procédure de coopération officielle entre les différentes autorités nationales de contrôle concernées (voir ci-dessous sous-chapitre intitulé « La Commission nationale comme autorité de chef de file »).

La charte élaborée définit les règles applicables au traitement de données personnelles par les entités du groupe eBay en cas de transfert en dehors de l'Union européenne. Plus particulièrement, les règles contraignantes d'entreprise visent à garantir que la protection dont bénéficient les individus dans les 14 États membres de l'Union européenne où eBay est implanté continue à s'appliquer lorsque les informations sont transférées en dehors de ces pays.

Soucieux de protéger les informations personnelles concernant ses employés et les utilisateurs de ses services, le groupe eBay a décidé d'adopter volontairement cette charte BCR qui doit être respectée par toutes ses entités.

Une solution adaptée à la culture d'entreprise

Contrairement aux contrats sur la base de clauses contractuelles types élaborées par la Commission européenne et aux accords « Safe Harbor » (qui ne vise que les transferts vers certaines sociétés aux États-Unis), ces règles internes reflètent directement l'activité du groupe par lequel elles ont été élaborées. En ce qui concerne eBay, les règles contraignantes d'entreprise ont été adaptées spécifiquement aux types de données utilisées par le groupe concernant ses utilisateurs et ses employés.

Pour plus de détails concernant cet instrument juridique se prêtant aux entreprises multinationales, se reporter au chapitre 2.2.1.5 du présent rapport.

La Commission nationale comme autorité de chef de file

Les sociétés eBay et PayPal offrent l'ensemble de leurs services européens à partir du Luxembourg. Les utilisateurs européens de ces services sont donc des clients de la filiale « eBay Europe sàrl » établie et ayant son siège à Luxembourg. Par ailleurs, c'est également la filiale luxembourgeoise qui tranche la plupart des questions en matière de protection des données. Pour ces raisons, la multinationale a choisi la Commission nationale comme autorité de chef de file (« lead authority »), conformément à la procédure applicable en la matière. C'est pour la première fois que l'autorité luxembourgeoise se voit attribuer ce rôle important.

Après l'acceptation de son rôle de « lead authority » par les autorités nationales de contrôle des 13 autres pays européens où le groupe est implanté, la CNPD était chargée de la coordination de la procédure d'approbation

entre les autorités nationales impliquées dans le dossier et le groupe eBay. Les autorités nationales des pays suivants ont participé à la procédure de coopération : Royaume-Uni, France, Allemagne, Pays-Bas, Italie, Irlande, Espagne, République tchèque, Danemark, Pologne, Estonie, Belgique et Suède.

Elle a ainsi effectué une analyse en profondeur des règles appliquées au sein du groupe eBay de façon à ce qu'elles soient conformes aux standards ambitieux de la législation européenne et aux exigences des pays concernés.

Champ d'application des règles contraignantes d'entreprise

La charte BCR concerne quelque 200 sociétés, succursales et filiales du groupe eBay à travers le monde.

Elle s'applique tant aux renseignements sur les clients/utilisateurs des plateformes et services (essentiellement sur Internet) qu'aux informations sur les salariés collectées et transmises par le groupe.

La charte BCR revêt une portée importante pour ce groupe dont l'activité principale est le commerce en ligne, notamment par un système de vente aux enchères mondialement connu. Avec plus de 90 millions d'utilisateurs actifs au monde, eBay représente la plus grande place de marché sur Internet. À ceci s'ajoutent plus de 81 millions de personnes enregistrées auprès du service PayPal faisant également partie du groupe eBay. La société luxembourgeoise « PayPal (Europe) sàrl et Cie SCA » est un établissement bancaire soumis à la loi du 5 avril 1993 relative au secteur financier et au contrôle de la CSSF (Commission de surveillance du secteur financier). PayPal permet aux internautes, disposant d'une adresse de courrier électronique, d'effectuer des transactions en ligne sans avoir à communiquer leurs données financières aux vendeurs. Au début des négociations, Skype appartenait encore au groupe eBay et les BCRs devaient également s'appliquer à ses sociétés. Néanmoins, cette branche, offrant des services de communication tels que la téléphonie via Internet, a été vendue quelques semaines avant l'aboutissement de la procédure et ne fait désormais plus partie des entités du groupe eBay. Les BCRs du groupe ne sont dès lors pas applicables à Skype.

Mesures organisationnelles prises par le groupe eBay

Le groupe eBay a pris des mesures efficaces au niveau de son organisation afin de garantir le respect des règles prévues dans les BCRs. Tout d'abord, les directions générales de toutes les entités du groupe ont été impliquées en signant une déclaration d'adhésion à la charte, rendant juridiquement contraignant les règles dans la pratique quotidienne. Le groupe eBay a ensuite mis en place un réseau de chargés à la protection des données au niveau de toutes les sociétés affiliées. Cette équipe (« privacy team ») intervient aussi bien dans la formation et la sensibilisation du personnel que dans la gestion des plaintes et des demandes de vérification. Le recours périodique à des audits effectués par des experts externes ou internes est un moyen organisationnel supplémentaire que s'est imposé le groupe pour assurer le respect des principes de la protection des données de ses utilisateurs et employés.

À côté de l'examen du texte des règles contraignantes d'entreprise, la Commission nationale est, en tant qu'autorité de chef de file, chargée de contrôler également si le groupe eBay met effectivement en œuvre les mesures organisationnelles mentionnées ci-dessus.

Coopération constructive et procédure d'approbation rapide

Après son analyse finale de la charte, la Commission nationale a annoncé l'approbation des BCRs d'eBay dans sa délibération du 11 novembre 2009. La plupart des autorités de protection des données des 13 autres pays européens où le groupe est implanté ont fait connaître leur décision de reconnaissance mutuelle (« mutual recognition ») et se sont ralliées d'emblée à la décision de la Commission nationale. Elles n'ont dès lors pas procédé à un examen détaillé du dossier pour délivrer l'autorisation requise pour les données transférées à partir de leur pays. Quelques autorités nationales impliquées dont le Danemark, l'Estonie, la Belgique et l'Italie ont fait part de leurs commentaires à la CNPD qui, de son côté, s'est empressée à les communiquer à la direction du groupe eBay. Leurs remarques concernaient principalement les six points suivants : délai de gestion des plaintes, subordination du droit de saisir la juridiction compétente au fait

d'avoir épuisé le système de gestion des plaintes, droit de la personne à s'adresser directement à l'autorité nationale compétente, juridiction compétente, transfert de données vers des sous-traitants (externes et internes au groupe) et niveau de détail des données traitées/transférées.

Tous ces points ont pu être clarifiés avec la direction du groupe et ont, par la suite, été pris en considération dans le texte final de la charte.

La durée de la procédure d'approbation s'est limitée à 10 mois, durée totale très courte si on considère que cette phase de coopération entre autorités de protection des données européennes dépasse généralement la durée d'un ou deux ans. Les BCRs du groupe eBay ont pu être approuvées si rapidement grâce à un rythme de travail soutenu et une coopération efficace entre toutes les parties impliquées.

Dans un climat constructif de négociation, eBay Luxembourg a agi comme tête de pont pour l'ensemble des entités européennes du groupe. L'approbation des règles contraignantes d'entreprise d'eBay n'aurait par ailleurs pas été possible sans la participation active du Chief Privacy Officer d'eBay, Scott Shipman, et le cabinet d'avocats Allen&Overy Luxembourg, ainsi que la collaboration constructive des 13 autres autorités de protection des données impliquées dans la procédure.

Suivi permanent de la Commission nationale

L'approbation des BCRs d'eBay ne met cependant pas fin au travail de la Commission nationale concernant ce dossier. En tant que « lead authority », le suivi des activités d'eBay par l'autorité luxembourgeoise est permanent. Le fonctionnement efficace du système de gestion des plaintes et le contrôle de la mise en œuvre correcte des mesures organisationnelles prévues dans la charte reviennent ainsi à la Commission nationale.

Parallèlement à la procédure d'approbation, des demandes de vérification de la part d'utilisateurs d'eBay ou de PayPal ont déjà amené la Commission nationale à contacter le groupe, notamment dans des cas où des utilisateurs ont effacé leur compte mais auquel il était toujours possible d'accéder.

En général, n'importe quel utilisateur ou employé, quel que soit son pays de résidence au sein de l'Union européenne, peut rendre responsable eBay Luxembourg en cas de violation des règles fixées par les BCRs. Les personnes concernées peuvent s'adresser directement à la Commission nationale, aux juridictions luxembourgeoises ou à l'autorité de protection des données de leur pays en vue de réclamer le respect des règles et le cas échéant une indemnisation pour un préjudice subi.

Au cours des semaines et mois suivant l'introduction des règles contraignantes d'entreprise, les employés des différentes sociétés du groupe eBay ont été informés des changements induits par la nouvelle charte à laquelle ils devront se conformer dans l'exécution de leurs tâches quotidiennes. Les procédures internes ont été adaptées à ce nouveau cadre applicable, à travers le monde, aux informations personnelles concernant les clients/utilisateurs et les salariés des entités européennes.

3.2 L'affaire « Google Street View »

La fonctionnalité « Street View » de Google, module complémentaire au service de cartographie « Maps », a connu une très grande popularité depuis son lancement en 2007. Une vue dynamique à 360° permet aux internautes de visualiser des images panoramiques en ligne et de naviguer virtuellement dans les rues et localités photographiées par les véhicules de l'entreprise américaine.

L'internaute peut ainsi compléter la cartographie classique par des photos détaillées des rues et bâtiments d'une localité recherchée pour découvrir à l'avance des destinations futures, préparer ses vacances ou voyages professionnels ou satisfaire sa curiosité touristique de façon virtuelle. Si au début « Street View » était seulement disponible pour cinq villes américaines, le service s'est développé rapidement et des clichés d'une douzaine de pays en Amérique du Nord, Europe et Asie sont désormais consultables sur Internet.

À ce jour, « Street View » a déjà collecté des images des villes et des axes de circulation d'une partie importante du globe à l'aide de ses véhicules dotés d'appareils de prises de vues panoramiques. Ces voitures « Google » sont même parfois suppléées par des vélos permettant de photographier des zones difficilement accessibles telles que les pistes cyclables, chemins de promenade ou campus d'université.

Toutefois, le degré de détail des clichés soulève des questions concernant les atteintes potentielles à la vie privée des personnes concernées. À l'échelle internationale, le service a suscité une vive polémique depuis sa création. Des réserves ont été émises tant par des citoyens que par les autorités de protection des données de nombreux pays.

Deux problèmes principaux ont été soulevés : d'abord, le risque général d'intrusion dans la vie privée d'une personne par la publication photographique détaillée de son habitation privée avec ses environs (pouvant par exemple servir à planifier des cambriolages) ; puis, le risque plus spécifique de capter accidentellement l'image de personnes se trouvant dans une « situation embarrassante ».

La presse a rapporté de nombreux cas où les prises d'images ont eu une incidence directe sur la vie privée des citoyens et l'entreprise américaine a déjà été assignée en justice plusieurs fois à propos de son service, que ce soit par des particuliers estimant que leur vie privée a été violée ou par des autorités de protection des données.

M. Hanspeter Thür, chargé fédéral suisse de la protection des données, a demandé à Google d'appliquer des critères plus stricts lors du traitement et du stockage des données, notamment en exigeant une amélioration au niveau de l'anonymisation des images. Considérant que Google n'a pas respecté les recommandations helvétiques et que « Street View » n'est pas conforme à la loi suisse sur la protection des données, M. Thür a saisi le tribunal fédéral administratif pour statuer sur la question.

Plus concrètement, la Suisse s'est inquiétée du floutage insuffisant des visages et plaques d'immatriculation ainsi que de la hauteur des caméras permettant de voir au-dessus des murs et des haies. Toutefois, un accord a pu être trouvé mi-décembre : aucune nouvelle photographie prise en Suisse ne pouvait être mise en ligne avant la décision du Tribunal administratif fédéral. Google restait cependant autorisé à poursuivre ses prises de vues et à exploiter les images déjà prises. Par ailleurs, l'entreprise américaine a entre-temps publié une liste avec les localités où elle procèdera à des prises de vues pour son site.

En Grèce, le service « Street View » a même été interdit par l'autorité en charge de la protection des données, qui a exigé plus de garanties en matière de protection de la vie privée. Au Japon, le service de Google a également suscité une vive polémique. Les prises de vues ont dû être renouvelées entièrement suite à de nombreuses plaintes. Dans les 12 villes déjà filmées, on a vu apparaître des clôtures et des jardins d'habitations privées, un scandale pour les Japonais très sensibles à la préservation de leur intimité.

Avant de procéder à des prises de vues au Luxembourg, Google a contacté la Commission nationale en automne 2008 en vue de se conformer aux pré-requis luxembourgeois en la matière. La firme américaine a ainsi introduit en février 2009 une notification des traitements des données conformément aux articles 12 et 13 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 - suivant en cela la position commune adoptée en février 2009 par les autorités de protection des données d'une trentaine de pays – a estimé que les prises de vue et la mise en ligne des images en soi ne sont pas contraires à la législation luxembourgeoise en la matière. Néanmoins, Google devrait mettre en place des mesures de sauvegarde adéquates pour respecter les droits des personnes concernées et les autres règles légales.

Les conditions à respecter par Google ont été précisées en détail dans la réponse de Monsieur le Ministre des Communications et des Médias François Biltgen à la question parlementaire posée par Monsieur le Député Gilles Roth en date du 11 septembre 2009 :

- *« Annonce publique préalable des périodes de prises de vues avec indication des principales localités concernées ;*
- *« Floutage » soigneux des images préalablement à la mise en ligne sur Internet en vue d'éviter que des personnes ou leurs voitures n'apparaissent de façon à pouvoir être identifiées ;*
- *Instauration d'une procédure simple et gratuite permettant à tout un chacun de signaler des images où l'anonymisation des personnes ou*

d'objets pouvant être mis en relation avec elles n'étant pas suffisante ou sur lesquelles des situations gênantes sont en outre visibles ;

- *Retrait ou retouchage approprié de telles images rapidement après leur signalement à Google ;*
- *Respect du droit d'opposition des personnes concernées dans les conditions prévues par la loi ;*
- *Abstention de toute commercialisation ou transmission des images à des tiers ou de tout usage autre que pour le service « Street View » ;*
- *Garantie de la confidentialité et de la sécurité des données à caractère personnel dans toute la chaîne de production (des prises de vues à la mise en ligne sur Internet) et durée de la conservation des images brutes (non encore retouchées, anonymisées) limitée au strict nécessaire. »*

Le droit d'opposition contre l'utilisation et la publication d'enregistrements (sous quelle forme que ce soit) portant sur un bâtiment, une habitation ou un terrain doit être exercé directement auprès du responsable de traitement, à savoir la société Google. Cette dernière n'ayant pas d'établissement au Luxembourg, les demandes doivent être adressées à un avocat représentant la société au Grand-Duché.

La Commission nationale a mis une lettre-type à disposition des personnes concernées afin de faciliter les démarches pour faire valoir leur droit d'opposition. Celle-ci est disponible sur le site de la Commission nationale (www.cnpd.lu) et peut directement être adressée à Google. L'autorité nationale de protection des données intervient seulement en cas de non-respect des droits reconnus aux personnes concernées.

En mai 2009, la Commission nationale s'est vu obligée de suspendre les prises de vue au Luxembourg pour « Street View » : elles étaient considérées comme illicites tant que certains des pré-requis n'étaient pas remplis. Même si la Commission nationale avait reçu de Google un certain nombre d'assurances concernant les conditions évoquées ci-dessus par Monsieur le Ministre des Communications, quelques points restaient encore à régulariser.

En particulier, la Commission nationale avait demandé à Google de faire connaître à l'avance au public luxembourgeois les périodes exactes pendant lesquelles les prises de vues étaient prévues dans les différentes régions du Grand-Duché, en lui laissant le choix de publier cette information soit par les médias, par des annonces insérées dans la presse écrite ou par une page web dédiée accessible via la page d'accueil de Google ou de « Google Maps ».

Après avoir rempli les pré-requis de notification en août 2009, Google a repris le captage d'images dans sept communes luxembourgeoises. La Commission nationale suit de près les développements dans cette affaire.

3.3 Enquête de la Ville de Luxembourg en matière de logement

En 2009, la Ville de Luxembourg s'est proposé de mener une enquête concernant les loyers pratiqués sur son territoire pour les logements locatifs. La base légale invoquée se trouve dans les articles 27 et 28 de la loi du 21 septembre 2006 sur le bail à usage d'habitation.

L'article 27 concerne la déclaration obligatoire à charge des propriétaires de logements inoccupés alors que l'article 28 prévoit la possibilité pour les communes d'établir annuellement ou périodiquement un cadastre des loyers.

L'objectif principal cette loi consiste à rendre plus attractif l'investissement dans le logement locatif afin de parer à la pénurie de logements mis en location, tout en continuant à assurer la protection du locataire.

Relevé exhaustif des logements et cadastre des loyers

Le cadastre des loyers a vocation à fournir des indications mises à jour périodiquement sur le niveau moyen des loyers pour les différents types de logements. L'objectif du législateur était de créer un instrument pouvant servir à mieux suivre, en toute transparence, l'évolution des loyers et du marché locatif.

Pour la mise en œuvre de l'enquête ayant vocation de recueillir auprès des personnes interrogées des renseignements nécessaires pour l'une et l'autre finalité (articles 27 et 28), le collège échevinal a fait élaborer un questionnaire par l'institut de recherche CEPS-Instead.

La constitution de ce cadastre nécessite la collecte de données à caractère personnel concernant les bailleurs et les locataires.

Les recommandations que la Commission nationale a exprimées concernant l'interprétation et l'application de l'article 28 de la loi sur le bail à usage d'habitation ont fait l'objet d'un avis émis en date du 23 novembre 2007 (délibération n°228/2007). L'avis analyse comment le traitement de ces données en vue de l'établissement du cadastre des loyers peut se faire dans le respect des règles en matière de protection des données.

Dans son avis, la Commission nationale a estimé d'une part que la collecte de données devait être limitée aux renseignements mentionnés à l'alinéa 1er de l'article 28 de la loi, et que, d'autre part, le cadastre des loyers devait reposer sur un fichier anonyme (c'est-à-dire ne contenant aucune donnée à caractère personnel).

L'anonymisation des données concorde avec la vocation purement statistique du cadastre, prévue par la loi. Elle consiste à calculer périodiquement sur base des données effectives et fiables, le niveau moyen des loyers pratiqués pour les différents types de logements dans une commune (ou une partie de celle-ci) et à rendre ces informations disponibles, sur demande, au Ministre ayant le Logement dans ses attributions.

Le fichier ne devait donc pas être établi en fonction des noms des propriétaires et/ou locataires, ni en fonction de l'adresse de l'immeuble, mais il devait être structuré suivant la typologie retenue des logements (nature, nombre de pièces, surface habitable, année de construction/rénovation, etc.) et par quartier et par localité. Le souci d'anonymisation a imposé par ailleurs de renoncer à une différenciation par quartiers dans les petites communes. L'anonymisation devait ainsi exclure toute mise en relation ultérieure entre le loyer déclaré, d'une part, et l'identité des propriétaires et des occupants du logement d'autre part.

En outre, la Commission nationale a préconisé dans son avis que :

- Les données à caractère personnel figurant sur les formulaires, à savoir les noms, prénoms et adresses des bailleurs, et des locataires, ne soient pas transcrites dans le fichier du cadastre des loyers lors de leur saisie informatique ;
- Les formulaires et, le cas échéant, les listes d'adresses correspondantes soient détruites dès que le niveau moyen des loyers pour les différents types de logements aura été déterminé ;
- Les données au cadastre des loyers ne soient pas rapprochées ou mises en corrélation avec d'autres bases de données nominatives de la commune ou de tiers.

À ces recommandations sont venues s'ajouter celles concernant la déclaration obligatoire de l'état d'occupation des habitations. La Commission nationale a tenu de préciser que la collecte de données relatives à l'occupation des immeubles devait être limitée aux seuls renseignements mentionnés à l'alinéa 1er de l'article 27 paragraphe (2) de la loi du 21 septembre 2006 (à savoir le volume inoccupé, le nombre de pièces et le montant du loyer).

Après de longues et âpres négociations avec la Ville de Luxembourg et le CEPS-Instead, une méthode d'anonymisation des données a pu être trouvée.

La Commission nationale a également insisté sur le fait d'établir une distinction claire entre la partie obligatoire et facultative du questionnaire. Afin de rendre les citoyens attentifs sur les questions optionnelles, permettant une analyse statistique plus détaillée, celles-ci ont été marquées par un astérisque.

La Ville de Luxembourg a donc suivi pleinement les recommandations exprimées dans l'avis de la Commission nationale et a demandé au CEPS-Instead de s'y conformer.

À la suite de la saisie informatique des renseignements fournis dans les questionnaires, la Commission nationale a pu constater que toutes les garanties nécessaires dans la mise en œuvre du cadastre des loyers ont effectivement été respectées.

Étude d'impact de la loi du 21 septembre 2006 sur le bail à usage d'habitation

Par ailleurs, la Chambre des Députés a demandé au Gouvernement, dans une motion relative à la loi du 21 septembre 2006, d'évaluer les effets engendrés par les nouvelles dispositions.

Dans la prédite motion, le Gouvernement est en effet invité à charger l'Observatoire de l'Habitat *« à procéder, un an après l'entrée en vigueur des modifications apportées à la législation sur le bail à loyer, à une évaluation approfondie des répercussions de la nouvelle législation sur le marché locatif national, ainsi que des répercussions éventuelles au niveau de la demande de logements sociaux auprès des communes et des promoteurs publics de logements locatifs sociaux. »*

Ne pouvant pas directement faire suite à cette demande compte tenu du peu d'informations exhaustives disponibles sur les loyers au niveau de l'Observatoire de l'Habitat, le service du Ministère du Logement a souhaité utiliser les informations nominatives recueillies dans le cadre du recensement fiscal des années 2006 à 2008.

L'objectif poursuivi par le Ministère était de permettre le suivi de l'évolution des loyers pour les logements locatifs avant et après l'entrée en vigueur de la nouvelle législation et de continuer la collecte des données une fois que ledit recensement aura été supprimé par l'Administration des Contributions Directes.

La Commission nationale a considéré que l'Observatoire du Logement aurait le droit de réaliser, sous certaines conditions, cette étude impliquant la réutilisation de données, et estime qu'une autorisation formelle pourrait être délivrée à cette fin. (L'autorisation préalable de la Commission nationale est requise pour pouvoir utiliser ultérieurement des données collectées à l'origine pour d'autres finalités).

Il convient donc de bien faire une distinction entre l'étude d'impact de la nouvelle loi, d'un côté, et l'enquête menée auprès des habitants de la Ville de Luxembourg afin d'établir un cadastre de loyers, de l'autre côté.

Contrairement au traitement des données relatif à la création d'un cadastre des loyers qui nécessite l'introduction d'une déclaration préalable par voie de notification, la réutilisation des données nominatives dans le cadre de l'étude d'impact est soumise à une autorisation préalable.

Bien que le fait d'effectuer aussi bien l'étude d'impact que l'enquête auprès des habitants ne se heurte pas aux prescrits de la loi, les deux fichiers ne doivent pas être combinés : si le Ministère du Logement décide d'effectuer cette étude d'impact, il n'a pas le droit de se baser sur le fichier du cadastre des loyers.

3.4 Identifiant unique et registre national de la population

Dans son avis du 10 mars 2009 (en annexe du présent rapport), la Commission nationale a présenté ses réflexions, commentaires et propositions au sujet du projet de loi n°5950 relatif à l'identification des personnes physiques, au registre national de la personne physique et à la carte d'identité.

Selon l'exposé des motifs, l'objectif du projet de loi est de *« régler tout ce qui concerne l'identification des personnes physiques au niveau national ».* Dans ce contexte, il s'agit d'abord de mettre en place un nouveau numéro d'identification des personnes physiques : cet « identifiant unique », remplaçant l'actuel matricule de sécurité sociale, permet l'identification numérique et biométrique des personnes. Ensuite, il est établi un répertoire général de personnes physiques se substituant à l'actuel répertoire général des personnes. Finalement, cette réforme comporte l'introduction d'une « carte d'identité électronique ».

Étant donné que ce projet nécessite l'implication d'un grand nombre d'acteurs, le Gouvernement a chargé un groupe de travail interministériel ad hoc dénommé « identifiant unique » de l'élaboration du projet de loi. La révision de la loi du 30 mars 1979 instituant l'identification numérique des personnes physiques et morales (ci-après : la loi du 30 mars 1979) est par ailleurs directement liée aux travaux effectués par le Comité National pour la Simplification Administrative en faveur des Entreprises (CNSAE).

De 2006 à 2009, la Commission nationale a été consultée périodiquement par le groupe de travail « identifiant unique ». Tout au long du projet, elle a eu des discussions animées avec les représentants des ministères impliqués concernant les aspects relatifs à la protection des données.

Le grand défi dans l'élaboration de la nouvelle loi consistait sans doute dans la conciliation entre la simplification administrative et la protection des données, deux principes potentiellement contradictoires.

D'une part, l'utilisation d'un identifiant unique peut contribuer à faciliter les démarches administratives. 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 fait d'avoir seulement besoin de se rappeler d'un seul identifiant peut également représenter un avantage pratique pour les citoyens, réduisant le temps consacré habituellement aux relations avec les administrations.

D'autre part, la mise en place d'un identifiant unique peut présenter des risques au niveau des libertés et droits des citoyens.

La possibilité de croiser des informations contenues dans différents fichiers concernant la même personne constitue le danger majeur de l'utilisation d'un identifiant unique. L'interconnexion des informations, provenant de plusieurs fichiers d'administrations poursuivant des missions et finalités différentes, permettrait de tracer les individus dans tous les actes de la vie courante. La personne est « transparente » : toutes les informations la concernant sont susceptibles d'être disponibles.

En outre, il existe un risque réel de détournement de finalité : des personnes travaillant dans une administration ayant recours au numéro d'identification seraient en mesure d'accéder à des informations personnelles des citoyens alors que ces renseignements ne sont pas forcément nécessaires et/ou utiles dans le cadre de leurs activités. La recherche d'informations pourrait être mue simplement par la curiosité.

Afin d'éviter les risques d'abus, l'introduction d'un « identifiant unique » doit être accompagnée de garanties appropriées, aussi bien sur le plan juridique que technique. La nécessité de reconstituer des garanties qui se révèlent aujourd'hui insuffisantes, voire défaillantes et/ou 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.

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.

Les garanties techniques 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.

La Commission nationale a estimé dans son avis qu'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 résolue à ne pas remettre en cause le recours à un numéro d'identification unique à utilisation multiple pratiqué depuis presque trente ans et qui, de plus, ne heurte guère la sensibilité de l'opinion publique.

Lors des réunions avec le groupe de travail interministériel, la Commission nationale a donné son éclairage sur les bénéfices et inconvénients respectifs des systèmes d'autres pays européens passés en revue pour l'examen des options envisageables au niveau juridique et technique.

À la lecture du projet final, la Commission nationale note cependant qu'elle ne semble pas avoir été suivie dans ses préconisations de recherche de solutions ambitieuses s'inspirant notamment des exemples d'autres pays pour la modernisation des dispositions de la loi de 1979 et la mise en place d'une plateforme alliant efficacité du fonctionnement des échanges de données entre administrations et garanties pour la protection de la vie privée des administrés.

L'avis a examiné en particulier les aspects relatifs :

a. au rôle central du système 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 national ;

e. à l'enregistrement d'un historique de consultation du registre national des personnes physiques.

3.5 Données sensibles dans le domaine de la recherche

Ces dernières années, le Grand-Duché de Luxembourg a réalisé des investissements importants en vue de développer le secteur de la recherche. Ces investissements se sont accompagnés d'un accroissement de l'activité de la recherche et se sont traduits au niveau de la Commission nationale par une augmentation des demandes d'autorisation introduites par les chercheurs.

Les dites demandes ont trait essentiellement à la recherche médicale ou à la recherche statistique. Dans le premier cas, les traitements contiennent toujours des données sensibles. Dans le second cas, les données ne sont pas systématiquement sensibles au sens de l'article 6 paragraphe (1) de la loi modifiée du 2 août 2002.

La Commission nationale relève que les méthodologies utilisées dans le cadre de ces recherches pour collecter des données sensibles peuvent engendrer des atteintes à la vie privée.

Ainsi, dans certains cas, les organismes requérants souhaitent se voir accorder un accès direct à ces bases de données. Or, cet accès direct risque de conduire à la création de bases de données de plus en plus exhaustives.

Ensuite, lors de l'examen des dossiers touchant au secteur de la recherche, elle constate régulièrement que certaines données utilisées par les centres de recherche comme le STATEC ou le CEPS/INSTEAD, l'Université du Luxembourg, le SESOPI-CI ou le Ministère de l'Éducation Nationale et de la Formation professionnelle ne sont pas récoltées directement auprès des personnes participant aux recherches au moyen, par exemple, de formulaires ou d'enquêtes, mais sont plutôt issues de bases de données préexistantes détenues par d'autres organismes. Ces utilisations secondaires, appelées « traitements ultérieurs de données » dans la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, sont tout à fait possibles et sont soumises à l'autorisation préalable de la Commission nationale.

Dans le cadre des traitements ultérieurs de données, certaines études, essentiellement statistiques, souhaitent obtenir des informations contenues dans les fichiers publics tels les bases de données du registre public des communes, les fichiers d'élèves, les fichiers du Centre Commun de la Sécurité Sociale ou encore de l'IGSS.

De plus, les chercheurs souhaitent parfois effectuer leurs travaux à l'aide de données nominatives, c'est-à-dire non anonymisées. La Commission nationale ne peut ignorer que le recours à des données nominatives souvent sensibles et la valeur importante de données auxquelles les chercheurs ont accès revêt par nature un caractère intrusif susceptible de porter atteinte à la vie privée des personnes dont les données sont traitées. Dans ce contexte, le risque de détournement de finalité est très important. Une personne ayant accès à une base de données pourrait par exemple collecter des informations sur d'autres personnes, informations qui n'ont pas de lien direct avec son étude.

Enfin, l'interconnexion des données traitées par différents acteurs (pour des finalités distinctes) constitue un autre risque qui est d'autant plus important dans un pays comme le Luxembourg, ayant un faible taux d'habitants et possédant un nombre restreint de chercheurs et d'instituts de recherche.

Malgré ces risques, la Commission nationale est convaincue qu'il est tout à fait possible de concilier à la fois les intérêts de la recherche avec les droits des personnes. Diverses solutions peuvent alors être envisagées : l'utilisation de données anonymes ou codées, le recours au procédé d'anonymisation par une fonction de hachage ou encore l'intervention d'un tiers de confiance. Cet acteur externe a pour mission de dépersonnaliser et coder les données reçues par l'organisme fournisseur avant de transférer celles-ci au chercheur requérant. Ainsi, les fournisseurs des données et les chercheurs ne sont plus en relation directe. En tout dernier recours, si la recherche ne peut avoir lieu avec des données possédant un moindre degré d'identification, la Commission nationale peut consentir à ce qu'un transfert de données permettant l'identification directe des personnes ait lieu, à condition que les données

soient anonymisées dès que leur identification n'est plus nécessaire à la réalisation du projet de recherche.

Par ailleurs, la Commission nationale note que dans le cadre du développement de la recherche, les données traitées dites sensibles ne portent pas seulement sur les données socioprofessionnelles. En effet, de plus en plus d'études englobent des facteurs relatifs aux migrations et à l''origine des populations non-luxembourgeoises (p.ex. : populations immigrées). Le sujet des statistiques ethniques et raciales a été abordé lors du déjeuner-débat « Mesurer les diversités tout en respectant la protection de la vie privée ». Cette réunion a été une bonne opportunité pour la Commission nationale et le président de la CNIL, M. Alex Türk, de montrer que les principes de la protection des données ne sont pas incompatibles avec la collecte et l'analyse de données relatives à l'origine raciale et ethnique et aux croyances religieuses (voir partie 2.3.4 pour plus de détails à ce sujet).

3.6 Accès de la police à des fichiers des administrations publiques

La loi du 22 juillet 2008 règle l'accès des magistrats et officiers de la police judiciaire à un certain nombre de banques de données appartenant à des administrations ou établissements publics.

Le projet de loi n°5986 est venu modifier quelques dispositions légales nouvellement introduites par la loi mentionnée ci-dessus en raison de difficultés pratiques et opérationnelles constatées lors de sa mise en œuvre.

La presse nationale a largement relayé les difficultés d'application de la loi dans le cas d'infractions mineures à la législation relative à la circulation routière (recouvrement des avertissements taxés en cas de stationnement irrégulier). En effet, le fichier des véhicules routiers, tenu par le Ministère des Transports, ne pouvait être consulté que dans les cas où le seuil de gravité correspondait à une peine correctionnelle dépassant deux années d'emprisonnement. S'agissant d'une simple contravention dans le cas d'un avertissement taxé pour stationnement irrégulier, les policiers se trouvaient dans l'impossibilité d'examiner le fichier en question.

Le projet de loi ne s'est cependant pas limité à résoudre le problème apparu en matière d'avertissements taxés pour infractions bénignes à la législation sur la circulation. Il a également assoupli un certain nombre de restrictions, conditions et modalités inscrites dans la loi comme mesures de sauvegardes destinées à éviter un recours disproportionné à l'accès aux fichiers administratifs publics.

Dans son avis du 4 mai 2005 relatif à l'avant-projet de loi ayant précédé l'adoption de la loi du 22 juillet 2008, la Commission nationale avait exprimé le souhait que le texte détermine limitativement les fichiers publics concernés, les catégories de données ouvertes à la consultation et les finalités de la consultation. Dans cet avis, elle avait également préconisé qu'il encadre les accès aux traitements des données personnelles par des mesures techniques adéquates assurant la sécurité du système, le retraçage des données accédées ainsi que des motifs de la consultation et permettant le contrôle du respect des restrictions prévues par la loi.

Elle n'avait cependant pas jugé nécessaire la fixation d'un seuil de gravité de la peine encourue jugeant que le texte du projet de loi n°5563 représentait un compromis équilibré entre les intérêts d'efficacité du travail de la Police et de la Justice et les libertés publiques et droits fondamentaux des citoyens.

Dans son avis du 3 avril 2009 sur le projet de loi n°5986, la Commission nationale a estimé qu'il faudra préserver l'essentiel des garanties dont le législateur avait précédemment souhaité entourer l'ouverture des banques de données à la consultation par la Police et la Justice, à savoir :

- Détermination claire du périmètre à une liste limitative de banques de données énumérées expressément dans la loi ;
- Limitation des catégories de données ouvertes à la consultation et notamment exclusion des données de santé ;
- Exigence d'un motif précis justifiant la consultation et la journalisation des accès (informations consultées, par qui, pourquoi) permettant de déceler d'éventuels abus ;

- Limitation des données consultées aux informations pertinentes et nécessaires dans le strict respect du principe de proportionnalité ;
- Limitation du cercle des personnes autorisées à accéder aux données personnelles aux seuls magistrats et aux policiers ayant le rang d'officier de police judiciaire.

La plupart de ces recommandations ont été prises en considération à l'exception de deux éléments importants, à savoir la limitation de l'accès aux officiers de police judiciaire et le traçage des personnes ayant consulté les bases de données.

Cette dernière recommandation qui avait été écartée par le Gouvernement en raison de difficultés d'implémentation technique à court terme a toutefois été reprise au cours des débats parlementaires dans une motion du 29 avril 2009 (en annexe du présent rapport), déposée par l'honorable députée Madame Colette Flesch : « *La Chambre des Députes, (…) soucieuse de voir la confidentialité des informations se trouvant dans les bases de données garanties et d'éviter des abus, insiste sur le fait qu'un contrôle efficace de ces consultations doit être assuré, notamment au niveau du motif, de la traçabilité et de l'identification des personnes ayant procédé à la consultation. (…) Regrettant qu'actuellement les programmes informatiques des fichiers concernés ne permettent pas la saisie de l'identifiant numérique des faits, ni du motif de la consultation, la Chambre des Députés invite le Gouvernement à mettre en place, dans un délai approprié, des solutions technologiques modernes destinées à éviter les risques d'abus et notamment un système informatique permettant de retracer le respect des conditions légales, c'est-à-dire du principe de proportionnalité et du lien direct des données consultées avec les faits ayant motivé la consultation* ».

Même si ses deux principales préconisations n'ont pas été retenues, la Commission nationale a noté avec satisfaction que la motion de la Chambre des Députés a été votée à l'unanimité et espère que le Gouvernement va la mettre en pratique dans un avenir proche.

3.7 Une sophistication de plus en plus grande des applications et services en ligne

Il ne se passe guère de semaines sans que des géants de la Toile comme Google ou Facebook ne lancent de nouveaux produits ou services, aussi novateurs qu'impressionnants. Ceux-ci fonctionnent toujours selon le même modèle: ils sont gratuits, les fournisseurs assurant leurs revenus par le biais de la publicité. Plus le nombre des utilisateurs s'accroît et plus leurs besoins sont analysés de manière ciblée, plus les recettes publicitaires des fournisseurs augmentent. Ces derniers mettent donc tout en œuvre pour rassembler un maximum d'utilisateurs et de possibilités de publicité. Voici quelques exemples récents :

- Facebook offre un outil permettant à ses membres de synchroniser leurs agendas et leurs carnets d'adresses sur sa plateforme. Mais les contacts ainsi téléchargés sont mis à la disposition non seulement des utilisateurs eux-mêmes, mais aussi de Facebook. Cette société a donc accès à des informations concernant des personnes qui ne sont pas au courant de cette transmission de données et n'y ont pas consenti.
- Google a également depuis peu pénétré le marché lucratif des réseaux sociaux et offre, avec « Google Buzz », aux utilisateurs de Gmail un outil grâce auquel ils peuvent échanger des informations avec des « amis ». Un tollé général s'en est suivi. En effet, Google avait structuré les fonctions de base du programme de telle manière que l'ensemble des échanges de courriels entre les 176 millions d'utilisateurs de Gmail qui cliquaient sur cet outil étaient rendus publics.
- Twitter possède désormais un outil de localisation. Avec ce dernier, on peut donc non seulement communiquer ses pensées et ses activités à ses amis (« followers »), mais aussi leur indiquer l'endroit où l'on se trouve : les navigateurs permettent de poursuivre les utilisateurs de Twitter pas à pas et d'établir leurs coordonnées. Mis à part le fait que les amis Twitter savent ainsi en tout temps où l'on se trouve, Twitter le sait également et peut cibler sa publicité avec

davantage de précision : la personne se tenant tout près d'un magasin de vêtements par exemple recevra alors une offre intéressante par SMS.

- Avec « Goggle », Google s'essaie à la reconnaissance faciale automatique grâce à un logiciel pour téléphone portable. Un moteur de recherche permet de déterminer si la personne photographiée figure déjà dans une banque de données accessible sur Internet et transmet le résultat de ses recherches sur le portable.

Le téléphone portable muni de la fonction de localisation permettra en tout lieu de recevoir des informations sur l'endroit où l'on se trouve, de repérer les curiosités touristiques, de retrouver des amis et d'identifier des personnes. Ainsi, le monde réel devient en quelque sorte une interface-utilisateur numérique qui permet d'accéder à des données en tout temps et en tout lieu.

Les données collectées à l'occasion de leurs activités en ligne auprès de millions d'utilisateurs permettent d'établir des profils de comportement et d'intérêts des internautes. La publicité peut ainsi être ciblée en fonction des caractéristiques particulières de l'utilisateur (lieu, heure, produit et personne) avec un degré de sophistication jusqu'ici jamais atteint. Rien d'étonnant à ce que les supports publicitaires traditionnels du monde entier, surtout dans la presse, craignent pour leurs recettes : aux États-Unis, la publicité en ligne a déjà dépassé la publicité imprimée.

Cette évolution soulève une question intéressante : comment ces nouveaux produits vont-ils influencer notre comportement ? Lorsque des algorithmes influent de plus en plus sur notre vie, nous disent ce que nous sommes et ce que nous devrions faire, l'autodétermination en tant qu'essence de notre modèle social libéral est remis en question. Des études sont en cours concernant les répercussions, sur les mécanismes démocratiques de décision, de nos perceptions et de nos prises de décision lorsque celles-ci sont régies par des algorithmes.

Face à ce genre d'évolutions, rien ne sert de verser dans le pessimisme culturel et de voir tout en noir, même si l'on ne peut nier qu'il s'agit là d'un grand défi pour tous ceux qui se sentent tenus de veiller à la protection de la sphère privée. Ce n'est pas seulement la protection des données qui est concernée, mais bien la société toute entière :

En premier lieu, les utilisateurs : ceux-ci doivent tout d'abord rester conscients que les informations personnelles qu'ils communiquent ont de la valeur. Il leur appartient alors d'apprécier au cas par cas si l'offre qui leur est faite mérite que ces données soient diffusées sur Internet. Trop souvent nous négligeons de lire ce qui est imprimé en tout petits caractères et de vérifier à quoi serviront les informations que l'on nous demande, en sachant bien qu'elles permettent d'établir des profils de la personnalité très détaillés. Les utilisateurs doivent aussi devenir plus critiques et prudents pour ne pas mettre en réseau des informations concernant amis et connaissances (par exemple des photos prises lors de fêtes de famille ou de cours d'école) sans le consentement de toutes les personnes concernées.

Les utilisateurs qui ne veulent pas de cette protection sont libres d'y renoncer, mais trop souvent ils doivent accomplir eux-mêmes les démarches nécessaires pour ce faire et adapter les fonctions de base de leurs comptes. Dans ce contexte, il est important de souligner qu'à elles seules, les réglementations nationales ne pourront résoudre le problème. Des mesures à l'échelon international s'imposent également.

Les médias et les écoles sont aussi concernés : pour mieux préparer les jeunes et sensibiliser les utilisateurs adultes aux risques de l'utilisation des nouvelles techniques, il devient de plus en plus important de leur fournir les informations et explications nécessaires. Ici, l'école a pour mission de donner aux enfants et aux jeunes une base suffisamment solide pour qu'ils prennent conscience de la valeur de leur sphère privée. Chaque niveau de la formation doit aborder cette réalité que sont les nouveaux moyens de communication et montrer comment s'en servir.

Enfin, les fournisseurs de ce type de services devraient prendre davantage en considération la protection de la sphère privée de leurs clients. Dans l'intérêt de leur propre image, il devrait leur tenir à cœur de ne mettre sur le marché que des produits respectueux de la protection des données de sorte que l'utilisateur ne soit pas encore obligé de prendre des mesures supplémentaires dans ce sens. Seule la pression de l'opinion publique amènera

les grands fournisseurs sur le chemin de la vertu. Dans le cas de « Google Street View », qui nous a fort occupés au cours de l'année écoulée et qui nous occupera encore, nous touchons là au point essentiel. Même si de plus en plus de personnes semblent se résigner à l'abandon quasi total du « privé », la conclusion que le chef de Google, Eric Schmidt, a récemment tirée que la vie privée est une valeur dépassée ne devrait pas - et pour longtemps encore - rassembler la majorité des suffrages.

Or les utilisateurs montrent tous les jours qu'ils n'entendent pas que leurs données personnelles soient considérées avec désinvolture. Ils protestent, ils bloguent, ils constituent des groupes d'intérêts et obtiennent des améliorations. En notre qualité d'autorité de protection des données, nous ne pouvons que soutenir entièrement cette tendance.

3.8 Sensibilisation aux risques sur Internet

Une étude récente, réalisée par Eurostat et publiée par le STATEC, a révélé qu'Internet est de plus en plus présent dans le quotidien des Luxembourgeois. En 2009, 87 % des ménages ont été connectés à Internet, représentant une progression de 9 % par rapport à l'année précédente et une deuxième position parmi les 27 pays membres de l'UE. Interactivité, rapidité et facilité d'utilisation sont les caractéristiques principales ayant rendu ce média si populaire, en particulier chez les jeunes.

Devenu presque incontournable dans notre quotidien, le « Web » ne permet pas seulement d'accéder à des quantités considérables d'information, mais aussi de tisser des liens sociaux, d'échanger des idées, des messages et des documents ou encore d'acheter et de vendre des produits. La mise en place d'un site web, d'un blog ou d'un profil dans une communauté virtuelle représente en outre un moyen d'afficher sa propre identité. La création et l'échange de contenus est désormais à la portée de chacun par le biais de forums de discussions, sites encyclopédiques ou encore des « réseaux sociaux » virtuels tels que Facebook, MySpace ou StudiVZ.

Loin de constituer de simples « présentoirs virtuels », les réseaux sociaux permettent de visualiser les profils d'autres membres, d'interagir et de communiquer avec eux, de faire des nouvelles connaissances, de se regrouper avec d'autres personnes partageant les mêmes préférences et de rester au courant de ce que font les connaissances réelles et virtuelles. De plus, les utilisateurs peuvent se divertir avec des jeux et applications mises à disposition par le fournisseur d'un réseau ou par des parties tierces. La tendance de partager ses données et sa vie privée avec autrui est encore renforcée par l'essor de nouvelles technologies, ainsi que par le développement des technologies mobiles, grâce auxquelles les appareils des internautes restent connectés en continu.

La multiplication des activités en ligne (communications, opérations bancaires, achats en ligne, réservation de vacances, etc.) et en particulier l'essor fulgurant des réseaux sociaux, favorisant l'échange à grande échelle d'informations de tout genre, sont pourtant source de nouveaux enjeux à l'égard de la protection des données et de la vie privée et donnent lieu à certaines préoccupations.

Noms, dates de naissance, adresses, numéros de cartes de crédit ou d'autres renseignements personnels constituent des informations fortement convoitées. Non sécurisées, elles risquent d'être perdues, détournées ou même vendues. Une fois diffusées sur la Toile, ces données peuvent échapper à ceux auxquels elles se rapportent et risqueront de réapparaître encore bien des années plus tard. Il peut s'avérer très difficile de garder le contrôle sur les divers usages qui peuvent en être faits, souvent à l'insu de l'internaute et trop souvent à des fins malhonnêtes.

Les informations personnelles (intérêts, orientation sexuelle, mode de vie,…) se trouvant sur Internet ou renseignées par le système informatique de l'usager peuvent par ailleurs être utilisées à des fins de profilage pour établir un suivi des consultations sur Internet ou encore pour lui adresser des publicités de plus en plus personnalisées. Cette collecte de données peut ainsi comprendre l'adresse IP, le nom d'hôte, le système d'exploitation, le navigateur, la résolution d'écran, les requêtes entrées dans un moteur de recherche ou encore la localisation.

Les autorités nationales de protection des données de l'Union européenne (dont la Commission nationale),

réunies dans le groupe de travail « Article 29 », se sont penchées sur cette question et ont élaboré un papier de guidance précisant les règles applicables tant pour les fournisseurs des services de « réseaux sociaux » que pour les personnes utilisant ces services (avis n° 5/2009 du 12 juin 2009, WP 163 - voir aussi partie 2.6.1.1).

Ce papier souligne notamment l'importance du droit de toute personne concernée de choisir elle-même ce qu'il advient des informations la concernant. Il se consacre en particulier à la protection accrue qui doit être accordée aux utilisateurs mineurs.

Dans ce contexte, le papier énumère certaines obligations incombant aux fournisseurs de service (même s'ils sont situés hors de l'UE) :

- L'utilisateur doit pouvoir choisir lui-même dans quelle mesure ses informations seront publiques (à défaut, le compte doit être paramétré de sorte que la publicité des données soit limitée) ;
- Il doit être clairement mis en connaissance du « qui », du « pourquoi » et du « comment » de l'usage des données qu'il stocke dans le réseau ;
- Il doit être d'accord avec tout usage qui est fait de ses données ;
- Il doit avoir le droit de rester anonyme par rapport au public (par le biais d'un pseudonyme).

De plus :

- Toute personne (membre ou non du réseau social) concernée doit pouvoir se plaindre et demander la suppression de données la concernant ;
- Les comptes restés inactifs pendant une certaine période doivent être supprimés ;
- Le fournisseur de service doit assurer que les tiers offrant des applications et services additionnels dans le cadre du réseau se conforment aux dispositions légales relatives à la protection des données et à la vie privée ;
- Les utilisations des données à des fins commerciales ou de marketing doivent se faire dans le respect des dispositions légales et des droits des personnes que ces données concernent ;
- Le fournisseur de service doit faire preuve d'une décence particulière vis-à-vis des utilisateurs mineurs et mettre en place des mesures pour les protéger.

Internet n'est donc pas une « zone de non-droit ». Les lois et règles de la « vie réelle » y trouvent bien application, notamment les lois en vigueur concernant la protection des données et de la vie privée.

Une protection et un encadrement particulier doivent être accordés aux utilisateurs mineurs. Même s'ils sont très familiers avec l'usage des nouvelles technologies, ils ne sont pas toujours conscients des dangers auxquels ils se soumettent en exposant leurs données personnelles sur Internet. En l'occurrence, des actions pouvant sembler anodines comme la diffusion de photos ou vidéos sur des réseaux sociaux risquent d'avoir une influence négative sur leur avenir professionnel. De manière générale, ils sont plus influençables et moins critiques que les adultes.

Par conséquent, les mineurs ont besoin d'une protection accrue : les fournisseurs de services sur Internet doivent donc faire preuve d'une loyauté particulière à leur égard en omettant de leur demander des données sensibles ou leur consentement (sans celui des parents) à des usages ultérieurs des informations à des fins autres, voire de faire du marketing ciblé à leur égard. Les mineurs doivent également être protégés de personnes malveillantes, notamment en séparant techniquement les communautés réservées aux adultes de celles dédiées aux mineurs.

Au niveau de la sensibilisation et de l'information sur les risques, un rôle important revient aux autorités nationales et régionales dans le domaine de la protection des données et de la vie privée.

Dans ce contexte, la Commission nationale a participé au « Safer Internet Day » en février 2009. Ce programme, organisé par le réseau LuSI (Luxembourg Safer Internet) et subventionné par la Commission européenne a comme objectif de promouvoir un usage plus sûr de l'Internet et des nouveaux moyens de communication auprès des jeunes, des parents et des éducateurs.

A côté de sa présence sur le stand d'information, la Commission nationale a organisé une conférence-débat

au sujet de « la protection des données sur Internet », donnant aux personnes intéressées la possibilité de se renseigner et de poser des questions au personnel de la Commission nationale. L'objectif principal de l'événement était de sensibiliser les internautes aux règles s'appliquant sur le Web et de les informer sur leurs droits concernant leurs données personnelles.

Les risques sont nombreux : abus potentiels à l'intérieur des réseaux sociaux, usurpation d'identité, redirection de l'internaute d'un site original vers un site frauduleux, création d'adresses mail ou de profils truqués,…

L'information du public sur les risques et les droits en matière de protection de la vie privée constitue une des priorités pour les années à venir. Selon une étude de SafeNet, seulement 15% des Européens s'estiment suffisamment informés sur l'utilisation de leurs données personnelles. Il existe donc toujours de nombreuses incertitudes auprès des citoyens concernant la protection de leurs données et le besoin d'être informé sur leurs droits en la matière reste présent. Ce constat est vérifié par une enquête de CASES montrant qu'une personne sur quatre est prête à révéler son mot de passe à des inconnus en échange de la promesse d'une petite récompense. Ces exemples confirment qu'il est important d'améliorer la prise de conscience des utilisateurs d'Internet en ce qui concerne la nécessité de protéger leurs données personnelles.

3.9 Investigations dans le secteur des télécommunications

En 2009, le groupe de travail « Article 29 » a lancé une action concertée relative à l'application de la directive « rétention des données ».

Dans ce cadre, les autorités nationales de protection des données ont analysé dans leurs pays respectifs si l'utilisation des données de trafic par les fournisseurs de télécommunications et d'Internet était conforme à la législation nationale, basées sur la Directive 2002/58/CE (transposée par la loi modifiée du 30 mai 2005 relative à la protection de la vie privée dans le secteur des communications électroniques) ainsi que sur la Directive 2006/24/CE sur la conservation des données.

L'objectif principal de cette étude consistait à analyser dans quelle mesure les garanties requises en relation avec la protection des données (et en particulier au regard des données stockées, des mesures de sécurité, de la prévention d'abus et des durées de conservation) étaient fournies dans le secteur des télécommunications des différents États membres.

À cet égard, la Commission nationale a mené des investigations auprès de trois opérateurs de téléphonie mobile et de cinq fournisseurs de services Internet. Les résultats de cette investigation permettront d'évaluer de quelle manière la directive sur la conservation des données a été implémentée en pratique dans les différents États membres.

À côté de l'initiative au plan européen mentionnée ci-dessus, la Commission nationale a également procédé à des actions d'investigation de sa propre initiative, c'est-à-dire sans qu'une demande n'ait été portée à son attention.

Ainsi, elle a poursuivi son action dans le secteur des communications électroniques en vérifiant si les traitements des données des opérateurs privés de téléphonie mobile Orange (anc. VOX) et Tango étaient conformes 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. Dans ce secteur « sensible », le public est en droit d'être assuré que la confidentialité des informations relatives aux communications est rigoureusement respectée.

Dans les années 2007-2008, la Commission nationale avait mené le même type d'investigation auprès du département « Télécommunications » de l'Entreprise des P&T. Cette investigation avait permis de constater un niveau élevé de conformité du traitement des données aux exigences légales même si certaines recommandations d'amélioration ont été émises dans le rapport final de la Commission nationale.

3.10 Décision type en matière de surveillance de l'utilisation de l'outil informatique

Avant de mettre en place une surveillance du courrier électronique, de l'utilisation d'Internet et du réseau informatique, l'employeur doit obtenir une autorisation préalable de la Commission nationale. Afin de faciliter la tâche aux entreprises souhaitant mettre en oeuvre une telle surveillance, la Commission nationale a élaboré, en 2008, une décision type qui en définit les limites. En même temps, elle peut être considérée comme un guide pour implémenter les mesures de contrôle dans le respect des règles en matière de protection de la vie privée et des données à caractère personnel.

Lors de la mise au point de la décision type, qui vise à concilier respect de la sphère privée des salariés sur le lieu de travail et intérêts légitimes des employeurs, la Commission nationale a tenu compte des nombreuses demandes d'autorisation et demandes de renseignement qui lui ont été soumises. Elle a ainsi retenu un catalogue limitatif des finalités pour lesquelles des mesures de surveillance peuvent être acceptées. Ainsi, un tel traitement peut être effectué pour garantir le bon fonctionnement des systèmes informatiques de l'entreprise ou la protection de ses intérêts économiques, commerciaux et financiers auxquels est attaché un caractère de confidentialité (notamment, la protection contre la divulgation de secrets d'affaires et de fabrication et contre les violations du secret bancaire).

En 2009, 166 traitements ont été autorisés concernant la surveillance de l'outil informatique sur le lieu de travail. La majorité des demandes proviennent d'entreprises issues du secteur financier et de l'assurance.

Les questions qui se posent pour 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 de la surveillance et des contrôles des salariés par l'employeur.

L'employeur est obligé d'informer les salariés des limites et de l'usage à des fins personnelles qu'il tolère en matière d'utilisation des outils informatiques sur le lieu de travail. Dans un souci de transparence et étant donné qu'il n'est pas toujours possible de distinguer clairement entre ce qui relève de la vie professionnelle et ce qui relève de la vie privée, la Commission nationale recommande que l'employeur adopte une charte ou un règlement interne relatif à l'utilisation des outils informatiques.

Une ligne directrice de la décision type est la proportionnalité dans la surveillance. Même en cas d'interdiction totale de l'utilisation des outils informatiques à des fins privées, l'employeur n'a pas le droit de contrôler l'usage de manière continue. La surveillance doit toujours être graduée (selon la notion allemande de « *progressive Kontrollverdichtung* »). Dans un premier stade, l'employeur ne peut effectuer qu'une surveillance ponctuelle. Seulement si des indices d'abus ou de comportements irréguliers sont identifiés, ces vérifications peuvent être intensifiées.

Pour plus de détails, se reporter à la décision type de la Commission nationale en matière de surveillance de l'utilisation de l'outil informatique se trouvant en annexe.

4 Perspectives

Après les scandales de 2008 qui ont porté les préoccupations de protection des données personnelles à l'avant-plan de l'actualité en RFA et qui ont conduit aux récentes modifications du cadre légal applicable aux répertoires de solvabilité des personnes (« *Kreditauskunfteien* » ; p.ex. *Schufa*) dans le domaine de la cession de fichiers d'adresses de clients et du démarchage téléphonique ainsi que de la protection de la vie privée sur le lieu du travail, l'année 2009 a surtout été marquée par des gros titres de la presse focalisés sur les risques pour la vie privée sur Internet, les nouvelles technologies qui envahissent notre vie quotidienne et le dialogue transatlantique relatif aux données des citoyens européens qui doivent être rendues accessibles aux entités américaines dans le contexte de la lutte contre le terrorisme.

Google, Facebook, RFID, SWIFT

Outre les prises de vues et les collectes de données effectuées à bord des voitures spéciales dans les rues de nos villes pour une visualisation à 360° en ligne qui a alimenté une controverse incessante à travers l'Europe quant à leur légitimité, les activités de Google étaient également visées tout comme celles de Yahoo, Microsoft et d'autres exploitants de moteurs de recherche sur Internet par des démarches coordonnées des autorités nationales de protection des données à travers le groupe « Article 29 ». Le groupe a demandé aux exploitants de limiter la durée de conservation des données enregistrées en relation avec l'usage des moteurs de recherche, sinon de les anonymiser mieux et plus rapidement. L'introduction de Google Buzz pour les utilisateurs de Gmail a aussi donné lieu à la divulgation non voulue des coordonnées de leurs correspondants et a soulevé une levée de boucliers à laquelle Google a cependant réagi rapidement en corrigeant le tir. Mais c'est surtout à l'occasion des modifications apportées unilatéralement par Facebook à ses conditions générales d'utilisation et respectivement aux réglages configurés par défaut sur son site de réseau social que fût attirée l'attention de l'opinion publique sur les risques d'exhibition de la vie privée sur Internet et les difficultés à y remédier par la suite.

La question du « droit à l'oubli » sur Internet fût clairement posée dans ce contexte, notamment dans les débats du Sénat français et la revendication exprimée de l'introduction d'un droit individuel à l'effacement de texte informatisé, photos ou autre donnée à caractère personnel des sites Internet qui l'affichent souvent en la reprenant d'autres sites de sorte que le consentement et la finalité légitime ne sont plus retraçables.

Les risques auxquels s'exposent les mineurs, bien plus réceptifs et nombreux à adopter ces nouveaux modes de communication, ont été à l'origine de réflexions menées à l'échelle européenne et d'actions d'information et de sensibilisation des jeunes et de leurs parents. La publicité ciblée suivant le comportement des internautes (*Behavioural advertising*) mettant à profit le profilage sous toutes ses formes est un autre exemple d'enjeu. Les nouvelles technologies de l'information et de la communication (TIC) et leur impact sur la vie privée des utilisateurs et les moyens nécessaires pour permettre à ces derniers de se protéger et pour assurer une réelle transparence des traitements des données opérés à l'insu des concernés furent le dénominateur commun de discussions qui ne manqueront pas de marquer les travaux d'une future révision de la Directive 95/46/CE (protection des données et libre circulation) qui s'annoncent pour la fin de l'année 2010.

Ainsi, le socle juridique européen sera modernisé et simplifié pour s'assurer que le respect de la vie privée évolue avec la technologie. Les 350 millions d'utilisateurs du réseau social Facebook fin 2009, l'identification biométrique ou encore le traçage des déplacements par la géolocalisation ne sont que quelques exemples témoignant des changements dans la manière dont les données personnelles sont collectées, traitées et utilisées.

La mondialisation des flux de données a influencé aussi le sujet délicat du juste équilibre à respecter dans le recours aux données privées des citoyens pour les besoins de la sécurité publique et de la lutte contre le terrorisme et la criminalité organisée.

L'avenir de la protection des données

Les travaux vont démarrer à l'automne pour la mise en chantier de la directive de 1995. Déjà quelques idées phare ont été lancées quant aux objectifs majeurs : simplification, « accountability », allègement des contraintes administratives, amélioration de l'efficacité de la protection légale, droits individuels renforcés pour

les citoyens/utilisateurs/consommateurs, sanctions et supervision plus efficaces.

Le rôle des autorités nationales, chargées de la mise en œuvre et du contrôle de l'application, s'en trouvera sans aucun doute renforcé de manière à ce que leur action puisse correspondre aux attentes des citoyens à notre époque numérique marquée par la mondialisation et l'essor des technologies de l'information et de la communication.

Gageons que l'avenir ne sera pas fait de moins de défis, de sollicitations et de responsabilités par la petite équipe de la CNPD et que les moyens qui lui sont alloués ne seront pas de trop pour assurer, comme par le passé, avec engagement les missions qui lui sont confiées par la loi.

5 Ressources, structures et fonctionnement de la Commission nationale

5.1 Rapport de gestion relatif aux comptes de l'exercice 2009

L'activité de la Commission nationale au cours de l'année 2009 a été marquée par :

- L'examen et l'approbation des règles contraignantes d'entreprise du groupe eBay nécessitant une analyse approfondie et de nombreuses suggestions et modifications de la part de la Commission nationale afin de rendre cette charte applicable à une échelle mondiale et conforme aux standards du droit européen ;
- La concertation avec de nombreux ministères et organismes publics au sujet de dossiers et projets justifiant des recommandations relatives aux traitements des données personnelles ;
- L'adoption de six avis formels relatifs à des projets de loi ou règlements grand-ducaux ;
- L'optimisation des procédures internes et de l'infrastructure informatique en vue de l'accélération du traitement des nombreuses demandes d'autorisation introduites ;
- L'élaboration d'un nouveau formulaire de notification intégrant la signature électronique ;
- Le renouvellement du site Internet www.cnpd.lu avec un contenu plus étoffé et une présentation plus attractive ;
- 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 concrètement le respect des obligations légales dans le secteur des communications électroniques.

Dépenses de fonctionnement

Les loyers et charges locatives relatifs aux locaux provisoires de la Commission nationale (pris en location dans l'attente de son implantation dans le 1er bâtiment à ériger par l'État à Belval-Ouest) ont atteint 107.711,76€, dépassant légèrement les prévisions, vu qu'un bureau supplémentaire a été loué.

Les effectifs en personnel de la Commission nationale se composaient en 2009, 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 fonctionnaire et d'un employé de l'État bénéficiant du statut de travailleur handicapé assurant le secrétariat et l'administration, de trois attachés à la direction affectés au service juridique et d'un attaché stagiaire affecté à la communication et à la documentation.

Les charges relatives au personnel permanent ont progressé par rapport à l'exercice 2008 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 2009, les dépenses sont restées en-dessous des prévisions.

Les trois juristes ont terminé avec succès leur période de stage et ont été titularisés comme attaché de direction à l'issue de l'examen afférent en avril 2009. Le fonctionnaire assurant le secrétariat et l'administration a terminé avec succès sa période de stage et a été titularisé comme rédacteur à l'issue de l'examen afférent en décembre 2009.

La Commission nationale a également dû recourir à des prestations d'experts à défaut de disposer de ressources spécialisées nécessaires en interne, notamment dans des domaines comportant des aspects technologiques et informatiques complexes, bien qu'il eut été sans doute préférable pour la continuité du service, d'acquérir ou de conserver depuis 2002, les compétences afférentes au sein de l'établissement public.

Parmi les dépenses d'honoraires, frais d'experts et prestataires externes pour un montant de 210.707,94 €, 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, les frais de port et de télécommunications et les

autres charges générales d'exploitation ont connu une progression linéaire suivant l'augmentation du nombre de collaborateurs en activité.

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 dépenses d'information du public et de communication (44.634,06 €) ont dépassé légèrement les montants prévus alors que le coût des annonces de presse publiées dans le cadre de la campagne menée à l'occasion de la journée européenne du 28 janvier est venu s'ajouter à des dépenses ponctuelles non récurrentes. Le travail de sensibilisation des citoyens (en particulier des jeunes quant aux risques sur Internet) a pris une importance primordiale dans l'activité de 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 au cours de l'exercice 2009 à diverses investigations dont la Commission a pris l'initiative depuis 2005 même en dehors des plaintes et demandes de vérification qui lui sont soumises. Pour le contrôle sur place, audits et vérifications à effectuer dans ce domaine, la Commission nationale a eu recours à un expert externe spécialisé dans les questions de sécurité informatique et à de bonnes pratiques organisationnelles.

La Commission nationale a procédé en 2009 à des investissements relatifs au développement et à la mise en service de l'application informatique spécifique dédiée à l'établissement du registre public des traitements prévu à l'article 15 de la loi et au suivi des dossiers de notifications et demandes d'autorisation préalables ainsi qu'à l'optimisation des procédures administratives. Les formulaires ont été considérablement améliorés et permettent désormais aux déclarants une meilleure convivialité dans l'utilisation et simplifient la gestion de leur déclaration intégrant la signature électronique.

Les frais relatifs à la gestion et à la 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 25.204,17 €.

Le total des frais de fonctionnement encourus par l'établissement public au cours de l'exercice 2009 s'élève à 1.483.062,94 €.

Recettes

Le montant des redevances perçues en application des articles 37 paragraphe (4) et 13 paragraphe (4) de la loi s'élevant à 52.545 € est resté conforme à nos prévisions. En outre des produits financiers (intérêts créditeurs) ont pu être enregistrés à hauteur de 4.789,15 €.

Résultat d'exploitation

Compte tenu de la dotation annuelle de 1.476.000 € dont la Commission nationale a bénéficié en 2009 de la part de l'État en application de l'article 37 paragraphe (4) de la loi, le résultat d'exploitation de l'établissement public s'établit à 50.271,21 € au 31 décembre 2009 qui sera reporté à nouveau sur l'exercice suivant.

5.2 Assermentation de trois nouveaux juristes

Le 10 avril 2009, Monsieur le Ministre des Communications Jean-Louis Schiltz a procédé à l'assermentation de trois nouveaux juristes. MM. Michel Sinner, Georges Weiland et Christian Welter ont ainsi rejoint les rangs des fonctionnaires de l'État dans la carrière supérieure de l'attaché de direction.

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.

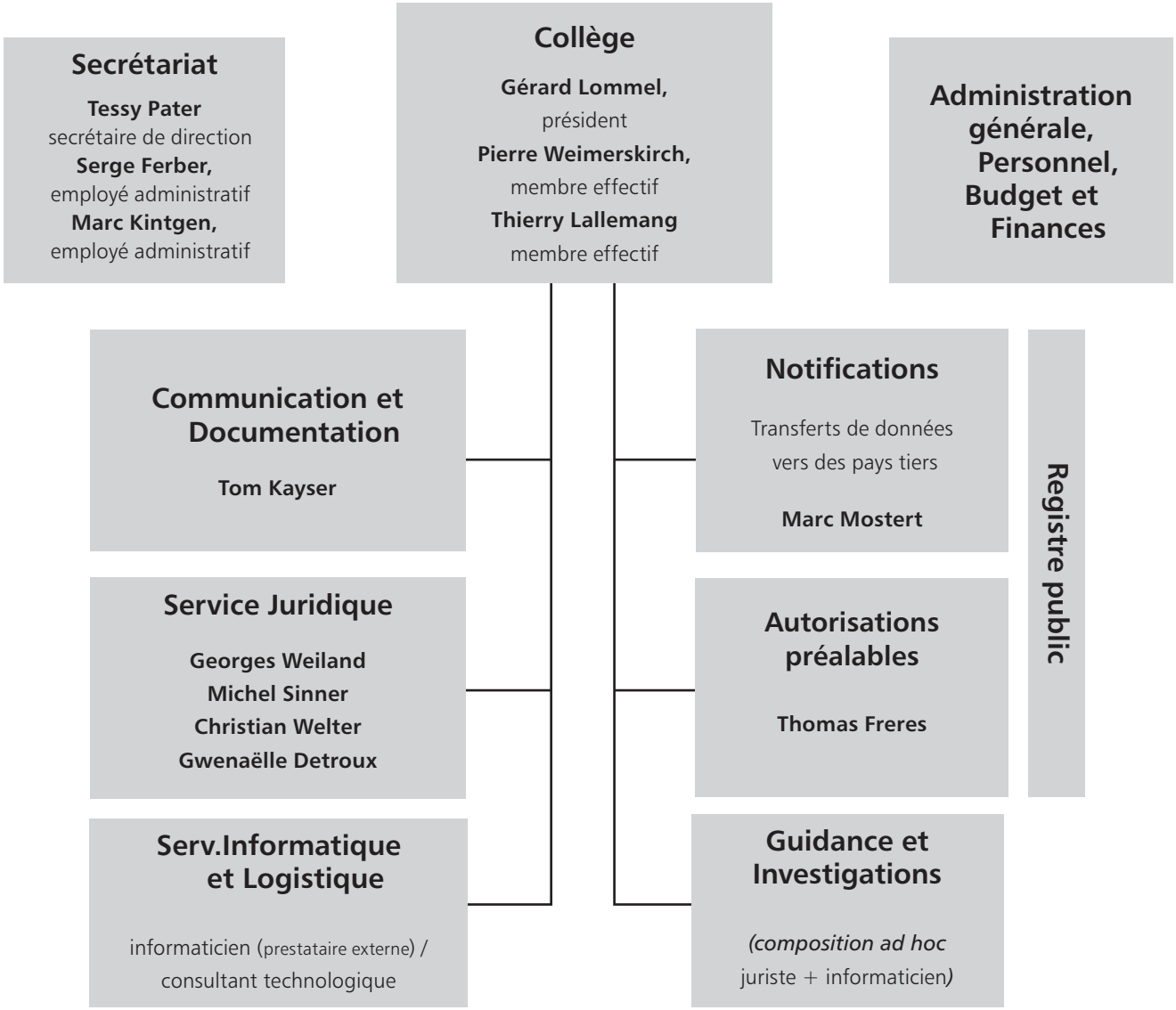
Conformément à son règlement intérieur, les services suivants ont été mis en place depuis 2003 :

- 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.

Collège	
	Gérard LOMMEL, Président Thierry LALLEMANG, membre effectif Pierre WEIMERSKIRCH, membre effectif
Membres suppléants	
	Josiane PAULY Marc HEMMERLING Tom WIRION
Service juridique	
	Georges WEILAND, attaché de direction Michel SINNER, attaché de direction Christian WELTER, attaché de direction Gwenaëlle DETROUX, 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	
	Informaticien (prestataire externe) Consultant technologies et sécurité (prestataire externe)
Secrétariat, administration générale et finances	
	Tessy PATER, secrétaire de direction Serge FERBER, employé administratif Marc KINTGEN, employé administratif
Service communication et documentation	
	Tom KAYSER, attaché de direction stagiaire

En 2009, un poste supplémentaire de rédacteur a été pourvu. Les effectifs permanents ont ainsi été portés de 11 à 12 fonctionnaires et employés publics (y compris les 3 membres permanents).

5.4 Organigramme de la Commission nationale



6 La Commission nationale en chiffres

Formalités préalables

	2003	2004	2005	2006	2007	2008	2009	
a) Notifications								**TOTAL**
- notifications ordinaires	2.646	850	500	250	760	385	345	5.736
- notifications simplifiées	750	900	720	890	537	-	-	3.797
- engagements de conformité	-	-	-	-	-	942	227	1.169
(Total a)	**3.396**	**1.750**	**1.220**	**1.140**	**1.297**	**1.327**	**572**	**10.702**
b) Autorisations préalables								
- demandes d'autorisation	765	406	317	295	392	606	542	3.323
- engagements de conformité	718	14	17	19	151	220	70	1.208
(Total b)	**1.483**	**420**	**334**	**314**	**543**	**826**	**612**	**4.531**
(Total général a) + b))	**4.879**	**2.170**	**1.554**	**1.454**	**1.840**	**2.153**	**1.184**	**15.234**
Déclarants (responsables ayant accompli des formalités)	2.220	2.500	2.850	3.300	3.754	4.357	4.772	

Demandes de renseignements

	2004	2005	2006	2007	2008	2009
a) Demandes de renseignements par courrier :						
- administrations publiques	18	7	8	6	5	11
- entreprises	49	10	8	5	12	8
- professions libérales	3	4	9	2	2	2
- citoyens	12	9	7	12	8	6
- associations	7	5	2	4	3	1
(Total a)	**89**	**35**	**34**	**29**	**30**	**28**
b) Demandes de renseignements par courriel :						
(Total b)	**67**	**82**	**116**	**119**	**108**	**110**
c) Demandes de renseignements par téléphone :						
(Total c)	**1.780**	**1.550**	**1.930**	**1.870**	**1.586**	**1.407**
(Total général a) + b) + c))	**1.936**	**1.667**	**2.080**	**2.018**	**1.724**	**1.711**

Plaintes et investigations

	2003	2004	2005	2006	2007	2008	2009
- plaintes, demandes de vérification de licéité et investigations :	**15**	**38**	**40**	**30**	**34**	**63**	**133**

Séances de délibération

	2004	2005	2006	2007	2008	2009
	39	**36**	**39**	**40**	**40**	**37**

Participations aux groupes de travail sur le plan européen

	2004	2005	2006	2007	2008	2009
	28	**33**	**23**	**22**	**22**	**32**

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

	2004	2005	2006	2007	2008	2009
- secteur public	**47**	**62**	**32**	**56**	**52**	**54**
- secteur privé	**30**	**38**	**12**	**40**	**44**	**52**
(Total)	**77**	**100**	**44**	**96**	**96**	**106**

Séances d'information, conférences, exposés

	2004	2005	2006	2007	2008	2009
	4	**10**	**11**	**14**	**11**	**23**

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

	2004	2005	2006	2007	2008	2009
Articles et interviews parus dans :						
- les quotidiens	**14**	**16**	**67**	**127**	**59**	**104**
- les hebdomadaires	**5**	**6**	**4**	**9**	**11**	**10**
- les mensuels	**0**	**7**	**5**	**4**	**2**	**1**
- les médias audiovisuels	**1**	**3**	**3**	**3**	**16**	**13**
(Total)	**20**	**32**	**79**	**143**	**88**	**128**

ANNEXES :

Avis et décisions

Avis de la Commission nationale pour la protection des données relatif aux mesures à prendre par les établissements bancaires en ce qui concerne les transactions personnelles effectuées par leurs salariés

Délibération n° 21/2009 du 30 janvier 2009

Faisant suite à la demande d'avis émanant de l'Association Luxembourgeoise des Employés de Banque et Assurance (ALEBA) du 30 juillet 2008 concernant le traitement de données personnelles relatif aux opérations sur titres personnelles des employés des établissements financiers, la Commission nationale précise ci-après sa position à l'égard des questions soulevées.

Comme l'ALEBA le souligne dans son courrier du 30 juillet 2008, les mesures en question se fondent sur le *règlement grand-ducal du 13 juillet 2007 relatif aux exigences organisationnelles et aux règles de conduite dans le secteur financier et portant transposition de la directive 2006/73/CE de la Commission du 10 août 2006 portant mesures d'exécution de la directive 2004/39/CE du Parlement européen et du Conseil en ce qui concerne les exigences organisationnelles et les conditions d'exercice applicables aux entreprises d'investissement et la définition de certains termes aux fins de ladite directive*. Le règlement précité prévoit que « *les établissements de crédit et les entreprises d'investissement doivent établir, mettre en œuvre et maintenir des dispositifs adéquats en vue d'empêcher* » certaines transactions personnelles de la part de ses salariés.

L'article 5, paragraphe (1) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel dispose que le traitement peut être effectué s'il est « *nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis* ».

Eu égard à l'obligation légale des établissements financiers susmentionnés résultant du règlement grand-ducal du 13 juillet 2007 précité et d'autres textes légaux, le recours à un traitement de données personnelles leur permettant d'avoir connaissance de certaines transactions personnelles de leurs salariés est légitime au sens de l'article 5, paragraphe (1) précité.

Force est cependant de constater que le règlement grand-ducal du 13 juillet 2007 ne donne que peu de détails concrets relatifs à la mise en place des « dispositifs adéquats » en question.

En tout état de cause, le traitement de données personnelles effectué doit être conforme aux principes de finalité, de nécessité et de proportionnalité résultant notamment de l'article 4, paragraphe 1er de la loi modifiée du 2 août 2002 :

« *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 ;

(…) »

Quant aux salariés concernés

Il est certain que parmi les différentes natures de fonctions professionnelles existant au sein d'un établissement financier, toutes ne sont pas visées par l'article 12 du règlement grand-ducal du 13 juillet 2007.

Chaque établissement financier doit déterminer, parmi les membres de son personnel, ceux tombant dans le champ d'application de la disposition précitée.

A l'égard des salariés autres que ceux visés par l'article 12, le traitement ne serait ni légitime au sens de l'article 5 de la loi modifiée du 2 août 2002, vu l'absence d'une obligation légale, ni nécessaire au sens de l'article 4 de cette loi.

Le cas échéant, parmi les salariés concernés, des distinctions peuvent encore être faites entre différentes fonctions, afin que les « dispositifs adéquats » à adopter par les établissements financiers soient adaptés aux responsabilités respectives des salariés concernés.

Enfin, pourraient également faire l'objet des mesures en question les salariés qui tombent dans le champ d'application de l'article 12 du règlement, non pas par la nature de leur fonction professionnelle proprement dite mais en raison des fonctions qu'ils occupent en leur qualité de représentant du personnel.

Quant aux données traitées

L'article 12 paragraphe (2), lettre b) du Règlement grand-ducal du 13 juillet 2007 ainsi que la directive 2006/73/CE disposent que l'entreprise est « *informée sans délai de toute transaction personnelle réalisée par une personne concernée, soit par notification de toute transaction de ce type, soit par d'autres procédures permettant à l'entreprise d'identifier ces transactions*. »

Selon les informations fournies par l'ALEBA, certains établissements financiers obligent leurs employés à fournir les numéros des comptes bancaires, ainsi que l'indication des établissements bancaires, sur lesquels ils peuvent réaliser des transactions personnelles sur titres.

La Commission nationale estime que l'établissement financier employeur devrait se borner à demander à son salarié de déclarer les transactions personnelles qu'il effectue sans exiger la communication du numéro du compte-titre et du nom de l'établissement bancaire auprès duquel le compte titre a été ouvert pour ce qui est des comptes ouverts auprès d'autres établissements que l'établissement employeur. En revanche, la banque peut légitimement demander à ses salariés les numéros des comptes dont ils sont titulaires auprès de cette banque-même.

Quant aux destinataires des données

Par application des principes de nécessité et de proportionnalité, le nombre des destinataires des données devrait être limité au strict minimum nécessaire et ne pas être excessif au regard des finalités recherchées.

Ainsi, il doit être évité que des personnes pouvant influer sur les avancements éventuels du salarié puissent avoir accès aux données. Il serait par exemple inadmissible que le fait que le salarié dispose d'un compte-titres auprès d'un établissement concurrent de son employeur soit susceptible d'avoir une quelconque incidence sur ses promotions. Une utilisation des données à de telles fins n'ayant aucun rapport quelconque avec le but originaire du traitement correspondrait d'ailleurs à un détournement de finalité contraire à l'article 4, paragraphe 1er, lettre (a) de la loi modifiée du 2 août 2002

De même, il convient d'éviter que les supérieurs hiérarchiques ou les collègues directs des personnes concernées puissent avoir connaissance du contenu des données. Les supérieurs hiérarchiques peuvent seulement être mis au courant une fois qu'un abus a été constaté.

Il appartient à l'établissement financier de déterminer avec précision les personnes recevant communication des informations sur les transactions personnelles des salariés. Par ailleurs, en application de l'article 26, paragraphe (1), lettre (c) de la loi modifiée du 2 août 2002, les salariés concernés par le traitement doivent être informés sur ces destinataires.

Quant à la question des comptes pour lesquels des salariés ont une procuration

L'ALEBA indique que les renseignements à fournir par les employés des établissements financiers concernent aussi bien les comptes-titres propres des employés que ceux pour lesquels les employés disposent d'une procuration.

L'article 11, lettre b) du Règlement grand-ducal du 13 juillet 2007 prévoit expressément l'hypothèse des opérations effectuées par la personne concernée pour le compte d'une personne avec laquelle elle a des liens familiaux ou des liens étroits ainsi que celles effectuées pour « *une personne dont le lien avec la personne concernée est tel que cette dernière a un intérêt direct ou indirect important dans le résultat de l'opération, autre que le versement de frais ou commissions pour l'exécution de l'opération*. »

On peut également admettre que les risques d'abus liés aux transactions personnelles effectuées par le salarié pour son propre compte sont similaires à ceux liés aux transactions personnelles effectuées pour le compte de tiers.

Les mesures à prendre par les établissements financiers seraient donc certes insuffisantes si les comptes de tiers, pour lesquels des salariés ont une procuration, n'étaient pas pris en compte.

Dès lors, cette pratique semble légitime à la Commission nationale, à condition, bien entendu, que le salarié ayant reçu la procuration, fasse effectivement partie du cercle de ceux visés par l'article 12 du règlement grand-ducal du 13 juillet 2007.

Les tiers ayant donné une procuration à un employé sont alors à considérer comme des personnes concernées par le traitement au sens de loi modifiée du 2 août 2002. Cela implique qu'ils bénéficient de tous les droits attachés à cette qualité. Ainsi, leur droit à l'information et leur droit d'accès tels que prévus par la loi modifiée du 2 août 2002 doivent être respectés.

Avis de la Commission nationale pour la protection des données concernant 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

Délibération n° 48/2009 du 10 mars 2009

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'aviser « *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 que la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet 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.

Elle constate, à titre liminaire, que le projet de loi sous examen ne comporte pas de modification en profondeur du système existant en matière d'identification numérique des personnes physiques, et ce malgré les problèmes soulevés en pratique et ayant fait l'objet de discussions avant le projet de modification de la législation actuelle.

Avant de proposer ses réflexions et propositions au sujet du projet de loi sous examen, la Commission nationale estime qu'il est nécessaire de rappeler les préoccupations et intérêts en cause dont le législateur se doit de tenir compte et, plus particulièrement, les exigences de droit communautaire en matière d'identification numérique des personnes physiques.

I Introduction

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[1].

Concomitamment à la création de ce comité, la Chambre des Métiers a élaboré deux rapports relatifs à la réduction des charges administratives[2] dans lesquels elle estime nécessaire la mise en place rapide d'une politique de simplification administrative.

Le Conseil du Gouvernement a reçu du CNSAE une note du 31 mars 2006 intitulée « *identifiant unique* » qui suggère la révision de la loi du 30 mars 1979 instituant l'identification numérique des personnes. Suite à cette note, un groupe de travail interministériel ad hoc « *identifiant unique* » 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 n° 1.056 posée par l'honorable députée Madame Colette Flesch[3], 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*

1 La ligne « Directrice Intégrée 14 » prévoit que « *le gouvernement accordera une priorité à la simplification des formalités qui freinent le rendement et l'esprit d'initiative des PME* »

2 Réduction des charges administratives Perspectives d'une future politique de simplification administrative au Luxembourg, Centre de Promotion et de Recherche, décembre 2004

3 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.

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 morale en général et l'utilisation du numéro d'identité en particulier ».

Le CNSAE a remis son rapport « Entfesselungsplang fir Betriber » en février 2007.

Ce rapport a mis en exergue cinq préalables à la simplification administrative, l'un d'eux étant la mise en place d'un identifiant unique[4].

Ce rapport précise encore ce qui suit :

« L'identifiant numérique instauré par la loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales et les pratiques administratives s'y attachant doit être revu. (…)

Un nouveau système d'identification des personnes physiques et des entreprises répondant à la fois à la simplification administrative et aux exigences de protection des personnes à l'égard du traitement des données à caractère personnel s'avère nécessaire. (…)

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 publiques, ASBL, fondations, etc.) et un répertoire distinct pour les personnes physiques a été approuvée par le Conseil en Gouvernement.[5] »

Il ressort de ce qui précède que le groupe interministériel était confronté à deux problèmes 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[6].

Dès lors, le groupe de travail interministériel précité avait pour mission de parvenir à une simplification administrative tout en y intégrant de nouvelles garanties en termes de protection des données.

La Commission nationale a été consultée périodiquement par ce groupe de travail.

Lors d'une première consultation, elle a suggéré au groupe de travail de se poser la question de savoir si la réforme allait ou non apporter une réponse 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 observait, en effet, que l'identifiant numérique était de plus en plus utilisé en dehors du cadre légal. Le groupe de travail a confirmé ceci car cet élargissement formait une demande réelle des acteurs du secteur privé.

La Commission nationale a alors donné à considérer que l'élargissement à certains acteurs privés de l'usage de l'identifiant unique pouvait s'envisager pour tenir compte de l'évolution de la société actuelle mais devait alors être accompagné de solutions novatrices en vue de renforcer les garanties robustes destinées à éviter des risques d'abus et cela au moyen de solutions technologiques modernes qui n'existaient pas lors de l'adoption de la législation actuelle.

La Commission nationale était bien consciente que la première direction proposée n'était pas envisageable ;

4 CNSAE « Entfesselungsplang fir Betriber » Février 2007, page 34

5 Id. page 77

6 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

en effet, les garanties prévues par la loi du 30 mars 1979 étaient cantonnées aux seules relations entre l'administré et les administrations. Par conséquent, l'élargissement du numéro d'identification à des acteurs du secteur privé devait conduire à rechercher une palette plus large de garanties juridiques et techniques encadrant l'utilisation et les flux de l'identifiant numérique.

La Commission nationale a donc plaidé pour une démarche audacieuse plutôt que frileuse et conservatrice et donc pour envisager la mise en place de garanties juridiques et technologiques nouvelles. Dans le cadre de pistes de réflexion, elle présentait les systèmes adoptés dans d'autres pays européens et qui donnaient satisfaction en termes de protection des données.

Elle ne peut donc cacher une certaine déception à la lecture du projet de loi sous examen alors qu'elle semble ne pas avoir été suivie au niveau de ses préconisations de s'inspirer des exemples d'autres pays et des dispositions visant à assurer les principes régissant la matière de la protection des données à caractère personnel.

II Préliminaires

Principes régissant la protection des données

Tous les pays européens n'ont pas mis en place un 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[7].

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[8] que l'utilisation d'un identifiant unique multisectoriel pouvait être inconstitutionnel[9].

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* »[10].

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* »[11].

C'est d'ailleurs, à la suite d'un projet concernant un identifiant national unique que la CNIL a été créée. En effet, vers 1974, les services du Ministère de l'Intérieur finalisaient un projet intitulé SAFARI (pour « Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus ») révélé par la presse. Ce projet prévoyait d'instituer un identifiant unique pour interconnecter tous les fichiers des administrations. La révélation de ce projet a suscité une vive émotion de l'opinion publique qui craignait un fichage général de la population. Face à cette protestation, le gouvernement avait alors institué une commission appelée « Commission Informatique et Libertés » auprès du Ministère de la Justice pour proposer des mesures garantissant le développement de l'informatique dans le respect de la vie privée, des libertés individuelles et des libertés publiques. Cette commission avait suggéré la création d'une autorité indépendante; le projet de loi y afférant a été examiné à la fin de l'année 1977 et la loi a été votée le 6 janvier 1978[12].

Le danger majeur de l'utilisation d'un identifiant numérique multisectoriel est donc la possibilité de croiser les informations contenues dans divers fichiers

7 Par exemple, l'article 35 de la constitution au Portugal

8 Bundesverfassungsgericht BVerfGE 65, 1 – Volkszählung, "Volkszählungsurteil"

9 eID Interoperability for PEGS, National Profile Germany, November 2007, IDABC, page 9 http://ec.europa.eu/idabc/en/document/6485/5938

10 Rapport du Comité pour la protection des données 1978, chapitre 29 paragraphe 6

11 Echos des séances du 28 avril 2006

12 Loi No 78-17 relative à l'informatique, aux fichiers et aux libertés

et relatives à une même personne. C'est comme si on pouvait créer un puzzle sur une personne à partir des différents éléments contenus dans les divers fichiers grâce à une clé unique : les informations sont éparpillées dans les fichiers d'administrations distinctes poursuivant des activités et missions ayant des finalités différentes entre elles et ces informations sont toutes rassemblées – ou sont susceptibles de l'être – 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.

De plus, les personnes peuvent avoir le sentiment d'être réduites à une suite de chiffres dans leurs rapports avec l'administration, mettant ainsi de côté le rapport humain.

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.

La Cour européenne des Droits de l'Homme a eu à se prononcer à plusieurs reprises sur l'identifiant unique[13].

Elle affirme que l'utilisation d'un identifiant unique peut dans certains cas entraîner la violation de l'article 8 de la Convention de sauvegarde européenne des Droits de l'Homme et des Libertés fondamentales.

Il est un fait que le principe de la mise en place et de l'utilisation d'un identifiant national unique et multisectoriel n'est pas interdit pas les normes internationales ou européennes.

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.* »

L'exposé des motifs annexé à la dite recommandation précise encore :

« *34. Un numéro de sécurité sociale peut faciliter l'interconnexion et la contre-vérification des dossiers, simplifiant ainsi considérablement l'exécution des tâches des institutions de sécurité sociale. Aux termes du paragraphe 5.1, le droit interne doit prévoir des garanties adéquates lorsqu'un Etat membre introduit un numéro de sécurité sociale uniforme et unique ou un moyen d'identification analogue ou en fait usage s'il existe déjà. On estime que de telles garanties sont souhaitables compte tenu des craintes que suscitent les identifiants. On peut redouter, par exemple, que l'introduction d'un numéro de sécurité sociale permette à des autorités qui exercent leurs activités en dehors du secteur de la sécurité sociale de se servir de ce numéro à leurs propres fins. Ce qui a été conçu à l'origine comme un numéro délivré à une fin particulière pourrait rapidement devenir un numéro standard, bon pour tous les usages. Des soupçons peuvent aussi surgir à l'égard du type d'informations figurant sur les cartes d'identification dont la finalité est analogue au numéro de sécurité sociale.*

35. C'est pour parer à ces craintes et ces soupçons que le paragraphe 5.1 parle de la nécessité d'accompagner de garanties adéquates l'introduction et l'utilisation de numéros de sécurité sociale. L'introduction de numéro standard répondant à tous les besoins ne devrait pas se faire de manière clandestine. Il conviendrait également de prévoir des garanties à l'égard des informations

13 Par exemple, Lindquist c/ Suède 10879/84, Lundvall c/ Suède 10473/83 et Kolzer c/ Suède 11732/85

figurant sur les cartes d'identification. Ces informations devraient, par exemple, être lisible et ne pas être excessives au regard de leur finalité ».

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.

Le Conseil de l'Europe relève des aspects juridiques et techniques[14].

Concernant les garanties juridiques, il peut par exemple s'agir d'un formalisme préalable à l'utilisation du numéro d'identification. A titre d'exemple, au Danemark, l'identifiant national ne peut être enregistré par les organismes privés que si la loi le prévoit ou en cas d'autorisation expresse de la personne concernée. 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 dudit 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.

Des systèmes qui offrent des garanties appropriées au niveau juridique et technique existent dans des pays européens : 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.

Le meilleur exemple mis en place est celui qui existe en Autriche. D'autres systèmes proposent également des garanties significatives.

Exemples de systèmes existant dans des pays européens

Le système autrichien : un modèle conciliant parfaitement la protection des données avec l'efficacité administrative [15]

L'Autriche a mis en place un système de communication électronique sécurisé dans lequel la protection des données à caractère personnel est pleinement assurée.

L'identification des personnes physiques s'effectue à partir des enregistrements existant dans un registre de base (*Basisregister*) et avec un numéro d'identification de base (*Stammzahl)*. Pour les personnes physiques, le Registre Central des Résidents est le plus important « *Zentrales Melderegister – ZMR* ».

14 « Le numéro personnel d'identification : leur mise en œuvre, leur utilisation et la protection des données »
Etude préparée par le Comité d'experts sur la protection des données en 1991

15 "Behörden im Netz. Das ¨sterreichische E-Government ABC " ainsi que "Best Practice Katalog. E-Government in Österreich", Bundeskanzleramt Österreich, éd. Digitales Österreich

Les registres contiennent un nombre nécessaire d'identifiants pour garantir que les personnes sont identifiées de manière fiable les unes par rapport aux autres.

Le nombre d'identification de base (*CRR- Central Residents Register* également appelé source-PIN) est généré à partir d'un nombre dérivé du numéro *ZMR – Ergänzungsregisterzahl* et d'une clé secrète qui est gardée par la Commission autrichienne de protection des données dans son rôle d'autorité du registre e-government. Le nombre CRR est exclusivement enregistré sur la « carte de citoyenneté » (*Bürgerkarte*) utilisée par son titulaire dans tous ses rapports avec les administrations.

Ce nombre CRR ne peut être traité qu'avec un logiciel sécurisé spécifique.

Il sert d'identifiant unique et remplit la fonction de source unique d'identification. Il est ainsi le point de départ pour la création des identités électroniques protégées.

En effet, dans les communications électroniques avec l'administration, les personnes physiques sont identifiées par un identifiant personnel sectoriel (ci-après : ssPIN). Ces ssPIN sont calculés en appliquant un procédé cryptographique sur la source-PIN et sur le secteur procédural spécifique à l'administration. Le ssPIN est différent pour chaque administration, de sorte qu'un ssPIN valide pour une autorité ne peut pas être employé pour obtenir des informations sur le titulaire du numéro par une autre administration.

En d'autres mots, les autorités publiques emploient différents identifiants personnels dérivés de la source-PIN de la personne physique et du secteur procédural considéré. La dérivation est basée sur une opération cryptographique irréversible, ce qui assure que la source-PIN ne peut pas être identifiée à partir de l'identifiant dérivé.

Les passerelles entre fichiers d'administrations différentes sont possibles grâce à une « plaque tournante informatique » par laquelle les flux de données sont tous contrôlés et tracés.

Les systèmes de gestion des données personnelles sont fortement encadrés par différents règlements afin de garantir un niveau de sécurité optimal tout en garantissant le flux de ces données entre les divers services de l'administration publique.

Ce modèle présente l'avantage indéniable de protéger pleinement les données des administrés, car le système repose sur un numéro de référence unique qui arrive à brasser et à créer d'autres numéros qui sont seulement connus des administrations concernées. Ainsi, par exemple, à partir du numéro sectoriel qui lui est attribué, l'administration de la santé ne peut pas accéder aux données détenues par d'autres administrations : si, dans le cadre de la simplification des démarches administratives, elle souhaite obtenir une information d'un organisme de sécurité sociale, elle fait une demande qui transite par la « plaque tournante informatique ». Toutes les opérations sont journalisées aux fins de vérification et de contrôles ultérieurs.

Il convient de noter que la carte de citoyenneté n'est pas seulement utilisée dans le cadre des relations de son titulaire avec les administrations publiques mais qu'elle sert également dans des applications mettant le citoyen en relation avec des acteurs privés comme les banques.

A défaut de la validation d'un échange de données, une administration ne peut avoir connaissance des données des citoyens contenues dans les fichiers des autres administrations.

Compte tenu de la parfaite adéquation entre le principe de protection des données et les principes de simplification et d'efficacité administratives, certains pays ont tenté d'importer ce modèle. Ainsi, le Préposé Fédéral suisse avait recommandé publiquement son adoption par la Confédération helvétique.

Même si le groupe de travail interministériel n'a pas retenu le modèle autrichien, probablement à cause de son degré de sophistication et de son coût économique, susceptible de dépasser le cadre approprié pour un pays de petite taille, la Commission nationale donne à considérer que ce système s'appuie sur des idées maîtresses intéressantes qui pourraient bel et bien être reprises au Luxembourg. Il est incontestable que ce système apporte une meilleure protection contre d'éventuels abus concernant les données des citoyens.

Le système belge

La Belgique a mis en place un ensemble de mesures pour promouvoir la simplification administrative. D'ailleurs, depuis 1998, l'Agence pour la Simplification Administrative (ci-après : ASA) fait des propositions pour simplifier les obligations légales et les procédures administratives. L'ASA est rattachée à la Chancellerie du Premier Ministre et elle est dirigée par un comité d'orientation tripartite.

L'attribution d'un numéro unique aux personnes physiques et aux entreprises poursuit deux objectifs distincts, à savoir 1) devenir un outil de la simplification administrative, car les utilisateurs utilisent désormais un seul et même numéro en lieu et place des différents numéros sectoriels attribués par les administrations et, 2) la mise en place d'une clé d'identification unique pour échanger les données entre administrations et parvenir ainsi à une collecte unique des données[16].

Le système belge a développé le système des sources authentiques.

Une source authentique est une base de données fiables mise à la disposition de tiers autorisés. Lorsqu'une administration est autorisée à consulter une ou des sources authentiques, elle ne peut plus demander ces mêmes données aux administrés.

Les données de différentes sources authentiques relatives à un domaine sont regroupées dans les banques-carrefours.

Ces banques-carrefours sont contrôlées par des comités sectoriels institués auprès de la Commission pour la protection de la vie privée.

Les comités sectoriels sont composés, à parts égales, de membres de ladite Commission pour la protection de la vie privée et d'experts du secteur concerné. La présidence des comités revient en théorie au président de la Commission pour la protection de la vie privée. Lors des votes, la voix du président est prépondérante en cas de partage de voix[17]. De plus, le « *président recherche la position commune susceptible d'être adoptée* »[18].

16 ASA Guide de Simplification administrative, chapitre II : le Numéro unique – février 2008

17 Article 12, paragraphe 5 du Règlement d'ordre intérieur des Comités sectoriels

18 Id. article, 12 paragraphe 3

Les comités sectoriels sont également chargés de délivrer les autorisations préalables d'accès et de communications des données se trouvant dans la banque-carrefour qu'ils sont chargés de surveiller. Pour ce faire, ils procèdent notamment à une analyse de la finalité recherchée et des mesures organisationnelles et techniques des opérations de traitement.

A l'heure actuelle, il existe six comités sectoriels :

- le Comité sectoriel du Registre national, créé par la loi du 8 août 1983 organisant un registre national des personnes physiques. Il veille à la sécurité et à la protection des données enregistrées dans le registre national des personnes physiques et il contrôle l'utilisation du numéro d'identification nationale. Il accorde à ce titre les autorisations d'accès et de communications des données à des catégories de personnes préalablement déterminées par une loi, un décret ou une ordonnance et dans le cadre de leurs activités également délimitées[19].

- le Comité sectoriel de la Banque-Carrefour des Entreprises a été créé par la loi du 16 janvier 2003 portant création d'une Banque Carrefour des Entreprises.

- le Comité sectoriel de la Sécurité Sociale et de la Santé, créé par la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale. Il veille à ce que les traitements de données à caractère personnel effectués dans le cadre des activités de sécurité sociale n'aient pas de répercussion sur la vie privée des assurés.

- le Comité sectoriel pour l'Autorité Fédérale, créé par une loi du 8 décembre 1992, surveille le flux électronique de données à caractère personnel au sein de l'administration fédérale.

- le Comité de surveillance sectoriel Phenix, créé par une loi du 10 août 2005, veille à la sécurité et à la confidentialité des traitements de données à caractère personnel effectués par l'appareil judiciaire belge.

- le Comité de surveillance statistique, créé par une loi du 4 juillet 1962, contrôle la communication par le Directeur général Statistique et Information économique, de données codées à des tiers ainsi que leur utilisation par des tiers.

19 Article 5 de la loi précitée du 8 août 1983

Le registre national des personnes physiques contient les données d'identification des résidents sur le territoire belge. Chaque personne reçoit un numéro d'identification personnel et unique. Ce numéro est composé de onze chiffres[20] : les six premiers correspondent à la date de naissance, les trois chiffres suivants sont des numéros d'ordre pour départager les personnes nées à la même date (tout en tenant compte du fait que les hommes se voient attribuer un numéro impair et les femmes un numéro pair), les deux derniers chiffres forment un nombre de contrôle. Il est donc possible de retrouver des informations à caractère personnel sur les titulaires à partir de leur numéro d'identification.

L'utilisation dudit numéro d'identification est subordonnée à une autorisation préalable du Comité sectoriel du Registre national.

Les banques-carrefours mènent les échanges de données à caractère personnel entre les institutions qui ont été préalablement autorisées : par exemple, lorsqu'une institution a besoin de certaines données à caractère personnel pour l'exécution de ses missions, le répertoire des références effectue automatiquement le routage de cette demande vers l'institution qui est la plus apte à mettre ces informations à disposition. Une réponse est ensuite transmise à l'institution demanderesse.

Les données sont donc communiquées et échangées dans le cadre d'un réseau en étoile.

Ainsi, un contrôle préventif de la légitimité des échanges est mis en place car l'échange est effectué conformément à l'autorisation du Comité sectoriel concerné et selon les modalités décrites ci-dessus. Quand une personne autorisée a besoin de certaines données pour l'exécution de sa mission, elle est obligée d'adresser sa demande par voie électronique à la banque-carrefour.

De plus, toutes les demandes d'informations sont enregistrées par la banque-carrefour ou par l'organisme de gestion d'un réseau sectoriel afin de pouvoir éventuellement tracer *a posteriori* tout détournement de finalité ou tout usage détourné des données sollicitées.

Les banques-carrefours disposent ainsi du répertoire de référence pour retracer les échanges.

Ce système présente toutefois moins de garanties que le modèle autrichien.

La situation en Suisse

La législation relative au numéro d'identification national a été modifiée par loi fédérale sur l'assurance-vieillesse et survivants (LAVS) du 23 juin 2006 et mise en vigueur par le Conseil fédéral, le 1er décembre 2007.

Avant l'entrée en vigueur de cette loi, le numéro d'identification était composé de onze chiffres et fournissait des informations sur son titulaire (date et lieu de naissance notamment). Ce système était très ressemblant à celui qui existe actuellement au Luxembourg.

Désormais, le numéro d'identification est composé de treize chiffres. De plus, il est non parlant et il est attribué de manière aléatoire.

La structure du numéro d'identification est inscrite dans la loi[21].

De plus, l'utilisation dudit numéro est encadrée : une loi doit autoriser au préalable son utilisation et doit identifier la finalité poursuivie ainsi que ses utilisateurs.

Il est utile de préciser que le nouveau numéro d'identification est utilisé depuis le 1er juillet 2008, soit environ une année et demie après l'entrée en vigueur de la loi du 23 juin 2006 précitée, ce qui démontre que la période de transition a été brève.

Malgré la mise en place rapide d'un numéro non parlant, qui ne dévoile plus des informations personnelles, et tout en reconnaissant les améliorations par rapport au système antérieur, le Préposé Fédéral suisse à la protection des données a regretté que le système soit moins exigeant en matière de protection des données. Il regrette que la loi ne prévoie pas de mesure pour prévenir les interconnexions 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

20 Arrêté Royal du 6 novembre 2007 portant modification de l'Arrêté Royal du 3 avril 1984 portant sur la composition du numéro d'identification des personnes inscrites dans le Registre national des personnes physiques (Moniteur Belge 11 janvier 2008)

21 Article 50c point 3

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. (…) »[22].

L'exemple du système français : les identifiants sectoriels et l'utilisation particulière du numéro d'inscription au répertoire national

Comme la Commission nationale le signalait précédemment, la France n'a pas recours à un identifiant national unique. Chaque secteur d'activité a recours à un identifiant sectoriel qui lui est propre.

Il existe un numéro d'inscription au répertoire national (ci-après : NIR) géré par l'INSEE, également appelé « numéro de sécurité sociale » car il est utilisé dans le secteur de la sécurité sociale. Ce numéro d'identification à treize chiffres est attribué à toute personne physique. Ce numéro est unique, deux personnes ne pouvant pas avoir le même numéro. Ce numéro est composé d'une série de caractères permettant de déterminer le sexe, la date et le lieu de naissance. Il est donc similaire dans sa composition et dans son utilisation initiale au numéro d'identification nationale luxembourgeois.

A notre connaissance, le NIR est utilisé dans un seul secteur en dehors du celui de la sécurité sociale à savoir dans le domaine fiscal : un amendement à la loi de finances pour 1999 du 18 novembre 1998 autorise, en effet, l'administration fiscale à utiliser le NIR dans un souci d'éviter les erreurs d'identité dans le cadre des échanges d'informations entre l'administration fiscale et les organismes sociaux. Le Conseil constitutionnel avait déclaré que cette utilisation du NIR était conforme à la constitution tout en y apportant des réserves d'interprétation car cette utilisation devait être assortie de plusieurs garanties, telles le secret professionnel renforcé et la circonscription de la finalité pour laquelle le numéro est utilisé[23].

La loi modifiée du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés contient également diverses dispositions en rapport avec le NIR.

Ainsi, l'article 27 dispose ce qui suit :

« I. Sont autorisés par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'Informatique et des libertés :

1° Les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat, d'une personne morale de droit public ou d'une personne morale de droit privé gérant un service public, qui portent sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques. »

L'article 25 dispose encore :

« I. Sont mis en œuvre après autorisation de la Commission nationale de l'informatique et des libertés, à l'exclusion de ceux qui sont mentionnés aux articles 26 et 27 : (…)

6° Les traitements portant sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques et ceux qui requièrent une consultation de ce répertoire sans inclure le numéro d'inscription à celui-ci des personnes. »

Ainsi, la CNIL a-t-elle un rôle important avant la mise en œuvre d'un traitement de données contenant le NIR et ce quand bien même ce numéro ne serait pas multisectoriel.

Dans le cadre de sa mission de contrôle, la CNIL admet que ce numéro soit utilisé dans l'ensemble des fichiers

22 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

23 Décision du Conseil constitutionnel No 98-406 DC du 29 décembre 1998 relative à la loi de finances rectificative pour 1998

des organismes en relation avec ce secteur (employeurs, services de prestations chômage, organismes d'assurance maladie obligatoires et complémentaires santé, professionnels de santé) mais exclusivement dans leurs relations avec les organismes de sécurité sociale[24].

Elle refuse, par exemple, son utilisation par des organismes de recouvrement de créance ou des établissements de crédits[25] en considérant qu'au « *regard des risques présentés par la généralisation de l'usage du NIR et de l'application du principe de proportionnalité défini à l'article 6-3° de la loi du 6 janvier 1978, l'utilisation du NIR par un organisme n'intervenant pas dans le secteur de la sécurité sociale, ne pouvait être admise que si elle correspondait à la poursuite d'un besoin d'intérêt général* ».

Elle a encore précisé que « *la lutte contre la fraude ou l'homonymie sont des finalités qui, bien que légitimes, ne suffisent pas, à elles seules, pour justifier l'utilisation du NIR dans le cadre de gestion de produits d'épargne, de gestion de crédits ou encore de recouvrement de créance. (…) Les mutuelles, les entreprises d'assurances et les institutions de retraite complémentaire et de prévoyance sont autorisés à utiliser le NIR pour l'exercice de leurs activités d'assurance maladie, de maternité, d'invalidité complémentaires et d'assurance vieillesse mais non pour la gestion de la relation commerciale. Pour la gestion de ses relations commerciales, chaque organisme doit se doter d'un identifiant spécifique* [26].

Elle a également affirmé que ce numéro ne pouvait pas servir d'identifiant spécifique du dossier médical[27].

**

Au vu des principes guidant la matière de la protection des données et tout en gardant à l'esprit l'intérêt de la simplification administrative, la Commission nationale se propose maintenant de présenter ses réflexions et commentaires au sujet de la loi susmentionnée.

24 Conclusions de la Commission Nationale de l'Informatique et des Libertés sur l'utilisation du NIR comme identifiant de la santé, février 2007

25 Autorisations du 23 février 2006

26 Même référence

27 Conclusions de la Commission Nationale de l'Informatique et des Libertés sur l'utilisation du NIR comme identifiant de la santé, février 2007

III Examen du projet de loi N° 5950

La Commission nationale entend limiter ses observations aux dispositions traitant des aspects de protection des données.

Elle rappelle qu'il n'est pas dans son intention que le principe d'un numéro d'identification uniforme et non équivoque soit abandonné en faveur de l'adoption d'un système reposant sur des numéros d'identification sectoriels. 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 constituer des garanties qui se révèlent aujourd'hui défaillantes et/ou d'adjoindre des mesures de protection nouvelles mettant à profit notamment de nouveaux progrès techniques, nous semble indispensable alors que le projet de loi sous examen est sensé préparer une nouvelle ère de l'administration publique dans la société de l'information.

1. Le registre national des personnes physiques (article 1er, 5 et 6)

La vocation centrale d'un registre national des personnes physiques comprenant l'identifiant numérique des citoyens ne soulève pas de difficultés en soi.

1.1. Les données figurant dans le registre

La liste des données figurant dans le registre diffère quelque peu de celle qui existe actuellement dans le répertoire général des personnes prévu à l'article 3, paragraphe (2) de la loi du 31 mars 1979.

Ainsi, l'état civil ne figure plus dans le registre, le projet de loi évoquant désormais la situation de famille [article 6, paragraphe (2), lettre (e)]. De plus, sont ajoutés les numéros d'identifications des pères et mères et/ou des enfants auprès de qui la filiation est établie. Le registre précise encore l'éventuel statut de réfugié ou de protection subsidiaire.

Il s'agit des données communes à toutes les administrations susceptibles de recourir au registre national : ces données permettent de donner une signalétique des personnes figurant dans le registre.

La Commission nationale estime que les données figurant dans le registre sont nécessaires et non excessives. Le catalogue des données est clairement circonscrit. Elle constate avec satisfaction qu'aucune donnée biométrique ne sera enregistrée dans ce registre.

Elle considère que le registre ne devrait pas contenir d'autres informations sur les titulaires des numéros d'identification nationale.

1.2. Le rôle du registre national

Le texte sous examen précise que le registre a pour finalité « *de regrouper toutes les données relatives à l'identification des personnes physiques, d'établir des statistiques et de préserver l'historique de ces données* »[28]. Il indique encore que ledit registre « *garantit la source authentique de certaines données enregistrées* »[29].

Les finalités sont larges car le registre est conçu pour répondre aux besoins d'administrations accomplissant des missions différentes. A l'instar du système belge, le registre assure la source authentique de données à caractère personnel, ce qui est conforme au principe selon lequel les données doivent être exactes, aux termes de l'article 4, paragraphe (1), lettre (c) de la loi du 2 août 2002.

2 Le choix de la structure de l'identifiant (article 2)

La Commission nationale relève tout d'abord que le texte sous examen ne donne pas de précision sur la nouvelle structure du numéro d'identification et qu'il faut se reporter à l'exposé des motifs pour obtenir quelques informations.

L'exposé des motifs précise que l'identifiant passe de onze à désormais treize chiffres. Dans un second temps, le numéro d'identification nationale serait non parlant. Il est encore précisé qu'un règlement grand-ducal sera pris à ces fins.

Il est regrettable que la loi ne fixe pas elle-même la structure envisagée, ni même ne mentionne qu'un règlement grand-ducal devra obligatoirement être pris à ces fins en termes de sécurité juridique. Il serait préférable que la loi le prévoie. La loi suisse précitée sur l'assurance vieillesse qui modifie la structure de l'identifiant unique précisait que ce dernier serait non parlant.

En l'absence de contrainte légale, le système actuel est susceptible de perdurer, avec les défauts et les insuffisances qui ont déjà été critiqués.

La Commission nationale regrette que les auteurs du projet de loi sous examen n'aient pas pris en compte le caractère singulier de l'identifiant unique en ce qu'il continue à contenir des informations à caractère personnel sur les personnes. Ces derniers envisagent certes la mise en place « *à terme* » d'un numéro aléatoire, c'est-à-dire non parlant, mais cette phase transitoire paraît, au vu des explications données dans l'exposé des motifs, particulièrement longue et excessive.

La Commission nationale n'est pas convaincue de la nécessité d'une phase transitoire avant la mise en place d'un système reposant sur un identifiant personnel non parlant, même si la migration technique doit avoir lieu dans cinq ans. La Suisse avait un système similaire à celui qui existe au Luxembourg et elle n'a pas eu recours à une phase transitoire ; qui plus est, la mise en place des numéros non parlants est devenue effective un an et demie après l'entrée en vigueur de la loi qui l'instituait.

De plus, la double migration envisagée par les auteurs du projet de loi sous examen présente de nombreux désavantages. En sus de son coût financier significatif, les travaux de migration technique doivent être répétés avec le risque d'erreurs que cela peut engendrer. A cela s'ajoute que le citoyen risque de ne pas comprendre qu'il va recevoir deux numéros d'identification. Cette situation paraît être en contradiction avec le principe de la simplification administrative.

28 Article 5 paragraphe (1)

29 Article 5 paragraphe (2).

3. L'utilisation élargie du numéro d'identification nationale (article 3)

Le texte de loi en projet énumère les catégories de personnes pouvant utiliser l'identifiant national, sans qu'il soit pour autant nécessaire, comme dans le système actuel, de prendre des règlements grand-ducaux d'application.

La Commission nationale n'est pas surprise de cet élargissement pour les raisons ci-avant exposées. Cette ouverture permet de régler des situations de fait qui existent actuellement sans cadre légal.

Elle note encore que l'énumération des catégories de personnes du secteur de la santé doit s'entendre comme étant restrictive. Tous les professionnels du secteur de la santé qui ne sont pas énumérés ne pourront donc pas utiliser le numéro d'identification.

Le projet de texte sous examen interdit dans le secteur privé l'utilisation du numéro d'identification comme clé de recherche et le fait de pouvoir continuer ce numéro à des tiers.

Toutefois, il ne prévoit pas de sanctions au non respect de cette disposition. A cela s'ajoute que cette interdiction est un leurre car, d'un point de vue technique, toute donnée peut servir de clé de recherche. Cette interdiction se trouve donc en décalage avec les réalités techniques actuelles.

Les abus actuellement constatés pourraient donc persister en l'absence de sanction prévue dans le texte.

Dès lors, la Commission nationale estime que la disposition relative à l'interdiction d'utilisation du numéro d'identification comme clé de recherche et le fait de le continuer à un tiers n'est pas une garantie suffisante du point de vue de la protection des données.

De plus, elle constate que le projet de loi indique une finalité pour recourir à l'utilisation de l'identifiant unique. Toutefois, cette finalité est si large qu'elle peut englober tout type de situation.

Il est vrai que la loi du 31 mars 1979 précisait déjà que le numéro était réservé à un usage administratif interne ou aux relations avec le titulaire du numéro ; mais les règlements grand-ducaux d'application donnaient toutes les précisions sur les administrations concernées, sur les documents et les actes en cause.

Le texte sous examen fait ainsi l'impasse sur le principe de finalité, principe pourtant cardinal en la matière de protection des données.

Cette situation est d'autant plus délicate que des acteurs du secteur privé peuvent désormais utiliser le numéro d'identification unique. La Commission nationale marque des réserves sur le libellé du paragraphe (4) relatif à l'utilisation de l'identifiant national dans le secteur privé : il peut être interprété de manière très large, de manière que toute personne pourrait justifier l'utilisation dudit numéro. Cela risque de conduire à la banalisation et à la divulgation incontrôlée du numéro d'identification.

En outre, le texte sous examen ne prévoit plus de contrôle *a priori* de l'utilisation du numéro d'identification.

Dans son rapport précité de 1991, le Conseil de l'Europe affirmait que « *la législation nationale à la protection des données doit expressément mentionner les garanties contre l'utilisation excessive des PIN* [numéros d'identification personnelle] ».

Dans le système actuel, le traitement est apprécié lors de l'élaboration des règlements grand-ducaux d'application de la loi du 31 mars 1979.

Il aurait été souhaitable que le projet de loi sous examen prévoie des garanties au respect du principe de finalité.

A ce titre, la Commission nationale rappelle que le numéro d'identification nationale constitue une donnée à caractère personnel au sens de l'article 2 de la loi du 2 août 2002. Aux termes de son article 12, les traitements de données personnelles doivent être notifiés sauf dans les cas où ladite loi prévoit des exemptions de notification[30].

Lors de l'examen des notifications préalables, la Commission nationale sera en mesure de contrôler le respect des dispositions de l'article 6, paragraphe (1), lettre (b) de la directive précitée du 24 octobre 1995 aux termes duquel les données à caractère personnel doivent

30 Ne sont pas non plus soumis à notification les traitements qui relèvent des dispositions prévues aux articles 8, 14 et 17 de la loi (article 12, paragraphe (1), lettre (a))

être « *collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités* ».

Par conséquent, et dans un souci de transparence et de sécurité juridique, la Commission nationale préconise l'ajout à la fin de l'article 3 d'un paragraphe additionnel rappelant l'obligation de notification de ces traitements.

4. La problématique du traçage des éventuels échanges de données entre les personnes autorisées à utiliser le numéro d'identification nationale

Bien que l'échange de données entre les administrations détenant l'identifiant unique n'ait pas été abordé dans le projet de loi sous examen, ni même dans l'exposé de ses motifs, la Commission nationale entend présenter les observations qui suivent.

La possibilité d'échanger des informations entre administrations au moyen du numéro d'identification surgit en filigrane de la volonté de parvenir à la simplification et à l'efficacité administrative. Dans son rapport, la CNSAE évoque d'ailleurs les échanges et partages des données entre les administrations gouvernementales[31].

La Commission nationale est d'avis que de tels échanges, respectivement interconnexions, ne sont pas interdits en soi, mais ne devront s'opérer que dans le respect de garanties techniques et juridiques solides inscrites dans la loi.

Ainsi il faut souligner que certains pays qui ont mis en place des cadres légaux facilitant l'échange, respectivement les interconnexions, de fichiers entre administrations ont également prévu des garanties techniques et légales.

En Autriche tous les échanges, respectivement les interconnexions, de fichiers entre administrations passent par une « plaque tournante » centrale et sont contrôlés, autorisés et journalisés par l'autorité de protection des données.

En Belgique l'utilisation du numéro d'identification est subordonnée à une autorisation préalable du Comité sectoriel du Registre national. Les échanges, respectivement interconnexions, de fichiers entre administrations sont effectués à travers les différentes banques-carrefours et seront soumis à l'autorisation du Comité sectoriel concerné. Les banques-carrefours disposent d'un répertoire de référence pour retracer les échanges.

Au Luxembourg, de tels échanges, respectivement interconnexions, doivent expressément être prévus par un texte légal ou réglementaire, sinon faire l'objet d'une autorisation préalable de la Commission nationale.

Les textes légaux ou réglementaires autorisant une interconnexion de données doivent respecter le *ratio* des dispositions de l'article 16 de la loi du 2 août 2002[32]. Conformément à son paragraphe (1), l'interconnexion peut valablement être autorisée par voie légale.

Son paragraphe (3) traite 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 appropriée et 4) la qualité des données faisant l'objet de l'interconnexion.

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[33]. 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.

31 Par exemple, point 2.3.7. du rapport Entfesselungsplang fir Betriber précité

32 Documents parlementaires N° 4735/13, page 30

33 « 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

Ensuite, 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.

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. De plus, le recours aux fichiers interconnectés doit être justifié.

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 sont traitées loyalement et licitement et ne sont 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.

Conformément aux vues du Conseil d'Etat le cadre légal luxembourgeois considère l'interconnexion de données comme une opération délicate qui doit être entourée d'un maximum de garanties[34]. Toutefois, l'absence d'une « plate-forme centrale » comme celles des systèmes autrichien ou belge ne facilite par un contrôle à postériori des échanges des données effectuées.

5. Quant au droit d'accès à l'historique de consultation du registre national des personnes physiques

La Commission nationale est satisfaite de la mise en place d'une journalisation des consultations du registre national des personnes physiques.

Elle s'interroge toutefois de l'intérêt pratique de cette garantie technique : en effet, le registre en question ne contient que la signalétique des individus. Si des administrations veulent s'échanger entre elles des informations sur les administrés autres que les données d'identification, elles ne vont pas consulter le registre national des personnes physiques.

6. La Commission du registre national (article 12)

L'article 12 *in fine* du projet de loi sous examen dispose qu'un règlement grand-ducal « *peut être pris pour déterminer la composition et le fonctionnement de la commission* ».

La Commission nationale estime que la composition et le fonctionnement de cette commission sont d'une importance majeure. Elle suggère que le projet de loi sous examen pose les lignes directrices de sa composition et de son fonctionnement, respectivement qu'un règlement grand-ducal soit effectivement pris concomitamment avec la loi, sinon dans un délai particulièrement rapproché.

Elle se propose, par ailleurs, de participer à cette commission et d'y jouer une influence suffisante pour contrôler et apprécier le fonctionnement du registre national des personnes physiques à l'aune des principes de protection de données. A l'instar des comités sectoriels belges, cette influence peut se traduire par l'attribution d'un droit de vote prépondérant lors des séances de vote.

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

7. Quant aux données biométriques nécessaires à l'établissement des cartes d'identité

La Commission nationale marque sa satisfaction au fait que les données biométriques ne figureront pas dans des bases de données centralisées, elles sont uniquement conservées à titre préventif pendant les deux mois qui suivent la délivrance de la carte d'identité.

Cette conservation est nécessaire et justifiée.

Elle note également qu'aucune empreinte digitale ne sera collectée dans le cadre de la confection des cartes d'identité.

L'article 24, paragraphe (2) du texte sous examen précise qu'un règlement grand-ducal « *peut déterminer les normes et les simplifications techniques et fonctionnelles auxquelles doivent satisfaire les appareils et les applications qui rendent possible la lecture et la mise à jour des données prises de manière électronique dans la carte d'identité* ».

La Commission nationale est d'avis que ce règlement grand-ducal devrait être pris en même temps que la loi. Il est en effet primordial que des mesures de sécurité technique et technologique soient prises pour protéger les données insérées dans la carte à puce, et notamment le numéro d'identification nationale.

Comme pour les passeports biométriques, la puce qui sera contenue dans la carte d'identité pourra être lue à distance. Il existe en théorie un risque de lecture cachée des informations de cette carte à puce.

Le Règlement (CE) 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyages contraint les États membres à instaurer des normes de sécurisation pour la lecture de la carte à puce.

Il serait nécessaire que ces normes de sécurisation soient également arrêtées avant la délivrance des premières cartes d'identité soit dans un règlement grand-ducal, comme l'envisage le texte sous examen, soit dans le corps même du texte du projet de loi sous examen afin de leur donner une valeur contraignante.

Avis de la Commission nationale pour la protection des données concernant l'avant-projet de règlement grand-ducal instituant le « chèque-service accueil »

Délibération n° 49/2009 du 16 janvier 2009

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'aviser « *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 que la Commission nationale entend présenter ci-après, dès ce stade officieux de la procédure et connaissant les délais à respecter, ses réflexions et commentaires au sujet de l'avant-projet de règlement grand-ducal instituant le « chèque-service accueil », de façon à ne pas différer la politique de mise en œuvre du gouvernement.

Tout en voulant apporter son soutien dans la mise en œuvre d'une mesure importante du gouvernement sur le plan social et familial, la Commission nationale aimerait néanmoins exprimer sa préoccupation quant à un point particulièrement délicat.

Lors d'une première entrevue en date du 10 novembre 2008 avec les responsables du Syndicat Intercommunal de Gestion Informatique (SIGI), à laquelle un représentant du Ministère de la Famille a assisté, la Commission nationale n'a pas manqué d'exprimer ses réticences à voir collecter les données relatives aux revenus des ménages demandeurs au niveau des administrations communales. Lors d'une nouvelle réunion en date du 7 janvier 2009, les représentants du Ministère de la Famille ont indiqué qu'ils entendaient maintenir cette optique tout en veillant à ce que les administrations communales, compétentes pour les formalités d'inscription pour les cartes d'adhésion au chèque-service, ne conservent aucune trace des pièces justificatives quant aux revenus des citoyens demandeurs.

La Commission nationale, ayant examiné l'avant-projet de règlement grand-ducal instituant le chèque-service accueil, ne peut néanmoins aviser favorablement les modalités d'adhésion à ce service qui sont prévues par l'article 10 dudit avant-projet.

En effet, cet article de l'avant-projet dispose que la collecte des données sur la situation de revenu du ménage des parents est effectuée sous la responsabilité de l'administration communale.

Quand bien même le Ministère de la Famille pourrait légitimement invoquer la nécessité de recueillir ces données afin de classer les bénéficiaires des cartes dans une des catégories de tarif, la Commission nationale est amenée à penser que cette finalité du traitement relatif au chèque-service lui devra être seule réservée, et elle maintient dès lors ses réserves face à l'idée d'obliger les administrés à dévoiler leur situation patrimoniale à leur administration communale.

La Commission nationale pense également qu'une telle procédure risque de créer un précédent de mauvais augure alors que d'autres ministères ou administrations publiques seraient éventuellement tentés de recourir aux autorités communales en tant que sous-traitants pour d'autres démarches administratives allant dans le même sens et nécessitant de la part des administrés des données confidentielles voire même « sensibles ». Si certaines catégories de personnes concernées ne verraient alors pas d'objection à consentir à une telle transmission de leurs données à caractère personnel, d'autres y seraient découragés en redoutant une curiosité malsaine de la part des agents communaux.

L'idée d'avoir recours aux communes comme structure de réception et d'inscription des demandes du chèque-service est certes louable, alors que celles-ci facilitent la démarche administrative en raison de leur proximité vis-à-vis des citoyens, mais ce même caractère de proximité (notamment dans les petites communes) ne manquera

pas de s'avérer préjudiciable à la protection de la vie privée des citoyens. Le fait de révéler des données de revenus aux agents communaux qui viendraient à connaître non seulement les situations financières des ménages en besoin, mais de toutes les personnes voulant bénéficier des chèques-service, ce qui sera probablement le cas de la totalité des familles ou personnes ayant des enfants à charge, est, selon l'avis de la Commission nationale, inconciliable avec le principe de proportionnalité inscrit à l'article 4 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement de données à caractère personnel.

Confronté à la perspective de l'introduction du traitement de ces données de la part des autorités communales qui comporte un caractère intrusif dans la sphère privée des administrés, la Commission nationale aimerait relever le principe du paragraphe 2 de l'article 8 de la Convention Européenne des Droits de l'Homme qui dispose qu'il ne peut y avoir ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée et familiale que pour autant que cette ingérence soit prévue par la loi, ce qui n'est pas le cas en l'espèce.

À la lecture du texte de l'avant-projet de règlement grand-ducal et en tenant compte de la proposition purement verbale de la part du Ministère de la Famille consistant à ne pas voir mémoriser les données sur la situation de revenu des ménages au niveau communal, cette solution pratique semble inappropriée alors que si les agents communaux doivent d'un côté respecter une certaine rigueur administrative, il leur sera enlevé de l'autre côté la possibilité de garder une preuve justifiant sans équivoque la décision administrative (classement dans une des catégories de tarifs) en cas de réclamations ou de contestations. Par ailleurs, le libellé de l'article 10 de l'avant-projet de règlement n'exclut pas la possibilité pour les communes de garder malgré tout copie intégrale des documents relatifs à la situation de revenu du ménage présentés par les demandeurs.

La Commission nationale ne peut pas non plus approuver la solution proposée qui consiste à laisser aux parents ou représentants légaux la faculté de communiquer ou non les données sur la situation de revenu du ménage afin de pouvoir bénéficier du chèque-service alors que cela reviendrait à laisser aux personnes concernées de « choisir le moindre mal » dans le sens que les citoyens, soucieux de leur vie privée ou réticents à dévoiler leurs revenus, seraient alors soumis au plein tarif.

La Commission nationale estime dès lors qu'il semble indispensable de repenser la procédure envisagée et l'architecture de l'application informatique, de façon à limiter aux seuls services du Ministère de la Famille et de l'Intégration le traitement des données relatives aux revenus des demandeurs sans remettre en question la collecte et/ou la consultation des autres données au niveau communal respectivement à celui des prestataires.

À titre de comparaison, la Commission nationale voudrait rapprocher le présent cas à la récente loi sur le boni pour enfant dans laquelle le législateur avait expressément prévu une disposition spéciale autorisant la Caisse nationale des prestations familiales à recevoir directement communication des données de l'Administration des contributions directes.

Ainsi, en l'absence d'une telle base légale similaire et étant d'avis que les données sur la situation de revenu des ménages devraient uniquement être recueillies et traitées par le Ministère de la Famille, la Commission nationale voudrait suggérer au Ministère de la Famille de demander aux personnes concernées, lors de l'inscription à la commune, leur consentement afin que seul ledit Ministère de la Famille puisse obtenir communication des données nécessaires par l'Administration des contributions directes.

Avis de la Commission nationale pour la protection des données au sujet du projet de loi n° 5986 relatif à l'accès des autorités judiciaires, de la Police et de l'Inspection générale de la Police à certains traitements des données à caractère personnel mis en œuvre par 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

Délibération n° 63/2009 du 3 avril 2009

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'aviser « *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 à elle adressée par Monsieur le Ministre de la Justice, que la Commission nationale pour la protection des données entend présenter ici ses réflexions au sujet du projet de loi n° 5986 déposé à la Chambre des Députés le 29 janvier 2009 ayant pour objet de modifier, remplacer, voire compléter des dispositions de l'ancien projet de loi n° 5563 ayant donné lieu à la loi du 22 juillet 2008 relative à l'accès des magistrats et officiers de la police judiciaire à certains traitements de données à caractère personnel mis en œuvre par des personnes morales de droit public et portant modification :

- du Code d'instruction criminelle
- de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection Générale de la Police, et
- de la loi modifiée du 27 juillet 1997 portant réorganisation de l'administration pénitentiaire.

Selon l'exposé des motifs, le projet de loi sous examen se propose de modifier des dispositions légales nouvellement introduites par la loi du 22 juillet 2008 en raison de difficultés pratiques et opérationnelles constatées lors de sa mise en œuvre, alors que certaines requerraient, semble-t-il, la mobilisation de ressources disproportionnées par rapport aux objectifs poursuivis.

Il est vrai que la presse s'est fait l'écho des difficultés d'application apparues dans le contexte de la constatation des infractions à la législation relative à la circulation routière (recouvrement des avertissements taxés en cas de stationnement irrégulier) alors que le seuil de gravité permettant une consultation du fichier des véhicules routiers, tenu par le Ministère des Transports, est fixé à une peine correctionnelle dont le maximum correspond à ou dépasse deux années d'emprisonnement. S'agissant d'une simple contravention, ledit critère ne se trouve pas rempli en l'espèce et la consultation du fichier en question apparaît effectivement contraire aux dispositions légales en vigueur.

Le projet de loi sous examen ne se limite cependant pas à résoudre le problème apparu en matière d'avertissements taxés pour infractions bénignes à la législation sur la circulation, mais entend assouplir également un certain nombre de restrictions, conditions, modalités inscrites dans la loi comme mesures de sauvegarde destinées à éviter un recours disproportionné à l'accès à ces fichiers administratifs publics.

Il convient d'avoir présent à l'esprit que les objectifs de ces dispositions tendent à garantir la préservation des libertés et des droits fondamentaux des citoyens concernés par les renseignements inscrits dans les banques de données administratives auxquelles la loi ouvre l'accès, notamment à la Police, par système informatique direct.

Il est donc de notre devoir d'appeler le législateur à ne pas considérer trop facilement que la limitation des accès à certaines finalités et conditions, à certains fonctionnaires, à certaines données ou fichiers ou que les modalités de traçage informatique nécessiteraient des efforts, moyens ou contrôles disproportionnés sans avoir préalablement mis en balance soigneusement l'utilité dans l'activité judiciaire et policière avec les atteintes potentielles aux droits fondamentaux et à la protection de la vie privée des citoyens.

Contrairement à la façon avec laquelle les milieux des forces de l'ordre posent parfois le débat, le projet de loi a en effet pour objet d'ouvrir l'accès à ces bases de données aux organes de la Justice et de la Police et non pas de refuser une telle faculté aux agents de police judiciaire dans certaines situations ou hypothèses où ils en auraient déjà bénéficié précédemment.

Notre Commission nationale se doit d'emblée de saluer la démarche prudente et le souci de légalité qui a présidé à l'élaboration du projet de loi n° 5563 ainsi qu'au projet de loi sous examen dans un esprit de respect des libertés publiques et des droits fondamentaux des citoyens et de considération des besoins de la lutte contre la criminalité et de la constatation des infractions pénales dans le strict respect de l'article 8 de la Convention européenne des Droits de l'Homme et notamment des principes de proportionnalité inscrits à son 2ème paragraphe.

Aux vœux de la directive européenne 95/46/CE du 24 octobre 1995 transposée par notre loi modifiée du 2 août 2002 sur la protection des données personnelles, l'utilisation ultérieure de données à caractère personnel de manière incompatible avec les finalités primaires (intérêts publics poursuivis par les fichiers d'autres autorités et administrations) pour lesquelles elles ont été initialement collectées doit être légitimée expressément, notamment par l'adoption d'un texte légal. Le mérite revient au Ministre de la Justice d'avoir voulu régler cette matière délicate par un projet de loi clair et précis.

Aussi notre Commission nationale avait-elle dans son avis du 4 mai 2005 relatif à l'avant-projet de loi ayant précédé l'adoption de la loi du 22 juillet 2008 encouragé le gouvernement à soumettre au parlement un texte qui détermine limitativement les fichiers publics concernés, les catégories de données ouvertes à la consultation et les finalités de la consultation. Dans cet avis elle préconisait également d'instaurer des mesures techniques assurant la sécurité du système, le retraçage des données accédées ainsi que des motifs de la consultation et permettant le contrôle du respect des restrictions prévues par la loi.

Le texte du projet de loi n° 5563 déposé à la Chambre des Députés par M. le Ministre de la Justice avait recueilli l'avis favorable de notre Commission nationale qui avait jugé qu'il représentait un compromis équilibré entre les intérêts d'efficacité du travail de la Police et de la Justice et les libertés publiques et droits fondamentaux des citoyens.

Certains amendements opérés par la suite aux cours des travaux parlementaires sont venus renforcer le caractère restrictif des nouvelles facilités d'accès informatique aux fichiers d'autres administrations publiques dans le souci d'éviter qu'elles ne prennent une ampleur excessive au sens de l'impératif de proportionnalité de l'article 8, paragraphe 2 de la Convention européenne des Droits de l'Homme.

S'il est souhaité aujourd'hui d'apporter un peu de souplesse à certaines de ces dispositions ayant donné lieu à des difficultés d'applications incontestables, il faudra à notre avis cependant préserver l'essentiel des garanties dont le législateur avait souhaité entourer, il y a seulement quelques mois, l'ouverture des banques de données publiques à la consultation par la Police et la Justice, à savoir :

- détermination claire du périmètre à une liste limitative de banques de données énumérée expressément dans la loi ;
- limitation des catégories de données ouvertes à la consultation et notamment exclusion des données de santé ;
- exigence d'un motif précis justifiant la consultation et journalisation des accès (informations consultées, par qui, pourquoi) permettant de déceler d'éventuels abus ;
- limitation des données consultées aux informations pertinentes et nécessaires dans le strict respect du principe de proportionnalité ;
- limitation du cercle des personnes autorisées à accéder aux données personnelles aux seuls magistrats et aux policiers ayant le rang d'officiers de police judiciaire.

La Commission nationale se propose ici de limiter ses observations aux seules dispositions du projet de loi n° 5986 ayant trait aux garanties nécessaires dans un but de préservation des libertés et droits fondamentaux et de limitation des risques d'atteinte à la vie privée des citoyens qui opèrent un changement substantiel par rapport à la loi du 22 juillet 2008.

Commentaires des articles du nouveau projet de loi

a) Limitation des fichiers ouverts à l'accès direct par voie informatique.

La Commission nationale n'a pas d'observation à formuler à l'égard de la liste limitative précise appelée à être insérée au paragraphe 1 de l'article 48-24 du Code d'Instruction criminelle et de l'article 34-1 de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la police (inchangée par rapport à la loi du 22 juillet 2008).

b) Limitation des catégories de données ouvertes à la consultation.

Il en est de même des dispositions du projet de loi qui précisent que les données à caractère personnel des fichiers rendus accessibles à la police et à la justice qui pourront être consultés en vertu des nouveaux articles seront déterminés par règlement grand-ducal, ceux-ci excluant d'ailleurs expressément toutes les données relatives à la santé.

c) Exigence d'un motif déterminé justifiant la consultation des fichiers rendus accessibles et journalisation des accès.

Cette exigence est importante aussi bien pour prévenir des abus dans l'application pratique et opérationnelle que pour la prise de conscience des fonctionnaires que la faculté de consultation qui leur est ouverte représente une exception à la protection dont bénéficient les citoyens à l'égard des renseignements les concernant qui figurent dans les fichiers des administrations publiques. Il nous paraît important que la loi indique clairement que le recours à la consultation des fichiers énumérés par les nouvelles dispositions doit toujours correspondre à une finalité précise et que les motifs qui la justifient apparaissent pour le moins par l'inscription d'une indication faisant référence au dossier.

Nous estimons dès lors que les dispositions décrivant les modalités techniques de l'accès direct aux fichiers opéré par un système informatique qui précisent 1) l'exigence « d'un motif précis » et 2) « l'indication de l'identifiant unique propre aux faits déterminés en cause » ne constituent pas un détail sans importance, mais revêtent une certaine portée dans la sensibilité aux risques d'abus dont feront preuve dans leur travail quotidien notamment les personnels de l'administration judiciaire non magistrats et les agents de la police grand-ducale n'ayant pas la qualité d'officier de la police judiciaire, auxquels le projet entend élargir la faculté d'accès.

Nous nous permettons dès lors de suggérer de reconsidérer leur suppression envisagée et de rétablir l'exigence d'indication obligatoire d'une référence au dossier dont le traitement motive l'accès, et cela au moment même de celui-ci. Nous avons en effet de la peine à adhérer à l'argumentation de l'exposé des motifs développée à la fin de la page 12 du document parlementaire n° 5986 qui consiste à voir dans l'exigence de l'indication d'un motif explicite de la consultation un double emploi avec celle de la personne y ayant procédé et à croire qu'il suffirait que le libellé de la lettre (b), du paragraphe (4), de l'article 48-24 CIC et de l'alinéa (4) de l'article 34-1 de la loi du 31 mai 1999 sur la Police mentionne l'objectif de retraçage du motif d'une consultation pour qu'il soit possible d'y parvenir effectivement.

Est-ce que l'effet préventif recherché pourra être atteint, si la loi se contente pour assurer l'efficacité d'éventuels contrôles par les supérieurs hiérarchiques ou par l'autorité instituée à l'article 17 visant à prévenir des abus, du recours à la seule mémoire des fonctionnaires ayant eu accès aux données personnelles quant au motif exact ayant justifié la consultation ? N'y a-t-il pas danger qu'un tel système ne soit pas fiable et soit trop facile à déjouer ?

Si nous concevons que la configuration du système informatique ne sera peut-être pas prête instantanément pour recueillir ces renseignements à partir de l'écran de saisie même qui ouvre l'accès aux fichiers tiers mentionnés dans le projet de loi, les renseignements dont nous disposons ne peuvent néanmoins nous convaincre qu'une telle fonctionnalité serait d'une complexité telle pour ne pas pouvoir être rajoutée par la suite à des coûts non excessifs et dans des délais raisonnables.

L'exigence de l'indication d'un motif déterminé ou du moins d'une référence de dossier au moment même de l'accès aux banques de données d'administrations tierces

(et non par la suite, par exemple lors d'un contrôle) et le traçage informatique constituent à notre époque des standards de bonnes pratiques dans cette matière qu'il appartient à notre Commission nationale d'appeler de ses vœux, notamment à l'occasion de l'adoption d'un texte légal de la portée de celui examiné.

Bien entendu, une phase transitoire d'une durée limitée, durant laquelle un mécanisme de substitution serait utilisé pour adresser l'enregistrement des références de données sous forme papier ou d'e-mail crypté, pourrait être nécessaire. Un formulaire que les agents devraient adresser à la direction générale de la police grand-ducale et, respectivement, que les fonctionnaires de l'administration judiciaire devraient soumettre au Procureur général ou au Procureur d'Etat pour justifier la consultation, pourrait être élaboré.

Laisser le soin à chaque fonctionnaire de noter ces renseignements dans un carnet tenu au niveau de sa propre unité ne satisferait pas à notre avis à l'objectif, de sorte que nous recommandons de prévoir un suivi et une conservation centralisée, même pendant la phase transitoire.

d) Limitation des données consultées aux informations pertinentes et nécessaires.

Le projet de loi maintient l'exigence d'un « lien direct des données consultées avec les faits ayant motivé la consultation » et réaffirme que « seules les données strictement nécessaires dans le respect du principe de proportionnalité peuvent être consultées. »

La CNPD se félicite de ce que ces principes fondamentaux de la protection de la vie privée et des données à caractère personnel se retrouvent ainsi consacrés expressément dans le texte du projet de loi qui met, par ailleurs, l'accent sur l'importance des investigations à mener dans le cadre de sa mission de surveillance par l'autorité de contrôle instituée à l'article 17, paragraphe 2 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. En l'absence d'un traçage des motifs, les dispositions en question (lien direct des données consultées avec les faits) risquent néanmoins de rester lettre morte étant donné qu'un contrôle efficace s'avérera impossible.

e) Limitation du cercle des personnes autorisées à avoir recours à la consultation des données figurant dans les fichiers publics mentionnés dans le projet de loi.

Le projet de loi sous revue se propose de faire bénéficier de l'accès aux fichiers publics énumérés non seulement les magistrats des parquets et les officiers de police judiciaire mais de l'étendre également au personnel de l'administration judiciaire et au personnel administratif et technique de la police, ces collaborateurs devant toutefois être nommément désignés par le Procureur général ou le Procureur d'Etat (pour ce qui concerne l'administration judiciaire) respectivement le Ministre ayant la Police dans ses attributions (pour ce qui concerne le cadre administratif et technique de la Police).

La Commission nationale note que le cercle des personnes qui bénéficieront du droit exorbitant (dixit la Commission consultative des Droits de l'Homme) d'accès à des fichiers publics tenus par d'autres autorités et administrations dans l'exercice de leurs missions légales correspondant à des intérêts publics distincts se verra donc considérablement élargi.

Une véritable culture du respect de la vie privée et de la protection des données à caractère personnel devra s'instaurer au niveau des autorités visées et être encouragée par des mesures de formation des fonctionnaires concernés et par un contrôle de la mise en œuvre opérationnelle de la part des responsables hiérarchiques.

Si un élargissement aussi conséquent du nombre de personnes qui se verront bénéficier de l'accès aux fichiers est nécessaire, il rend d'autant plus indispensable la mise en place d'outils permettant de retracer le respect des conditions légales, c'est-à-dire du principe de proportionnalité et du lien direct des données consultées avec les faits ayant motivé la consultation.

Il justifie également qu'on se repose la question de la nécessité d'ouvrir l'accès à l'ensemble des fichiers publics en question. Notre Commission nationale estime que les fonctionnaires visés par le projet de loi autres que les magistrats, les officiers de police judiciaire et le cadre supérieur de l'Inspection générale de la police devraient être exclus de, non seulement, l'accès au fichier des assujettis à la TVA (9), mais également au fichier relatif aux affiliations des salariés, des indépendants et des

employeurs géré par le Centre commun de la sécurité sociale (2), au fichier des demandeurs d'asile du service des réfugiés de l'Immigration (4) et au fichier des autorisations d'établissement exploité par le Ministère des Classes moyennes (6).

Les agents ne sont pas non plus qualifiés pour procéder à des perquisitions (base légale utilisée précédemment pour accéder aux données à caractère personnel) et n'auront guère besoin de consulter ces fichiers de nature plus sensible dans les affaires de petite envergure (ou de circulation) où on peut effectivement s'imaginer qu'ils officient souvent sans rapporter directement à leurs supérieurs qui remplissent les conditions pour disposer du droit d'accéder aux autres fichiers.

Nous proposons donc d'amender en ce sens les articles 1.3 (48.24 § 2 du C I C) et II.2 (article 34-1 et 77-1) de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la Police.

f) Abandon du seuil de gravité minimum de la peine correspondant aux faits ayant motivé la consultation.

Sous réserve de ses observations qui précèdent portant, d'une part, sur la nécessité de réintroduire dans le texte une disposition nécessitant l'enregistrement (à terme également dans le cadre du dispositif informatique gérant ces accès) du motif justifiant l'accès aux données consultées et, d'autre part, sur la nécessité d'ajouter les fichiers énumérés sub (2), (4) et (6) à ceux dont sera exclu l'accès des personnes autres que les magistrats, officiers de police judiciaires et membres du cadre supérieur de l'Inspection générale de la police, la Commission nationale estime que le projet de loi contient suffisamment de garanties et de mesures de sauvegarde en vue de prévenir des atteintes illégitimes ou excessives à la vie privée des personnes figurant dans les fichiers visés. Le critère du seuil de peine qui s'est avéré inapproprié et inapplicable en pratique peut donc être abandonné.

Motion de Madame Colette Flesch : données à caractère personnel

29 avril 2009

Projet de loi n° 5986 relatif à l'accès des autorités judiciaires, de la Police et de l'Inspection générale de la Police à certains traitements de données à caractère personnel mis en œuvre par 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

Motion

Dépôt : Mme Colette FLESCH
Date : 29.04.2009

La Chambre des Députés

- considérant la loi du 22 juillet 2008 relative à l'accès des magistrats et officiers de police judiciaire à certains traitements de données à caractère personnel mis en œuvre par des personnes morales et portant modification du Code d'instruction criminelle, de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la Police, et de la loi modifiée du 27 juillet 1997 portant réorganisation de l'administration pénitentiaire,
- considérant les difficultés d'application apparues, notamment dans le contexte des infractions à la législation relative à la circulation routière,
- constatant que ces difficultés résultent en particulier de la fixation d'un seuil de gravité correspondant à une peine correctionnelle de deux ans d'emprisonnement,
- considérant qu'il s'avère difficile de conférer une qualification précise à des faits au stade précoce d'une enquête et approuvant par conséquent que la référence à un seuil de peine soit abandonnée,
- constatant que le projet de loi sous rubrique prévoit l'extension de l'accès informatique direct aux fichiers de données à caractère personnel au personnel de l'administration judiciaire et au personnel administratif de la police,
- soucieuse de voir la confidentialité de ces informations garantie et d'éviter des abus,
- insistant sur le fait qu'un contrôle efficace de ces consultations doit être assuré, notamment au niveau du motif de la traçabilité et de l'identification des personnes ayant procédé à la consultation,
- se félicitant que la durée de conservation des données de retraçage soit désormais limitée à trois ans,
- regrettant qu'actuellement les programmes informatiques des fichiers concernés ne permettent pas la saisie de l'identifiant numérique des faits, ni du motif de la consultation,
- rappelant la nécessité de trouver un juste équilibre entre la lutte contre la criminalité et le respect des Droits de l'Homme,
- se référant à article 8 de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales

Invite le Gouvernement à

- veiller au maintien du juste équilibre entre sécurité et respect des libertés individuelles,
- instituer un contrôle efficace des consultations des fichiers à caractère personnel au niveau opérationnel et une formation du personnel de la police fondée sur la culture du respect des droits fondamentaux,
- mettre en place, dans un délai approprié, des solutions technologiques modernes destinées à éviter les risques d'abus et notamment un système informatique permettant de retracer le respect des conditions légales, c'est-à-dire du principe de proportionnalité et du lien direct des données consultées avec les faits ayant motivé la consultation,
- encourager le respect des bonnes pratiques au sein de la Police et sanctionner les abus éventuels.

Avis de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal relatif à la coopération interadministrative entre l'Administration de l'Enregistrement et des Domaines et l'Administration des Douanes et Accises

Délibération n° 187/2009 du 19 juin 2009

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'aviser « *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 à elle adressée par Monsieur le Premier Ministre, Ministre des Finances en date du 14 mai 2009 que la Commission nationale entend présenter ci-après ses commentaires au sujet du projet de règlement grand-ducal relatif à la coopération interadministrative entre l'Administration de l'Enregistrement et des Domaines et l'Administration des Douanes et Accises.

Celui-ci a pour objet d'organiser la coopération entre ces deux administrations relevant du Ministère des Finances sur la base de la loi du 19 décembre 2008 sur la coopération interadministrative et judiciaire et le renforcement des moyens de l'Administration des Contributions directes, de l'Administration de l'Enregistrement et des Domaines et de l'Administration des Douanes et Accises et portant modification de différentes lois les concernant.

Ladite loi précise à son article 1er que l'établissement correct et le recouvrement des droits à l'importation et à l'exportation, des droits d'accises, de la taxe sur les véhicules routiers et de la taxe sur la valeur ajoutée nécessitent l'échange réciproque d'informations entre ces deux administrations et que les données à caractère personnel sont susceptibles d'être communiquées entre elles notamment par des procédés automatisés sous la forme d'interconnexion de fichiers de consultation à travers un accès direct à des fichiers déterminés.

Le projet de règlement grand-ducal sous revue distingue, selon que les données sont échangées via l'accès direct de l'une des administrations visées sur certains fichiers de l'autre (chapitre I), que les informations nécessaires sont échangées sur demande adressée par l'une à l'autre (chapitre II) ou sont spontanément transmises par l'une à l'autre (chapitre III) ou résultent de contrôles effectués simultanément par l'une et l'autre de ces deux administrations ou en commun (chapitre IV).

Dans toutes ces hypothèses des données à caractère personnel collectées dans l'exercice des missions dont l'une de ces administrations est investie sont destinées à être transmises à l'autre en vue de faciliter l'établissement correct et le recouvrement de droits et taxes dont la perception relève de ses attributions.

Il résulte donc de l'examen du texte du projet de règlement grand-ducal et de la loi du 19 décembre 2008 susvisée, sur laquelle il se fonde, que les finalités déterminées de ces échanges d'informations sont expressément et clairement prévues et répondent aux critères de légitimation de l'article 5 de la loi modifiée du 2 août 2002 relative à la protection des personnes (transposant la directive 95/46/CE du 24 octobre 1995, en particulier son article 7).

Les articles 4, 5 et 6 de ladite loi du 19 décembre 2008 prévoient les différentes formes suivant lesquelles les deux administrations visées sont autorisées à échanger les données à caractère personnel en vue de l'exercice de leurs missions. L'échange de données sur demande et celui résultant de contrôles simultanés ou effectués en commun ne soulève donc pas de problème particulier alors qu'il va de soi qu'un tel échange devra rentrer dans les prévisions des dispositions spécifiques afférentes.

Notre Commission nationale entend dès lors limiter ses observations à la suggestion de compléter le « Chapitre Ier » du projet de règlement grand-ducal par un article ou un alinéa additionnel en vue de répondre

au vœu de l'article 4 de la loi du 19 décembre 2008 susmentionnée.

Les deux dernières phrases de cet article disposent en effet que les procédés automatisés se font moyennant interconnexion ou consultation de données à travers un accès direct à des fichiers de données à caractère personnel et sous garantie que l'accès soit sécurisé, limité et contrôlé. Les conditions, critères et modalités de l'échange sont déterminés par règlement grand-ducal.

Comme le texte du projet de règlement grand-ducal en revue précise déjà limitativement les fonctionnaires appelés à bénéficier des accès directs à instaurer et les motifs justifiant les consultations, il y a lieu de spécifier que l'accès aux données sera configuré de telle façon que les consultations soient retraçables en vue de la prévention d'éventuels abus et de l'efficacité des contrôles effectués le cas échéant.

Nous suggérons de reprendre le libellé suivant :

« Le système informatique par lequel l'accès direct est opéré doit être aménagé de sorte que les informations relatives à la personne ayant procédé à la consultation, les informations consultées, la date, l'heure et la référence du dossier dans le cadre duquel la consultation a été effectuée, ainsi que le motif précis de la consultation puissent être retracés. Les données à caractère personnel consultées doivent avoir un lien direct avec les faits ayant motivé la consultation. »

Il s'agit du texte de l'article 138, dernier alinéa de la loi du 29 août 2008 sur l'immigration qui correspond aux standards internationaux généralement acceptés comme bonne pratique en la matière.

Indication des voies de recours

La présente décision administrative peut faire l'objet d'un recours en annulation dans les 3 mois qui suivent sa notification à l'administré. Ce recours est à intenter par l'administré devant le tribunal administratif et doit obligatoirement être introduit par le biais du ministère d'avocat à la Cour inscrit auprès de l'un des deux tableaux de l'ordre des avocats.

Avis de la Commission nationale pour la protection des données concernant le projet de loi n° 6072 portant approbation d'un certain nombre de conventions bilatérales de non-double imposition et prévoyant la procédure applicable à l'échange de renseignements sur demande en matière fiscale

Délibération n° 410/2009 du 20 novembre 2009

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'aviser « *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* ».

Par courrier du 30 septembre 2009 Monsieur le Ministre des Finances avait invité la Commission nationale à se prononcer au sujet du projet de loi n° 6072 portant ratification d'un certain nombre de conventions signées par le Grand-Duché de Luxembourg avec d'autres Etats tendant à éviter les doubles impositions et à prévenir la fraude fiscale en matière d'impôts sur le revenu et sur la fortune.

L'article 1er du projet de loi vise l'approbation desdites conventions.

Les articles 2 à 4 du projet de loi sous examen prévoient la collecte et le traitement de données à caractère personnel par l'Administration des Contributions directes, l'Administration de l'Enregistrement et des Domaines et l'Administration des Douanes et Accises dans le cadre de la procédure applicable à l'échange de renseignements sur demande entre les Etats signataires des conventions bilatérales.

Dans l'exposé des motifs, le projet fait référence à la décision du 13 mars 2009 du gouvernement de se rallier intégralement au standard de l'OCDE en matière d'échange de renseignements sur demande entre administrations fiscales et aux efforts entrepris depuis lors pour concrétiser cet engagement.

Les conventions internationales soumises à la ratification du parlement sont entièrement conformes au modèle standard de l'OCDE dont l'article 26, paragraphe 5 (version de 2005) s'y trouve d'ailleurs intégré.

La Commission nationale note que la norme OCDE en question, reprise dans les conventions, s'applique à l'assistance administrative par l'échange de renseignements sur demande qui présuppose la « pertinence vraisemblable » des données à communiquer à l'Etat requérant et exclut aussi la possibilité « d'aller à la pêche aux renseignements » ou des demandes de renseignements dont il est peu probable qu'ils soient pertinents pour élucider les affaires fiscales d'un contribuable. Le texte n'envisage pas la possibilité d'un échange généralisé automatisé de données entre les Etats signataires. Les précisions apportées dans ce contexte, au point VII du commentaire des articles, sont de nature à garantir que le recours à la procédure prévue sera limité aux hypothèses qui sont compatibles avec les principes relatifs à la qualité des données à caractère personnel (finalité déterminée et légitime, pertinence, nécessité et proportionnalité), qui sont appelées à faire l'objet d'un traitement (collecte, transmission, enregistrement et usage) tels qu'ils figurent à l'article 6 de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 et ont été reproduits à l'article 4 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Les explications relatives à la signification des lignes directrices de son organisation formulées par le Secrétaire général de l'OCDE dans son courrier adressé le 13 mars 2009 à Monsieur le Ministre des Finances qui est reproduit à la page 27 du document parlementaire 6072/00, donnent des assurances solides sur la question que l'échange de renseignements sur demande consacré par accord bilatéral entre deux Etats n'est pas incompatible avec le secret bancaire en tant qu'instrument de la protection de la vie privée des citoyens et avec les libertés et droits fondamentaux gouvernant la protection des données personnelles.

Il appartient d'ailleurs à l'Etat requérant d'établir à l'appui de sa demande que les renseignements ne peuvent être obtenus par d'autres voies et moyens que l'entraide bilatérale via l'échange de renseignements entre administrations fiscales (principe de nécessité).

Outre la question de la conformité aux principes de base du cadre légal européen de la protection des données, la Commission nationale a examiné également les dispositions relatives à la procédure applicable au niveau de la collecte des données (articles 2-6) auprès des « détenteurs » des renseignements en question.

Le texte prévoit que ces derniers sont obligés de les fournir endéans un délai d'un mois à la demande des administrations compétentes (précisées à l'article 3) non sans que ces dernières aient dûment apprécié auparavant que la demande d'échange satisfait bien aux conditions légales, décision contre laquelle un recours en annulation devant les juridictions administratives est institué aux termes de l'article 6 du projet de loi.

Des moyens tirés d'une éventuelle violation des critères fondamentaux de la protection des données, notamment relatifs à la pertinence et à la nécessité et proportionnalité pourraient donc le cas échéant être opposés par les détenteurs des renseignements dans le cadre d'éventuels litiges concernant des demandes des administrations fiscales basées sur le texte sous revue.

Notons finalement que les personnes concernées ne doivent pas être informées de l'échange d'informations entre administrations fiscales dont elles font l'objet alors que l'article 13 de la directive (articles 27 et 29 de la loi du 2 août 2002) prévoit une exception applicable au principe de transparence en matière fiscale et des contrôles effectués dans le cadre de l'exercice de l'autorité publique.

Le droit d'accès aux données se trouve dans ce domaine également limité et différé.

Le cas échéant il appartiendra aux détenteurs des renseignements de prévenir les personnes concernées que des informations ont dû être communiquées dans le cadre de la procédure d'échange de renseignements sur demande en matière fiscale qui font l'objet des dispositions du projet de loi.

Ces dernières n'appellent pas d'observations ou de propositions de modification de la part de notre Commission nationale.

Délibération n°…/2009 du … 2009 de la Commission nationale pour la protection des données relative à la demande d'autorisation préalable en matière de surveillance du courrier électronique, de l'utilisation de l'internet et du réseau informatique de la société … S.A.

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 des 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 ; et

iii. la sécurité et/ou le bon fonctionnement des systèmes informatiques de la requérante, y compris le contrôle des coûts y afférents, ainsi que de 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 de l'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 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 du 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 privé] 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 au lieu de travail »[1] 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 personnels) 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 de l'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 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

2 http://www.edoeb.admin.ch/dokumentation/00445/00472/00532/index.html?lang=fr d. page 77

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 au lieu de travail* »[2] 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.*»

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.

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

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 de l'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 requis 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 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 conservées 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, de l'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)[3] :

« 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)[4].

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 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. »

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

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

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.

Ainsi décidé à Luxembourg en date du … 2009.

La Commission nationale pour la protection des données

Gérard Lommel	Président
Pierre Weimerskirch	Membre effectif
Thierry Lallemang	Membre effectif

Indication des voies de recours

La présente décision administrative peut faire l'objet d'un recours en annulation dans les 3 mois qui suivent sa notification à l'administré. Ce recours est à intenter par l'administré devant le tribunal administratif et doit obligatoirement être introduit par le biais du ministère d'avocat à la Cour inscrit auprès de l'un des deux tableaux de l'ordre des avocats.

Participations aux travaux européens

Documents adoptés par le groupe de travail en 2009

Document	Date d'adoption	Référence
L'avenir de la protection de la vie privée Contribution conjointe à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel	01.12.2009	WP 168
Avis 8/2009 sur la protection des données relatives aux passagers, collectées et traitées par les comptoirs de vente hors taxes des aéroports et des ports	01.12.2009	WP 167
Avis 7/2009 sur le niveau de protection des données à caractère personnel assuré dans la Principauté d'Andorre	01.12.2009	WP 166
Avis 6/2009 sur le niveau de protection des données à caractère personnel assuré en Israël	01.12.2009	WP 165
Contribution du groupe de travail Article 29 à la consultation publique de la DG MARKT concernant le rapport du groupe d'experts sur les historiques de crédit	01.12.2009	WP 164
Avis 5/2009 sur les réseaux sociaux en ligne	12.06.2009	WP 163
Deuxième avis 4/2009 sur le standard international pour la protection des renseignements personnels de l'Agence mondiale antidopage (AMA), sur les dispositions du code de l'AMA s'y rapportant et sur d'autres questions relatives à la vie privée dans le cadre de la lutte contre le dopage dans le sport par l'AMA et les organisations (nationales) antidopage	06.04.2009	WP 162
Avis 3/2009 concernant le projet de décision de la Commission relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants de données établis dans des pays tiers en vertu de la directive 95/46/CE (responsable du traitement de données vers sous-traitant de données)	05.03.2009	WP 161
Avis 2/2009 sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier des écoles)	11.02.2009	WP 160
Avis 1/2009 concernant les propositions modifiant la directive 2002/58/CE sur la protection de la vie privée dans le secteur des communications électroniques (directive « vie privée et communications électroniques »)	10.02.2009	WP 159
Document de travail 1/2009 sur la procédure d'échange d'informations avant le procès (« pre-trial discovery ») dans le cadre de procédures civiles transfrontalières	11.02.2009	WP 158

Working Party 29 – « Avis 5/2009 sur les réseaux sociaux en ligne »

Adopté le 12 juin 2009

Table des matières

Synthèse

Le présent avis se concentre sur la façon dont le fonctionnement des sites de réseautage social peut répondre aux exigences de la législation de l'UE en matière de protection des données. Il a principalement pour objectif de donner des indications aux fournisseurs de SRS quant aux mesures à mettre en place afin de garantir le respect du droit communautaire.

Cet avis souligne que les fournisseurs de SRS et, dans de nombreux cas, les fournisseurs tiers, sont responsables du traitement des données, avec les responsabilités que cela implique envers les utilisateurs de SRS. L'avis observe que bon nombre d'utilisateurs évoluent dans une sphère purement personnelle et qu'ils contactent des personnes pour gérer leurs affaires personnelles, familiales ou domestiques. L'avis estime que « l'exemption domestique » s'applique dans ces cas, qui ne sont donc pas régis par les réglementations relatives aux responsables de traitement des données. L'avis précise également dans quelles circonstances les activités d'un utilisateur de SRS ne sont pas couvertes par « l'exemption domestique ». La diffusion et l'utilisation d'informations disponibles sur les SRS à des fins secondaires, non recherchées, sont une préoccupation majeure du groupe de travail « article 29 ». L'avis recommande une sécurité robuste et des paramètres par défaut permettant de respecter la vie privée comme point de départ idéal pour tous les services offerts. La principale source de préoccupation semble être l'accès aux informations relatives au profil. L'avis aborde également des thèmes tels que le traitement de données ou d'images sensibles, la publicité ou le marketing direct sur les SRS ainsi que les problèmes de conservation des données.

Les recommandations essentielles portent sur les obligations des fournisseurs de SRS de se conformer à la directive relative à la protection des données et sur le maintien et le renforcement des droits des utilisateurs. L'engagement primordial des fournisseurs de SRS devrait être de donner aux utilisateurs dès leur inscription des informations sur leur identité et avancer toutes les raisons pour lesquelles les données à caractère personnel sont traitées. Une attention particulière devrait également être accordée au traitement des données à caractère personnel des mineurs. Selon l'avis, les utilisateurs ne devraient pas mettre en ligne des photos ou des informations concernant d'autres personnes sans le consentement de celles-ci. De plus, l'avis considère que les SRS sont également tenus de conseiller leurs utilisateurs en ce qui concerne les droits au respect de la vie privée d'autrui.

LE GROUPE DE PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995[35],

vu les articles 29 et 30, paragraphes 1, point a) et 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 ainsi que le règlement (CE) n° 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès public aux documents du Parlement européen, du Conseil et de la Commission,

vu son règlement intérieur,

A ADOPTÉ LE PRÉSENT AVIS:

1. Introduction

L'évolution des communautés virtuelles et des services hébergés tels que les services de réseautage social (« SRS ») est un phénomène relativement récent et le nombre d'utilisateurs de ces sites progresse de manière exponentielle.

Les informations personnelles publiées en ligne par un utilisateur, auxquelles s'ajoutent les données décrivant les actions et interactions de celui-ci avec d'autres personnes, peuvent donner un profil précis de ses centres d'intérêts et de ses activités. Les données à caractère personnel publiées sur les sites de réseautage social peuvent être utilisées par des tiers à des fins diverses, notamment commerciales, et peuvent présenter de grands risques tels que l'usurpation d'identité, les pertes financières, la perte d'activité économique ou de possibilités d'emploi ou l'atteinte à l'intégrité physique.

En mars 2008, le groupe de travail international sur la protection des données dans les télécommunications (Berlin) a adopté le *Memorandum de Rome*[36] . Ce mémorandum analyse les risques d'atteinte à la vie privée et à la sécurité posés par les réseaux sociaux et fournit des lignes directrices aux régulateurs, fournisseurs et utilisateurs. La résolution récemment adoptée sur la protection de la vie privée dans les services de réseaux sociaux[37] se penche aussi sur les problèmes posés par les SRS. Le groupe de travail tient également compte du document d'orientation publié en octobre 2007 par l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) intitulé « Problèmes de sécurité et recommandations pour les réseaux sociaux en ligne »[38] destiné aux régulateurs et aux fournisseurs de réseaux sociaux.

2. Définition d'un « service de réseautage social (SRS) » et modèle commercial

Les SRS peuvent être définis comme des plates-formes de communication en ligne permettant à des personnes de créer des réseaux d'utilisateurs partageant des intérêts communs. Au sens juridique, les réseaux sociaux sont des services de la société de l'information, tels que définis à l'article 1er, paragraphe 2, de la directive 98/34/CE, modifiée par la directive 98/48/CE. Les SRS partagent certaines caractéristiques:

- les utilisateurs sont invités à fournir des données à caractère personnel permettant de donner une description ou un « profil ».
- les SRS mettent également à disposition des outils permettant aux utilisateurs de mettre leur propre contenu en ligne (contenu généré par l'utilisateur tel que des photos, des chroniques ou des commentaires, de la musique, des vidéos ou des liens vers d'autres sites[39]);
- les « réseaux sociaux » fonctionnent grâce à l'utilisation d'outils mettant à disposition une liste de contacts pour chaque utilisateur avec une possibilité d'interaction.

35 JO L 281 du 23 novembre 1995, p. 31; http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

36 http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf

37 Adoptée lors de la 30ème Conférence internationale des commissaires à la protection des données et à la vie privée, à Strasbourg, le 17 octobre 2008, disponible à l'adresse suivante: http://www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_social_networks_fr.pdf

38 http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

39 Lorsque les SRS fournissent des services de communications électroniques, les dispositions de la directive 2002/58 « vie privée et communications électroniques » s'appliquent.

Les SRS génèrent la plupart de leurs revenus avec la publicité diffusée sur les pages web que les utilisateurs créent et auxquelles ils accèdent. Les utilisateurs qui publient sur leurs profils beaucoup d'informations concernant leurs centres d'intérêts offrent un marché précis aux publicitaires souhaitant diffuser des publicités ciblées sur la base de ces informations.

Il est donc important que les SRS opèrent en respectant les droits et les libertés des utilisateurs, qui s'attendent légitimement à ce que les données à caractère personnel qu'ils divulguent soient traitées conformément à la législation européenne et nationale concernant la protection des données et de la vie privée.

3. Application de la directive relative à la protection des données

Les dispositions de la directive relative à la protection des données s'appliquent dans la plupart des cas aux fournisseurs de SRS, même lorsque leur siège est situé en dehors de l'EEE. Le groupe de travail « article 29 » renvoie à son avis précédant sur les moteurs de recherche pour des informations complémentaires concernant l'établissement et l'utilisation du matériel aux fins de l'application de la directive relative à la protection des données ainsi que pour les règles découlant du traitement des adresses IP et de l'utilisation des « cookies » ou témoins[40].

3.1 Qui est responsable du traitement des données?

Fournisseurs de SRS

Les fournisseurs de SRS sont responsables du traitement des données conformément à la directive sur la protection des données. Ils fournissent les moyens permettant de traiter les données des utilisateurs ainsi que tous les services « basiques » liés à la gestion des utilisateurs (par exemple l'enregistrement et la suppression des comptes). Les fournisseurs de SRS déterminent également la manière dont les données des utilisateurs peuvent être utilisées à des fins publicitaires ou commerciales – y compris la publicité fournie par des tiers.

Fournisseurs d'application

Les fournisseurs d'application peuvent aussi être responsables du traitement des données s'ils développent des applications qui s'exécutent en complément de celles des SRS et si les utilisateurs décident de s'en servir.

Utilisateurs

Dans la plupart des cas, les utilisateurs sont considérés comme étant les personnes auxquelles les données en cause se rapportent. La directive n'impose pas les obligations d'un responsable du traitement des données à une personne qui traite des données à caractère personnel « pour l'exercice d'activités exclusivement personnelles ou domestiques » - ce qu'on appelle l'« exemption domestique ». Dans certains cas, l'exemption domestique peut ne pas couvrir les activités d'un utilisateur de SRS et on peut alors considérer que l'utilisateur a endossé certaines responsabilités d'un responsable de données. Quelques exemples sont développés ci-dessous:

3.1.1. Objet et nature

La tendance croissante des SRS est le passage du « Web 2.0 pour les loisirs » au « Web 2.0 pour la productivité et les services »[41] lorsque les activités de certains utilisateurs de SRS peuvent dépasser une activité purement personnelle ou domestique, quand, par exemple, le SRS est utilisé comme une plate-forme de collaboration pour une association ou une entreprise. L'exemption ne s'applique pas si un utilisateur de SRS agit au nom d'une entreprise ou d'une association ou qu'il utilise le SRS principalement comme une plate-forme à des fins commerciales, politiques ou sociales. L'utilisateur assume alors l'entière responsabilité d'un responsable du traitement des données qui révèle des données personnelles à un autre responsable du traitement des données (SRS) et à des tiers (autres utilisateurs de SRS ou même, potentiellement, autres responsables du traitement des données ayant accès aux données). Dans de telles circonstances, l'utilisateur a besoin du consentement des personnes concernées ou d'une autre base légitime figurant dans la directive relative à la protection des données.

40 WP148, « Avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche ».

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

Le plus souvent, l'accès aux données d'un utilisateur (données du profil, messages, chroniques…) est limité aux contacts qu'il a choisis. Parfois cependant, les utilisateurs peuvent acquérir un grand nombre de contacts tiers dont certains leur sont inconnus. Un nombre élevé de contacts peut indiquer que l'exception domestique ne s'applique pas et l'utilisateur sera alors considéré comme un responsable du traitement des données.

3.1.2. Accès aux informations du profil

Les SRS devraient garantir la mise en place de paramètres par défaut respectueux de la vie privée et gratuits afin de limiter l'accès aux contacts choisis par l'utilisateur.

Lorsque l'accès aux informations du profil va au-delà des contacts choisis, notamment quand tous les membres appartenant au SRS peuvent accéder à un profil[42] ou que les données sont indexables par les moteurs de recherche, l'accès dépasse la sphère personnelle ou domestique. De même, si un utilisateur décide, en parfaite connaissance de cause, d'élargir l'accès au-delà des « amis » choisis, il endosse les responsabilités d'un responsable du traitement des données. Dans la pratique, on applique alors le même régime légal que lorsqu'une personne utilise d'autres plates-formes technologiques pour publier des données personnelles sur Internet[43]. Dans plusieurs États membres, le manque de restrictions d'accès (et donc le caractère public des données) a pour conséquence que l'application de la directive relative à la protection des données[44] signifie que l'utilisateur endosse les responsabilités d'un responsable du traitement des données.

Il faut garder à l'esprit que, même si l'exemption domestique ne s'applique pas, l'utilisateur de SRS peut bénéficier d'autres exemptions comme, par exemple, pour les activités aux seules fins de journalisme ou d'expression artistique ou littéraire. Il convient alors de concilier la liberté d'expression et le droit à la vie privée.

3.1.3 Traitement des données tierces par les utilisateurs

L'application de l'exemption domestique est également limitée par le besoin de garantir les droits des tiers, particulièrement en ce qui concerne les données sensibles. Il convient en outre de noter que, même si l'exemption domestique s'applique, la responsabilité d'un utilisateur peut être engagée en application des dispositions générales du droit civil ou pénal national (notamment diffamation, responsabilité délictuelle pour violation du droit à la personnalité, responsabilité pénale).

3.2 Sécurité et paramètres de confidentialité par défaut

Le traitement sûr des informations constitue un élément clé de confiance dans les SRS. Les responsables du traitement doivent mettre en œuvre les mesures techniques et d'organisation appropriées « tant au moment de la conception du système de traitement qu'au moment même du traitement » pour assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger[45].

Un élément important des paramètres de confidentialité est l'accès aux données personnelles publiées sur un profil. Si cet accès n'est pas limité, un tiers peut accéder à des détails intimes concernant les utilisateurs, que ce soit en tant que membre du SRS ou via des moteurs de recherche. Cependant, seule une minorité des utilisateurs modifie les paramètres par défaut en s'inscrivant à ce genre de service. Les SRS devraient donc mettre en place des paramètres par défaut respectueux de la vie privée, qui permettent aux utilisateurs d'accepter librement et spécifiquement que des personnes autres que leurs contacts choisis accèdent à leur profil, afin de réduire le risque d'un traitement non autorisé. Les profils à accès limité ne devraient pas être repérables par les moteurs

42 Ou lorsqu'il peut être prouvé que l'acceptation des contacts ne fait pas l'objet d'une sélection, c'est-à-dire si les utilisateurs acceptent des « contacts » sans se soucier des liens existants.

43 Par exemple, avec des plates-formes de publication qui ne sont pas des SRS ou avec un logiciel auto-hébergé.

44 Par contre, la Cour de justice européenne avait jugé dans son arrêt Satamedia, point 44, que: « Il suit que cette dernière dérogation doit être interprétée comme se rapportant seulement aux activités effectuées au cours de la vie privée ou familiale des personnes (voir Lindqvist, point 47). Ceci ne s'applique manifestement pas aux activités de Markkinapörssi et Satamedia, dont le but est de rendre les données recueillies accessibles à un nombre illimité de personnes ».

45 Article 17 et considérant 46 de la directive relative à la protection des données.

de recherche internes, y compris par la fonction de recherche par paramètres tels que l'âge ou le lieu. Les décisions d'extension de l'accès ne doivent pas être implicites[46], par exemple avec un « opt out » fourni par le responsable du SRS.

3.3 Informations fournies par les SRS

Les fournisseurs de SRS devraient informer les utilisateurs de leur identité et des différentes raisons pour lesquelles ils traitent les données personnelles, conformément aux dispositions de l'article 10 de la directive relative à la protection des données, notamment:

- l'utilisation des données à des fins de marketing direct;
- le partage éventuel des données avec des catégories spécifiques de tiers;
- un aperçu des profils: leur création et leurs principales sources de données;
- l'utilisation des données sensibles.

Le groupe de travail recommande que:

- les fournisseurs de SRS mettent en garde de façon adéquate les utilisateurs contre les risques d'atteinte à leur vie privée et à celle des autres lorsqu'ils mettent des informations en ligne sur les SRS;
- les SRS rappellent à leurs utilisateurs que mettre en ligne des informations concernant d'autres personnes peut porter atteinte à leur droit à la vie privée et à la protection des données;
- les SRS conseillent à leurs utilisateurs de ne pas mettre en ligne des photos ou des informations concernant d'autres personnes sans le consentement de celles-ci[47].

3.4 Données sensibles

Les données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que celles concernant la santé ou la vie sexuelle sont considérées comme sensibles. Les données sensibles personnelles ne peuvent être publiées sur Internet qu'avec le consentement explicite de la personne concernée ou si elle a elle-même rendu ces données publiques[48].

Dans certains États membres de l'UE, les images de personnes concernées sont considérées comme une catégorie spéciale de données personnelles puisqu'elles peuvent être utilisées pour distinguer l'origine raciale/ethnique ou pour en déduire des croyances religieuses ou des données relatives à la santé. Le groupe de travail ne considère pas, en général, les images sur Internet comme des données sensibles[49], sauf si elles sont clairement utilisées pour révéler des données sensibles sur des personnes.

En tant que responsables du traitement des données, les SRS ne peuvent pas traiter des données sensibles concernant les membres ou les non-membres du réseau sans leur consentement explicite[50]. Si un SRS fait figurer sur les formulaires d'inscription des questions portant sur des données sensibles, le SRS doit indiquer très clairement qu'il est facultatif d'y répondre.

3.5 Traiter les données des non-membres

De nombreux SRS permettent aux utilisateurs de fournir des données sur d'autres personnes, notamment d'ajouter un nom à une image, d'évaluer quelqu'un ou d'énumérer les « gens que j'ai rencontrés/je veux rencontrer » à un événement. Ce marquage peut également identifier des non-membres. Cependant, le

46 Le Mémorandum de Rome signale des risques tels que l'idée erronée d'une communauté (p. 2), la fourniture de plus d'informations qu'on ne le pense (p.3). Une société de sécurité informatique avertit un SRS de l'accès par défaut aux membres d'un même lieu géographique : http://www.sophos.com/pressoffice/news/articles/2007/10/facebook-network.html

47 Ceci pourrait être facilité par des outils de gestion de marquage sur les sites Internet de réseaux sociaux, notamment en créant des espaces, sur un profil personnel, pour indiquer la présence d'un nom d'utilisateur dans des images ou vidéos marquées attendant le consentement de l'utilisateur en question, ou mettre en place des délais d'expiration pour les marquages n'ayant pas reçu le consentement de la personne marquée.

48 Les États membres peuvent prévoir des exemptions à cette règle; voir article 8, paragraphe 2, point a), deuxième phrase, et article 8, paragraphe 4, de la directive relative à la protection des données.

49 La publication d'images sur Internet suscite cependant de plus en plus d'inquiétudes en termes de respect de la vie privée vu le développement des techniques de reconnaissance faciale.

50 Le consentement doit être libre, informé et spécifique.

traitement par le SRS de ce type de données concernant des non-membres ne peut se faire que si l'un des critères visés à l'article 7 de la directive relative à la protection des données est rempli.

De plus, la création de profils de non-membres préremplis grâce à l'agrégation de données fournies indépendamment par des utilisateurs de SRS, y compris les données relationnelles déduites des carnets d'adresses en ligne, n'a aucune base juridique[51].

Même si le SRS était en mesure de contacter le non-utilisateur et de l'informer de l'existence de données personnelles le concernant, toute sollicitation électronique violerait l'interdiction prévue à l'article 13, paragraphe 4, de la directive « vie privée et communications électroniques » d'envoyer des messages électroniques non sollicités à des fins de prospection directe.

3.6 Accès de tiers au réseau

3.6.1 Accès par l'intermédiaire des SRS

En complément du service de base du SRS, la plupart des SRS proposent aux utilisateurs des applications additionnelles fournies par des concepteurs tiers, qui traitent aussi des données personnelles.

Les SRS devraient avoir les moyens de garantir que les applications tierces sont conformes aux directives relatives à la protection des données et à la protection de la vie privée dans le secteur des communications électroniques. Cela suppose, notamment, qu'ils informent les utilisateurs clairement et spécifiquement du traitement de leurs données personnelles et qu'ils aient seulement accès aux données personnelles nécessaires. Les SRS devraient donc offrir aux concepteurs tiers un accès progressif afin de limiter le mode d'accès. De plus, les SRS devraient s'assurer que les utilisateurs peuvent facilement faire part de leurs inquiétudes au sujet des applications.

3.6.2 Accès de tiers par l'intermédiaire des utilisateurs

Les SRS permettent parfois aux utilisateurs d'accéder et de mettre à jour leurs données grâce à d'autres applications. Les utilisateurs peuvent par exemple:

- lire et poster des messages de leur portable sur le réseau;
- synchroniser les coordonnées de leurs amis sur le SRS avec leur carnet d'adresses sur un ordinateur de table;
- mettre à jour automatiquement leur statut ou le lieu sur le SRS en allant sur un autre site web.

Les SRS publient sous forme d'une « interface de programmation » (API) la façon dont ce logiciel peut être créé. Cela permet à tout tiers de créer des logiciels pour accomplir ces tâches et les utilisateurs peuvent choisir entre plusieurs prestataires tiers[52]. Lorsqu'ils proposent un API permettant l'accès aux données personnelles, les SRS devraient :

- mettre en place un niveau de détail qui laisse l'utilisateur choisir un niveau d'accès destiné aux tiers limité au seul accomplissement d'une tâche donnée.

Lorsqu'ils accèdent à des données personnelles via les API des tiers au nom d'un utilisateur, les prestataires de services tiers devraient :

- traiter et conserver les données pendant une durée n'excédant pas celle nécessaire à la réalisation d'une tâche spécifique,
- limiter les opérations sur les données des contacts importés par l'utilisateur à l'usage personnel de l'utilisateur qui les a fournies.

51 Le considérant 38 de la directive relative à la protection des données précise: « considérant que le traitement loyal des données suppose que les personnes concernées puissent connaître l'existence des traitements et bénéficier, lorsque des données sont collectées auprès d'elles, d'une information effective et complète au regard des circonstances de cette collecte." Pour certains SRS, la publication des profils de non-membres semble devenir une façon non négligeable de commercialiser leurs « services ».

52 « API » est un terme technique large, mais il est fait référence ici à l'accès au nom d'un utilisateur, c'est-à-dire que les utilisateurs doivent fournir leurs données de connexion au logiciel pour que celui-ci agisse en leur nom.

3.7 Bases juridiques de la prospection directe

La prospection commerciale directe constitue une partie essentielle du modèle commercial des SRS; des modèles de marketing différents peuvent être utilisés par les SRS. Toutefois, la prospection utilisant les données personnelles des utilisateurs devrait respecter les dispositions applicables de la directive relative à la protection des données et celle sur la vie privée et les communications électroniques[53].

Le *marketing contextuel* est adapté au contenu que l'utilisateur voit ou auquel il accède[54].

Le *marketing segmenté* consiste à diffuser des publicités à des groupes d'utilisateurs ciblés[55]; l'utilisateur est placé dans un groupe en fonction des informations qu'il a communiquées directement au SRS[56].

Enfin, le *marketing comportemental* sélectionne les publicités par l'observation et l'analyse des activités de l'utilisateur au cours du temps. Ces techniques peuvent être soumises à des exigences juridiques selon les bases légales applicables et les caractéristiques des techniques utilisées. Le groupe de travail préconise de ne pas utiliser de données sensibles dans les modèles publicitaires comportementaux si toutes les exigences légales ne sont pas satisfaites.

Quels que soient le modèle ou la combinaison de modèles, les publicités peuvent être diffusées soit directement par le SRS (le fournisseur de SRS exerce ici une activité de courtage), soit par un publicitaire tiers. Dans le premier cas, il n'est pas nécessaire de divulguer les données personnelles des utilisateurs aux tiers. Dans le second cas toutefois, il est possible que le publicitaire tiers manipule les données personnelles des utilisateurs, s'il traite l'adresse IP de l'utilisateur ou un cookie placé sur son ordinateur, par exemple.

3.8 Conservation des données

Les SRS n'entrent pas dans la définition des services de communications électroniques inscrite à l'article 2, sous c), de la directive-cadre (2002/21/CE). Les fournisseurs de SRS peuvent offrir des services additionnels couverts par la définition des services de communications électroniques, comme un service de messagerie électronique accessible publiquement. Les dispositions de la directive relative à la protection des données et de la directive sur la protection de la vie privée dans le secteur des communications électroniques s'y appliqueront.

Certains SRS permettent à leurs utilisateurs d'envoyer des invitations à des tiers. L'interdiction d'utiliser les courriers électroniques à des fins de prospection directe ne s'applique pas aux communications personnelles. Pour se conformer à l'exception des communications personnelles, un SRS doit respecter les critères suivants:

- ni l'expéditeur ni le destinataire ne sont incités à communiquer;
- le fournisseur ne sélectionne pas les destinataires[57];
- l'identité de l'expéditeur est mentionnée clairement;
- l'expéditeur doit connaître le contenu entier du message qui sera envoyé en son nom.

Certains SRS conservent également les données d'identification des utilisateurs suspendus du service pour s'assurer qu'ils ne pourront pas se reconnecter. Ces utilisateurs doivent alors être informés qu'un tel traitement est en cours. En outre, les seules informations dont la conservation est autorisée sont les informations d'identification et non les raisons pour lesquelles ces personnes ont été suspendues. Ces informations ne devraient pas être conservées plus d'un an.

53 Le groupe de travail envisage de traiter prochainement les différents aspects de la publicité en ligne dans un autre document.

54 Par exemple, si la page regardée mentionne le mot « Paris », la publicité diffusée peut présenter un restaurant dans cette ville.

55 Chaque groupe étant défini par une série de critères.

56 Notamment au moment de son inscription au réseau.

57 C'est-à-dire qu'il est interdit d'envoyer des invitations à l'ensemble du carnet d'adresses d'un contact. 24 L'article 6, paragraphe 1, sous e), de la directive sur la protection des données dispose que les données doivent être « 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 ont été collectées ou pour lesquelles elles sont traitées ultérieurement ».

Les données personnelles fournies par un utilisateur lors de son inscription au SRS devraient être effacées dès que l'utilisateur ou le fournisseur de SRS décide de supprimer le compte24. De même, les informations supprimées par l'utilisateur lors de la mise à jour de son compte ne devraient pas être conservées. Les SRS devraient avertir les utilisateurs avant de procéder à ces formalités avec les moyens dont ils disposent pour les informer de ces périodes de rétention. Dans certains cas spécifiques, à des fins légales et sécuritaires, il pourrait être justifié de conserver pour une durée déterminée des données qui ont été mises à jour ou effacées et des comptes afin d'empêcher les opérations malveillantes résultant de l'usurpation d'identité et d'autres délits.

Lorsqu'un utilisateur n'utilise plus le service pendant un certain laps de temps, le profil devrait devenir inactif, c'est-à-dire qu'il ne devrait plus être visible pour les autres utilisateurs ou pour le monde extérieur et quelque temps après, les données du compte abandonné devraient être effacées. Les SRS devraient avertir les utilisateurs par tous les moyens disponibles avant de procéder à ces formalités.

3.9 Droits des utilisateurs

Les SRS devraient respecter les droits des personnes concernées par le traitement des données, conformément aux dispositions inscrites aux articles 12 et 14 de la directive relative à la protection des données.

Les droits d'accès et de rectification des utilisateurs ne sont pas limités aux utilisateurs du service mais à toute personne physique dont les données sont traitées[58]. Les membres et les non-membres des SRS doivent avoir un moyen d'exercer leur droit d'accès, de rectification et d'effacement. La page d'accueil des sites de SRS devrait clairement faire référence à l'existence d'un « bureau des réclamations » mis en place par le fournisseur de SRS pour la gestion des problèmes concernant la protection des données et de la vie privée ainsi que des plaintes des membres et non-membres.

L'article 6, paragraphe 1, point c), de la directive relative à la protection des données dispose que les données à caractère personnel doivent être « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et/ou pour lesquelles elles sont traitées ultérieurement ». Dans ce contexte, on observe que le SRS peut avoir besoin d'enregistrer certaines données d'identification de ses membres, mais qu'il n'a pas besoin de diffuser leur vrai nom sur Internet. Les SRS devraient donc pouvoir justifier le fait de contraindre leurs utilisateurs à agir sous leur véritable identité plutôt que sous un pseudonyme. D'importants arguments indiquent que les SRS doivent laisser le choix aux utilisateurs à cet égard et, dans au moins un État membre, il s'agit d'une exigence légale. Ces arguments s'imposent particulièrement lorsque le SRS concerné a des membres dans le monde entier.

L'article 17 de la directive relative à la protection des données prévoit que le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel. Ces mesures peuvent comprendre le contrôle d'accès ainsi que des mécanismes d'authentification susceptibles d'être mis en œuvre même si des pseudonymes sont utilisés.

4. Enfants et mineurs

Une grande partie des services de SRS est utilisée par des enfants ou des mineurs. L'avis WP147[59] du groupe de travail s'est penché sur l'application de principes de protection des données dans l'environnement scolaire et éducatif. L'avis a souligné le besoin de tenir compte du meilleur intérêt de l'enfant au sens de la Convention internationale des droits de l'enfant. Le groupe de travail veut aussi insister sur l'importance de ce principe dans le contexte des SRS.

Les autorités chargées de la protection des données ont lancé diverses initiatives intéressantes[60] dans le monde entier, qui se concentrent principalement sur la sensibilisation en matière de SRS et des risques possibles. Pour relever ces défis, le groupe de travail encourage des recherches complémentaires pour résoudre les difficultés entourant la vérification de l'âge requis et la preuve du consentement préalable.

58 C'est notamment le cas lorsque l'adresse électronique de cette personne a été utilisée par le service de SRS pour lui envoyer une invitation.

59 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp147_fr.pdf

60 Par exemple, l'initiative portugaise « Dadus » http://dadus.cnpd.pt/ ou encore le « Chat Check Badge » danois http://www.fdim.dk/

À la lumière de ce qui précède, le groupe de travail estime qu'une stratégie pluridimensionnelle résoudrait le problème de la protection des données des enfants dans le contexte des SRS. Cette stratégie multiple s'appuierait sur:

- des initiatives de sensibilisation, qui s'avèrent fondamentales pour un engagement actif de la part des enfants (via les écoles, l'insertion dans le programme scolaire de notions de base en matière de protection des données, la création d'outils éducatifs appropriés et la collaboration d'organismes nationaux compétents);
- le traitement équitable et légal des mineurs, par exemple: ne pas demander de données sensibles dans le formulaire d'abonnement, pas de prospection directe visant des mineurs, l'accord préalable des parents avant l'inscription ainsi que des niveaux adaptés permettant de séparer les communautés d'enfants et d'adultes;
- la mise en place de technologies pour la protection de la vie privée (PET) – c'est-à-dire des paramètres par défaut respectueux de la vie privée, des fenêtres pop-up d'avertissement à des étapes adaptées ainsi que des logiciels de vérification de l'âge;
- l'autoréglementation des fournisseurs afin d'encourager l'adoption de codes de bonne pratique avec des mesures d'application efficaces comportant des sanctions disciplinaires;
- si nécessaire, des mesures législatives appropriées pour décourager les pratiques déloyales et/ou frauduleuses dans le contexte des SRS.

5. Synthèse des obligations/droits

Applicabilité des directives communautaires

1. La directive relative à la protection des données s'applique généralement au traitement des données personnelles par les SRS, même si leur siège se trouve en dehors de l'EEE.
2. Les fournisseurs de SRS sont considérés comme responsables du traitement des données conformément à la directive relative à la protection des données.
3. Les fournisseurs d'application peuvent éventuellement être considérés comme responsables du traitement des données conformément à la directive relative à la protection des données.
4. Les utilisateurs sont considérés comme des personnes concernées par rapport au traitement de leurs données par les SRS.
5. Dans la plupart des cas, le traitement des données personnelles par des utilisateurs relève de l'exemption domestique. Dans certains cas, les activités d'un utilisateur ne bénéficient pas de cette exemption.
6. Les SRS n'étant pas couverts par la définition des services de communications électroniques, la directive sur la conservation des données ne s'applique pas aux SRS.

Obligations des SRS

7. Les SRS devraient informer les utilisateurs de leur identité et leur fournir des informations claires et complètes sur les raisons pour lesquelles ils ont l'intention de traiter des données personnelles ainsi que les différentes manières de procéder.
8. Les SRS devraient mettre en place des paramètres par défaut respectueux de la vie privée.
9. Les SRS devraient informer et mettre en garde leurs utilisateurs contre les risques d'atteinte à la vie privée lorsqu'ils téléchargent des données sur les SRS.

11. Les SRS devraient recommander à leurs utilisateurs de ne pas mettre en ligne des images ou des informations concernant d'autres personnes sans le consentement de celles-ci.

12. La page d'accueil des SRS, au moins, devrait présenter un lien vers un « bureau des réclamations » destiné aux membres et aux non-membres et couvrant les problèmes de protection des données.

13. L'activité commerciale doit respecter les règles établies par la directive relative à la protection des données et celle sur la protection de la vie privée dans le secteur des communications électroniques.

14. Les SRS doivent prévoir un délai maximal de conservation des données des utilisateurs inactifs. Les comptes abandonnés doivent être supprimés.

15. En ce qui concerne les mineurs, les SRS devraient prendre des mesures adéquates afin de limiter les risques.

Droits des utilisateurs

16. Les membres ainsi que les non-membres des SRS bénéficient le cas échéant des droits des personnes concernées, conformément aux dispositions des articles 10 à 14 de la directive relative à la protection des données.

17. Les membres et les non-membres devraient avoir accès à une procédure de traitement des plaintes mise en place par les SRS et facile à utiliser.

18. En général, les utilisateurs devraient être autorisés à prendre un pseudonyme.

Fait à Bruxelles, le 12 juin 2009

Pour le groupe de travail
Le président
Alex TÜRK

Working Party 29 – « L'avenir de la protection de la vie privée - contribution conjointe à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel »

Adopté le 1er décembre 2009

Résumé

Le 9 juillet 2009, la Commission a lancé une consultation sur le cadre juridique du droit fondamental à la protection des données à caractère personnel. Dans le cadre de sa consultation, la Commission appelle à la communication d'avis sur les nouveaux défis de la protection des données à caractère personnel, notamment au regard des nouvelles technologies et de la mondialisation. Elle entend ainsi recueillir des éléments de réflexion pour déterminer si le cadre juridique actuel répond aux besoins et quelles mesures devraient être prises à l'avenir pour relever les défis identifiés. Le présent document expose la réponse conjointe à cette consultation du groupe de travail Article 29 (ci-après dénommé « groupe de travail 29 ») et du groupe de travail « Police et justice ».

Le message central de cette contribution est que les principes essentiels de la protection des données restent valables en dépit des nouvelles technologies et de la mondialisation.

Il est possible d'améliorer le niveau de protection des données dans l'UE grâce à une meilleure application des principes actuels de protection des données dans la pratique. Cela ne signifie pas pour autant qu'aucun changement législatif n'est nécessaire. Au contraire, il est utile de saisir cette occasion pour:

- préciser les modalités d'application de certaines règles et principes clés en matière de protection des données (tels que le consentement et la transparence);
- moderniser le cadre actuel, par l'ajout de nouveaux principes (tels que la « prise en compte du respect de la vie privée dès la conception » et la « responsabilité »);
- renforcer l'efficacité du système par la modernisation des dispositions de la directive 95/46/CE (par exemple en limitant la charge administrative);
- intégrer les principes fondamentaux de la protection des données dans un cadre juridique global, qui s'applique également à la coopération policière et judicaire en matière pénale.

Dans le chapitre 1, une introduction présente brièvement l'historique et le contexte de la protection des données dans l'UE.

Le chapitre 2 propose l'introduction d'un cadre juridique global. Il reconnaît la nécessité d'élaborer des règles spécifiques (*leges speciales*), à condition que celles-ci s'inscrivent dans un cadre global et soient conformes aux principes essentiels. Les garanties et principes essentiels de la protection des données devraient s'appliquer au traitement des données dans tous les secteurs.

Les chapitres 3 et 4 examinent les principaux défis en matière de protection des données.

Le chapitre 3 sur la mondialisation expose qu'en vertu du droit de l'Union, la protection des données est un droit fondamental. L'UE et ses États membres devraient garantir à tous ce droit fondamental, dans la mesure de leurs compétences. Chaque individu devrait pouvoir réclamer la protection de ses données, même lorsqu'elles font l'objet d'un traitement à l'extérieur de l'UE. C'est pourquoi il est demandé à la Commission de promouvoir la poursuite de l'élaboration de normes internationales globales en matière de protection des données à caractère personnel. En outre, il est nécessaire de repenser le processus d'évaluation du caractère adéquat de la protection. Par ailleurs, les accords internationaux peuvent constituer des instruments pertinents pour la protection des données à caractère personnel, à l'échelon mondial, et le futur cadre juridique pourrait prévoir les conditions des accords conclus avec des pays tiers. Le traitement des données en dehors de l'UE peut également être protégé par des règles d'entreprise contraignantes.

Il convient de renforcer davantage la disposition sur les règles d'entreprise contraignantes et de l'intégrer dans le nouveau cadre juridique. En ce qui concerne le droit applicable, le groupe de travail 29 envisage de rendre son avis à la Commission au cours de l'année prochaine.

Selon le chapitre 4 consacré aux évolutions technologiques, la directive 95/46/CE a bien résisté aux nombreux progrès technologiques grâce à ses principes et concepts solides et neutres sur le plan technologique. Ces derniers demeurent tout aussi pertinents, valables et applicables dans le monde connecté actuel. Les avancées technologiques ont accru les risques liés à la protection de la vie privée et des données des personnes physiques. Pour compenser ces risques, le principe de la « prise en compte du respect de la vie privée dès la conception » devrait être introduit dans le nouveau cadre: la protection de la vie privée et des données devrait être intégrée dès la conception des technologies de l'information et de la communication. L'application d'un tel principe soulignerait la nécessité de mettre en œuvre des technologies visant à améliorer la protection de la vie privée, un paramétrage par défaut favorable à la prise en compte du respect de la vie privée et les outils indispensables aux utilisateurs pour mieux protéger leurs données à caractère personnel. Par conséquent, ce principe de « prise en compte du respect de la vie privée dès la conception » devrait non seulement être contraignant pour les responsables du traitement des données mais également pour les concepteurs et producteurs de technologies. Qui plus est, il conviendrait d'adopter, le cas échéant, des règlements applicables dans des circonstances technologiques spécifiques, prévoyant la prise en compte des principes de protection des données et de respect de la vie privée.

Selon les chapitres 5, 6 et 7, les principaux défis en matière de protection des données nécessitent un renforcement du rôle des différents acteurs.

L'évolution du comportement et du rôle des personnes concernées, ainsi que l'expérience acquise grâce à la directive 95/46/CE imposent d'accorder aux personnes une place plus importante en ce qui concerne la protection des données. Le chapitre 5 expose les propositions visant à donner à la personne les moyens de jouer un rôle plus actif. Pour atteindre cet objectif, il est notamment nécessaire d'améliorer les voies de recours. Les personnes devraient disposer de moyens plus nombreux pour exercer et faire valoir leurs droits, notamment par l'introduction de procédures de recours collectif, de procédures de plainte et d'autres modes de règlement des conflits plus accessibles, plus efficaces et moins coûteux. En outre, le nouveau cadre devrait prévoir des solutions alternatives permettant une plus grande transparence et l'introduction d'une notification générale en cas de violation de la vie privée. Le « consentement » est un motif de traitement important qui pourrait, dans certaines circonstances, donner plus de pouvoir à la personne concernée. Néanmoins, à l'heure actuelle, on prétend souvent à tort qu'il est le motif applicable, étant donné que les conditions du consentement ne sont pas entièrement réunies. En conséquence, le nouveau cadre devrait préciser les conditions du « consentement ». De plus, il convient de favoriser l'harmonisation, car l'absence d'harmonisation des législations nationales transposant la directive 95/46/CE empêche de donner plus de pouvoir aux personnes concernées. Enfin, le rôle des personnes concernées sur l'internet est un sujet de préoccupation qui doit être encore précisé dans la perspective du nouveau cadre juridique. En tout état de cause, quiconque propose des services à une personne physique devrait être tenu de fournir certaines garanties en matière de sécurité et, le cas échéant, de confidentialité des informations téléchargées par les utilisateurs, que son client soit ou non un responsable du traitement des données.

Le chapitre 6 vise à renforcer la responsabilité des autorités chargées du traitement des données. La protection des données devrait en premier lieu être ancrée dans les organisations. Elle devrait faire partie intégrante de leurs valeurs et pratiques communes, et il convient d'en attribuer expressément la responsabilité. Cette démarche aidera également les autorités chargées de la protection des données dans leurs missions de surveillance et de lutte contre les infractions, rendant ainsi la protection de la vie privée plus efficace. Les responsables du traitement des données doivent prendre un certain nombre de mesures proactives et réactives, précisées dans ce chapitre. En outre, il serait judicieux d'introduire le principe de responsabilité dans le cadre global, afin de contraindre les responsables du traitement des données à prendre les mesures nécessaires pour veiller à ce que

les principes et obligations essentiels de la directive actuelle soient respectés lors du traitement des données à caractère personnel, mais également pour disposer des mécanismes internes nécessaires démontrant le respect de ces exigences par les parties prenantes extérieures, y compris les autorités chargées de la protection des données. Les notifications d'opérations de traitement des données aux autorités nationales de protection pourraient être simplifiées, voire réduites. Il conviendrait d'examiner si, et dans quelle mesure, la notification pourrait être limitée aux situations dans lesquelles le risque pour la protection de la vie privée est élevé, ce qui permettrait aux autorités chargées de la protection des données d'être plus sélectives et de concentrer leurs efforts sur ces cas, mais également de déterminer les modalités de simplification de cette notification.

Le chapitre 7, point a, envisage un rôle accru et plus précis pour les autorités nationales chargées de la protection des données. À l'heure actuelle, les États membres ont des avis très divergents en ce qui concerne, notamment, le rôle, les ressources et les pouvoirs des autorités chargées de la protection des données. Les nouveaux défis auxquels la protection des données est confrontée réclament desdites autorités un contrôle renforcé, plus homogène et efficace. En conséquence, le nouveau cadre devrait garantir l'uniformité des normes en ce qui concerne l'indépendance, les pouvoirs réels, le rôle consultatif de ces autorités dans le processus législatif et leur capacité à fixer leur propre programme de travail, notamment la définition des priorités en matière de traitement des plaintes. De telles normes devraient être adoptées à haut niveau par des instances qui font autorité.

Le chapitre 7, point b, décrit comment la coopération entre les autorités chargées de la protection des données devrait être améliorée. Les autorités européennes chargées de la protection des données sont réunies au sein du groupe de travail 29. La première priorité devrait être de veiller à ce que toutes les questions liées au traitement des données à caractère personnel, en particulier dans le domaine de la coopération policière et judiciaire en matière pénale, fassent partie intégrante des activités du groupe de travail 29 actuel. En outre, les méthodes de travail du groupe devraient encore être améliorées. Il conviendrait, le cas échéant, de souligner l'engagement renouvelé des membres du groupe de travail à mettre en œuvre les avis de ce dernier, à l'échelon national. Les relations entre le groupe de travail 29 et la Commission, qui en assure le secrétariat, peuvent encore être améliorées par la description du rôle essentiel de chacun dans un protocole d'accord. Le groupe de travail 29 lancera en 2010 une consultation avec la Commission sur ce protocole.

Enfin, le chapitre 8 aborde les défis de la protection des données dans le domaine particulièrement préoccupant de la police et de la lutte contre la criminalité. Cette question, dans le contexte de l'UE, a évolué depuis l'entrée en vigueur du traité de Lisbonne. La décision-cadre 2008/977/JAI relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale peut être perçue comme un premier pas vers la création d'un cadre général relevant de l'ex-troisième pilier, bien qu'elle reste largement incomplète. Ces dernières années, le nombre de données à caractère personnel conservées et échangées dans le cadre d'activités policières et judiciaires a considérablement augmenté, en raison des besoins croissants d'utilisation de ces informations pour combattre les nouvelles menaces du terrorisme et de la criminalité organisée, et sous l'effet des évolutions technologiques. Dans ce contexte, les défis de la protection des données sont immenses et devraient être traités dans le futur cadre juridique. Le chapitre 8 détaille les conditions d'élaboration des lois et des politiques en matière de protection des données dans le domaine de la police et de la lutte contre la criminalité, à savoir un échange d'informations basé sur une stratégie cohérente; une évaluation périodique des mesures et instruments juridiques actuels et de leur application; la transparence et la prise en compte de l'accès et des droits de rectification dans un contexte transfrontalier; la transparence et le contrôle démocratique du processus législatif; l'architecture des systèmes de stockage et d'échange des données à caractère personnel; un cadre clair pour les relations avec les États tiers, qui soit contraignant pour toutes les parties et fondé sur la notion d'évaluation du caractère adéquat de la protection; une attention particulière accordée aux systèmes d'information à grande échelle dans l'UE; une prise en compte adaptée du contrôle indépendant, du contrôle judiciaire et des voies de recours, ainsi qu'une coopération renforcée entre les autorités chargées de la protection des données.

1. Introduction

La consultation

1. Le 9 juillet 2009, la Commission a lancé une consultation sur le cadre juridique du droit fondamental à la protection des données à caractère personnel. Dans le cadre de sa consultation, la Commission appelle à la communication d'avis sur les nouveaux défis de la protection des données à caractère personnel, notamment au regard des nouvelles technologies et de la mondialisation. Elle entend ainsi recueillir des éléments de réflexion pour déterminer si le cadre juridique actuel répond aux besoins et quelles mesures devraient être prises à l'avenir pour relever les défis identifiés.

2. Le présent document expose la réponse conjointe à cette consultation du groupe de travail Article 29 (ci-après dénommé « groupe de travail 29 ») et du groupe de travail « Police et justice ».

Historique et contexte

3. La convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108)[61] peut être considérée comme le premier cadre juridique européen du droit fondamental à la protection des données à caractère personnel. Le droit à la protection des données est étroitement lié, mais n'est pas identique, au droit à la vie privée visé à l'article 8 de la Convention européenne des droits de l'homme. Il est reconnu comme un droit fondamental autonome par l'article 8 de la Charte des droits fondamentaux de l'Union européenne.

4. Les principes de la Convention 108 ont été précisés dans la directive 95/46/CE2[62] qui est la pierre angulaire de la législation sur la protection des données dans l'UE. L'efficacité (future) de la directive est le principal objet de la consultation de la Commission. Les autres instruments législatifs de l'UE en matière de protection des données sont le règlement n° (CE) 45/2001[63] applicable au traitement des données par les institutions et les organismes de l'UE, la directive 2002/58/CE[64] sur la vie privée et les communications électroniques, et la décision-cadre 2008/977/JAI[65] relative à la protection des données dans le domaine de la coopération policière et judiciaire en matière pénale.

5. Le traité de Lisbonne accorde à la protection des données une importance considérable. Non seulement la Charte des droits fondamentaux de l'Union européenne est devenue contraignante, mais l'article 16 du traité sur le fonctionnement de l'Union européenne (TFUE), qui a été ajouté, constitue une nouvelle base juridique pour la protection des données applicable à tous les traitements de données à caractère personnel, dans les secteurs public et privé, y compris dans le domaine de la coopération policière et judiciaire et dans le cadre de la politique étrangère et de sécurité commune. L'article 16 renforce la protection des données.

6. Dans ce contexte, il convient de mentionner également le « Programme de Stockholm », programme pluriannuel de l'Union européenne qui accorde une grande importance à la protection des données dans un espace de liberté, de sécurité et de justice au service de la protection du citoyen.[66]

61 STE n° 108, 28.1.1981.

62 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, JO L 281 du 23.11.1995, p. 31.

63 Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par lesinstitutions et organes communautaires et à la libre circulation de ces données, JO L 8 du 12.1.2001, p. 1.

64 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitementdes données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), JO L 201 du 31.7.2002, p. 37; telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009.

65 Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, JO L 350 du 30.12.2008, p. 60, à transposer dans la législation nationale avant le 27 novembre 2010.

66 Le Programme de Stockholm: un espace européen ouvert et sûr, au service du citoyen et de sa protection, devant être approuvé par le Conseil européen en décembre 2009.

Message central

7. La consultation de la Commission arrive à un moment fort opportun en raison des importants nouveaux défis posés par les nouvelles technologies et la mondialisation, mais également dans la perspective du traité de Lisbonne.

8. Le message central est que les principes fondamentaux de la protection des données restent valables malgré ces défis importants. Le niveau de protection des données dans l'UE peut être amélioré grâce à une meilleure application des principes actuels de protection des données. Cela ne signifie pas pour autant qu'aucun changement législatif n'est nécessaire. Au contraire, il est utile de saisir cette occasion pour:

- préciser les modalités d'application de certaines règles et principes clés en matière de protection des données (tels que le consentement et la transparence);
- actualiser le cadre par l'ajout de nouveaux principes (tels que la « prise en compte du respect de la vie privée dès la conception » et la « responsabilité »);
- renforcer l'efficacité du système par la modernisation des dispositions de la directive 95/46/CE (par exemple en limitant la charge administrative);
- intégrer les principes fondamentaux de la protection des données dans un cadre juridique global, qui s'applique également à la coopération policière et judiciaire en matière pénale.

2. Un cadre global unique

Le cadre juridique actuel

9. La protection des données, telle qu'introduite dans le cadre juridique de l'Union européenne, relève du marché intérieur. La directive 95/46/CE est fondée sur l'article 95 CE. Son objectif est double. En effet, la création et le fonctionnement du marché intérieur nécessitent que les données à caractère personnel puissent circuler librement entre les États membres et que, dans le même temps, un niveau élevé de protection des droits fondamentaux des personnes soit garanti.

10. La directive 95/46/CE est conçue comme un cadre juridique général susceptible d'être complété par des régimes spécifiques de protection des données, pour des secteurs particuliers. Jusqu'à présent, un seul régime spécifique a été adopté: celui relatif à la protection de la vie privée dans le secteur des communications électroniques (actuellement la directive 2002/58/CE). En outre, plusieurs instruments législatifs sectoriels prévoient également des règles spécifiques en matière de traitement des données à caractère personnel[67] (blanchiment d'argent, législation douanière ou systèmes VIS, EURODAC ou SIS II).

11. Le recours à l'article 95 CE a eu une incidence sur le champ d'application de la directive 95/46/CE. Si la directive a été conçue comme un cadre général pour la protection des données et fonctionne en tant que tel à bien des égards, elle ne concerne ni le traitement par les institutions de l'UE, ni les opérations de traitement qui ne relèvent pas de l'ex-premier pilier (mais principalement de l'ex-troisième pilier). En ce qui concerne le traitement par les institutions de l'UE (dans la mesure où elles relèvent de l'ex-premier pilier), le règlement n° 45/2001, qui est en grande partie similaire à la directive 95/46/CE, a été adopté. La situation actuelle, au titre de l'ex-troisième pilier, peut être décrite comme un conglomérat de régimes de protection des données applicables dans diverses situations. Si certaines différences entre ces régimes tiennent à la spécificité du secteur concerné, d'autres sont simplement le fruit d'une histoire législative différente. La décision-cadre 2008/977/JAI peut être considérée comme un premier pas vers la création d'un cadre plus général.

12. Cette situation n'est pas satisfaisante, notamment en ce qui concerne le troisième pilier:

67 Par exemple la directive 2005/60/CE du Parlement européen et du Conseil du 26 octobre 2005 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, JO L 309 du 25.11.2005, p. 15 et les différents instruments juridiques pour les systèmes d'information à grande échelle SIS, VIS et EURODAC.

- il est de plus en plus admis que la protection des données est désormais une préoccupation générale de l'Union européenne qui n'est pas nécessairement liée au marché intérieur. En témoigne, par exemple, l'article 8 de la Charte des droits fondamentaux de l'Union européenne;
- ces dernières années, et assurément depuis les attentats terroristes du 11 septembre 2001 aux États-Unis, l'échange des données à caractère personnel entre les États membres fait désormais partie intégrante de la coopération policière et judiciaire, et requiert bien entendu une protection adéquate;
- l'ancienne structure en piliers ne reflète pas la réalité de la protection des données. Les données à caractère personnel sont utilisées dans des situations communes aux différents piliers, comme l'illustrent le PNR et les arrêts concernant la conservation des données rendus par la Cour de justice des Communautés européennes dans des affaires d'exploitation, aux fins de la lutte contre la criminalité, d'informations collectées initialement dans un contexte économique.

La nécessité d'un nouveau cadre

13. Les lacunes du système actuel imposent de réfléchir à « un cadre de protection des données global et cohérent, couvrant tous les domaines de compétence de l'UE »[68]. Le traité de Lisbonne prévoit une nouvelle approche horizontale de la protection des données et de la vie privée, ainsi que la base juridique nécessaire (article 16 du TFUE[69]) pour éliminer les différences et divergences actuelles qui nuisent à une protection complète, cohérente et efficace de chaque individu.

14. Les garanties et principes essentiels devraient s'appliquer au traitement des données dans tous les secteurs, de sorte à assurer une approche intégrée, mais également une protection complète, cohérente et efficace.

15. La directive 95/46/CE devrait servir de référence au cadre global qui a pour principal objectif l'efficacité et la protection efficace des personnes. Les principes actuels de la protection des données doivent être approuvés et complétés par des mesures permettant de les mettre en œuvre plus efficacement (et d'assurer une protection plus efficace des données à caractère personnel des citoyens).

16. Les principes essentiels de la protection des données devraient constituer l'épine dorsale d'un cadre global: les notions (qui/responsable de données – quoi/données à caractère personnel) et principes clés devraient être réaffirmés, en particulier les principes de licéité, d'équité, de proportionnalité, de limitation des finalités, de transparence, ainsi que les droits des personnes concernées et le contrôle indépendant par les autorités publiques. La refonte du cadre offre également l'occasion de clarifier la mise en œuvre de certaines notions clés telles que:

- le consentement: il convient d'éviter la confusion entre le consentement préalable (« opt-in ») et l'option de refus (« opt-out ») devrait être évitée, de même que l'utilisation du consentement dans des situations où il ne constitue pas la base juridique appropriée (voir également le chapitre 5);
- la transparence: elle est une condition préalable au traitement équitable. Il convient de préciser que la transparence ne conduit pas nécessairement au consentement. Elle est néanmoins une condition préalable à un consentement valable et à l'exercice des droits de la personne concernée (voir également le chapitre 5).

L'objectif devrait être d'améliorer la protection des données au niveau international, conformément aux principes et aux droits définis par la directive 95/46/CE, tout en maintenant le niveau actuel de protection (voir également le chapitre 3).

68 Formulation employée par la Commission dans COM (2009)262 final.

69 L'article 16 TFUE couvre non seulement le troisième pilier mais également le deuxième (politique étrangère et de sécurité commune) en ce qui concerne le traitement des données à caractère personnel par les institutions de l'UE. L'article 39 TUE prévoit une base juridique spécifique pour le traitement des données par les États membres au titre du deuxième pilier. Ces dispositions s'appliquent par exemple aux listes de terroristes établies par l'UE et les États membres, mais ne seront pas spécifiquement évoquées dans le présent chapitre.

17. L'adoption d'un cadre global unique permettrait aussi d'actualiser utilement les règles existantes, notamment en introduisant le principe général de « prise en compte du respect de la vie privée dès la conception » dans le prolongement des règle actuelles en matière de mesures d'organisation et de sécurité technique (voir également le chapitre 4) et le principe général de responsabilité (voir également le chapitre 6).

L'architecture d'un cadre global

18. L'existence d'un cadre global unique, reposant, conformément au traité de Lisbonne, sur une base juridique unique, ne signifie pas nécessairement que toute souplesse et toute différence entre les secteurs et entre les États membres est exclue du champ d'application dudit cadre. Des règles spécifiques (*leges speciales*) pourraient le compléter et améliorer la protection, à condition qu'elles soient conformes à la notion de cadre global et respectent les principes essentiels précédemment évoqués.

19. Des règlements sectoriels et spécifiques supplémentaires pourraient être envisagés, par exemple en ce qui concerne:

- des secteurs spécifiques, tels que la santé publique, l'emploi ou les systèmes de transport intelligents;
- les outils et services liés au respect de la vie privée, tels que les certifications et les audits (voir également les chapitres 4 et 6);
- les violations de la sécurité (en complément du principe de sécurité, voir également les chapitres 5 et 6);
- la coopération policière et judiciaire, telle qu'explicitement prévue dans la déclaration 21 annexée au traité de Lisbonne (voir ci-après le chapitre 8);
- la politique en matière de sécurité nationale, telle qu'explicitement prévue dans la déclaration 20 annexée au traité de Lisbonne.

20. Des règlements nationaux supplémentaires pourraient être envisagés, compte tenu des différences culturelles et de l'organisation interne des États membres, à condition qu'ils ne nuisent pas à l'harmonisation nécessaire dans une Union européenne sans frontières intérieures.

21. Une harmonisation accrue est indispensable dans un cadre juridique clair et non équivoque, sans pour autant exclure la valeur ajoutée que peut apporter une certaine souplesse, comme le reconnaît actuellement la directive 95/46/CE, par exemple, si cette souplesse est nécessaire en raison de différences culturelles. On pourrait également laisser au législateur national la possibilité d'attribuer les responsabilités et de reconnaître les différents rôles des secteurs public et privé.

3. Mondialisation

Le contexte et le cadre juridique actuel

22. Dans le droit de l'UE, la protection des données est un droit fondamental, consacré par l'article 8 de la Charte des droits fondamentaux de l'Union européenne (voir également le chapitre 1). Dans d'autres régions du monde, la nécessité de protéger les données est largement reconnue, mais pas nécessairement avec le statut d'un droit fondamental.

23. L'UE et ses États membres devraient garantir ce droit fondamental à toute personne, dans la mesure de leurs compétences. Dans un monde globalisé, cela signifie que les personnes physiques peuvent également réclamer la protection de leurs données si ces dernières font l'objet d'un traitement à l'extérieur de l'Union européenne.

24. La directive 95/46/CE répond à ce besoin de protection dans son article 4. Elle est applicable au traitement des données dans le monde entier et donc aussi à l'extérieur de l'UE[70] (a) lorsque le responsable du traitement des données est établi dans l'UE et (b) lorsqu'il est établi en dehors de l'UE mais utilise des équipements situés dans l'Union.

70 Dans ce contexte, l'UE englobe également les pays de l'AELE.

25. En outre, les articles 25 et 26 de la directive 95/46/CE prévoient un régime spécifique pour le transfert des données à caractère personnel vers les pays tiers. La règle fondamentale de l'article 25 autorise le transfert des données uniquement vers les pays tiers qui assurent un niveau de protection adéquat. L'article 26 prévoit un certain nombre de dérogations à cette règle. Des notions bien connues, comme les règles d'entreprise contraignantes et les clauses contractuelles types, mettent en œuvre cette disposition.

Droit applicable

26. La portée exacte de la directive 95/46/CE n'est toutefois pas suffisamment claire. On ne sait pas toujours si le droit de l'UE est applicable, quel droit national s'applique et quel(s) droit(s) s'appliquerai(en)t lorsque plusieurs établissements d'une société multinationale sont implantés dans différents États membres. L'article 4 de la directive, qui détermine les cas où celle-ci est applicable au traitement des données, laisse le champ libre à différentes interprétations.

27. En outre, certaines situations ne relèvent pas du champ d'application de la directive. C'est le cas lorsque les activités de responsables du traitement des données établis en dehors de l'UE concernent des résidents de l'UE, ce qui donne lieu à la collecte et à un traitement supplémentaire de données à caractère personnel. C'est le cas par exemple des commerçants en ligne et d'autres fournisseurs qui utilisent des publicités « couleur locale », des sites web qui ciblent directement les citoyens de l'UE (dans leur langue notamment). Si ces activités sont menées sans utiliser d'équipements installés dans l'UE, la directive 95/46/CE ne s'applique pas.

28. Le groupe de travail 29 prépare actuellement un avis sur la notion de droit applicable, qu'il envisage de rendre à la Commission européenne au cours de l'année prochaine. Cet avis pourrait comprendre de nouvelles recommandations en faveur d'un futur cadre juridique.

Les normes internationales et la résolution de Madrid

29. Il devient indispensable d'élaborer des normes globales pour la protection des données. Elles faciliteraient également la circulation transfrontalière des données qui, en raison de la mondialisation, devient la règle plutôt que l'exception. Tant que des normes globales ne seront pas mises en place, la diversité perdurera. La circulation transfrontalière des données doit être facilitée et, dans le même temps, un niveau élevé de protection des données à caractère personnel doit être assuré lorsque celles-ci font l'objet d'un transfert et d'un traitement dans des pays tiers.

30. La « résolution de Madrid », proposition conjointe de normes internationales pour la protection de la vie privée adoptée le 6 novembre 2009 par la Conférence internationale des commissaires à la protection des données et de la vie privée, mérite d'être soutenue. La proposition présente un projet de norme globale et réunit toutes les approches possibles en matière de protection des données à caractère personnel et de la vie privée, en intégrant la législation des cinq continents. Elle propose une série de principes, droits et obligations qui devraient constituer le socle de la protection des données de tout système juridique dans le monde, et démontre que des normes globales offrant un niveau adéquat de protection des données peuvent être élaborées en temps utile.

31. Il est demandé à la Commission de:

- prendre des initiatives pour renforcer le développement de normes internationales globales pour la protection des données à caractère personnel, afin de promouvoir un cadre international pour la protection des données et faciliter ainsi la circulation transfrontalière des données, tout en assurant un niveau de protection adéquat des personnes concernées. Ces initiatives devraient également examiner la faisabilité d'un cadre international contraignant;
- promouvoir, en l'absence de normes globales, le développement de la législation en matière de protection des données pour assurer un niveau de protection adéquat, et la création d'autorités indépendantes chargées de la protection des

données dans les pays extérieurs à l'Union européenne. Les principes fondamentaux de la protection des données, tels qu'énoncés dans la « résolution de Madrid », devraient constituer la base universelle d'une telle législation.

Ces missions spécifiques de la Commission devraient figurer dans le futur cadre juridique.

Amélioration des décisions relatives au niveau de protection adéquat

32. Dans un environnement mondialisé, le nombre d'opérations de traitement de données à caractère personnel ne cesse de progresser. Assurer la libre circulation des données à caractère personnel tout en garantissant le niveau de protection des droits des personnes est une exigence toujours plus forte. Il est donc nécessaire de repenser le processus d'évaluation du caractère adéquat de la protection:

- en définissant de manière plus précise les critères permettant d'atteindre le statut juridique de « niveau de protection adéquat », en tenant pleinement compte de l'approche du groupe de travail 29[71] et de diverses autres approches de la protection des données dans le monde, et notamment les droits et principes définis par la proposition conjointe de normes internationales sur la protection de la vie privée;
- en rationalisant les procédures d'analyse des régimes juridiques des pays tiers, afin de prendre davantage de décisions sur le niveau de protection adéquat.

Le futur cadre juridique devrait préciser ces questions.

Accords internationaux

33. Il a été pris bonne note des activités du groupe de contact à haut niveau UE/États-Unis sur le partage d'informations et la protection de la vie privée et des données à caractère personnel. Ces activités pourraient conduire à un accord transatlantique prévoyant des principes communs pour la protection de la vie privée et des données applicables à l'échange d'informations avec les États-Unis, dans le cadre de la lutte contre le terrorisme et la criminalité transnationale grave[72].

34. Les accords internationaux sont des instruments appropriés pour la protection des données à caractère personnel dans un contexte mondial, à condition que le niveau de protection offert soit au moins équivalent aux normes globales précédemment évoquées, que toute personne physique dispose d'un recours facile et efficace, notamment au niveau juridique, et que des garanties spécifiques soient fournies en ce qui concerne la finalité envisagée pour ces données à caractère personnel.

35. Si ces conditions sont remplies, l'accord transatlantique envisagé pourrait servir de modèle pour l'échange d'informations avec d'autres pays tiers et à d'autres fins. Le futur cadre juridique pourrait prévoir les conditions applicables aux accords conclus avec des pays tiers.

36. En outre, l'UE devrait encourager la coopération entre les autorités internationales de protection des données, par exemple, au niveau transatlantique. Une telle coopération permettrait de promouvoir efficacement la protection des données à l'extérieur de l'UE.

Règles d'entreprise contraignantes/responsabilité

37. Le traitement des données à l'extérieur de l'UE peut également être protégé par des règles d'entreprise contraignantes, codes de conduite internationaux pour les sociétés multinationales, qui prévoient un transfert des données au niveau mondial au sein d'une entreprise multinationale. Les règles d'entreprise contraignantes ont été introduites par le groupe de travail 29 en 2003. Les autorités chargées de la protection des données comme les multinationales les considèrent comme un moyen efficace de faciliter la circulation internationale des données tout en garantissant la protection des données à caractère personnel. Néanmoins, la directive 95/46/CE ne tient pas expressément compte de ces règles. Par conséquent, le processus

71 Voir en particulier le document de travail 12 du groupe de travail 29, intitulé « Transferts de données personnelles vers des pays tiers: application des articles 25 et 26 de la directive relative à la protection des données », adopté le 24 juillet 1998.

72 À cet égard, le problème transatlantique concernant les recours reste à résoudre.

d'adoption des règles d'entreprise contraignantes, qui repose sur l'article 26, paragraphe 2, de la directive 95/46/CE, requiert l'approbation de tous les États membres concernés. Dès lors, le processus d'évaluation et d'approbation des règles d'entreprise contraignantes prend beaucoup de temps. Le groupe de travail 29 n'a pas ménagé ses efforts pour promouvoir et faciliter l'utilisation et l'approbation des règles d'entreprise contraignantes dans le cadre juridique actuel. Pour aller plus loin, dix-neuf autorités chargées de la protection des données ont à ce jour convenu d'une procédure d'approbation des règles d'entreprise contraignantes, appelée « reconnaissance mutuelle ».

38. Dans ce contexte, le nouveau cadre juridique devrait comprendre une disposition renforcée sur les règles d'entreprise contraignantes, pour répondre à plusieurs objectifs:

- reconnaître que les règles d'entreprise contraignantes constituent un outil pertinent capable d'offrir les garanties adéquates;
- définir les principaux éléments de contenu et de procédure de ces règles, conformément aux avis rendus par le groupe de travail 29 sur cette question.

39. En outre, de manière générale, le nouveau cadre législatif pourrait comprendre une nouvelle disposition prévoyant que les responsables du traitement des données demeureraient responsables de la protection des données à caractère personnel dont ils ont la responsabilité du traitement, même en cas de transfert de ces données à d'autres responsables établis à l'extérieur de l'UE (pour la question de la « responsabilité », voir aussi plus généralement le chapitre 6).

Conclusion

40. Ce chapitre aborde la mondialisation en tant que telle, même si, d'une manière ou d'une autre, tous les chapitres de la présente contribution traitent ce thème. On associe fréquemment la « mondialisation » à l'activité économique. Pourtant, les opérations de traitement des données à caractère personnel effectuées dans un contexte mondialisé sont toujours plus nombreuses. Si le contexte local est souvent celui dans lequel évoluent les personnes physiques, ces dernières utilisent de plus en plus l'internet, où leurs données font l'objet d'un traitement mondial. La mondialisation dépend dès lors de la technologie (chapitre 4), de la place occupée par la personne concernée (chapitre 5), du responsable du traitement des données (chapitre 6), des autorités chargées de la protection des données/du groupe de travail 29 (chapitre 7) et de la lutte contre la criminalité (chapitre 8).

4. Évolutions technologiques: la prise en compte du respect de la vie privée dès la conception, un nouveau principe

41. Les concepts de base de la directive 95/46/CE ont été élaborés dans les années 1970, à une époque où le traitement des informations se caractérisait par l'utilisation de fichiers manuels, de cartes perforées et de gros systèmes informatiques. Aujourd'hui, l'informatique est omniprésente, mondiale et connectée. Les systèmes sont de plus en plus miniaturisés et équipés de cartes réseau, de WiFi et d'autres interfaces radio. Dans presque tous les bureaux et foyers, les utilisateurs peuvent communiquer avec le monde entier via l'internet. Les services du web 2.0 et l'informatique dématérialisée ne permettent plus de distinguer les responsables du traitement des données des sous-traitants et des personnes concernées.

42. La directive 95/46/CE a bien résisté à ces évolutions technologiques, grâce à des principes et des concepts qui sont non seulement solides mais aussi neutres sur le plan technologique. Ces principes et concepts restent tout aussi pertinents, valables et applicables dans le monde connecté actuel.

43. S'il est clair que les évolutions technologiques décrites précédemment sont généralement bénéfiques pour la société, elles n'en ont pas moins accru les risques en matière de protection de la vie privée et des données à caractère personnel. Pour compenser ces risques, le cadre juridique de protection des données devrait être complété. Premièrement, le principe de « prise en compte du respect de la vie privée dès la conception » devrait

être introduit dans le nouveau cadre juridique; deuxièmement, il conviendrait d'adopter, le cas échéant, des règlements applicables à des contextes technologiques spécifiques, prévoyant la prise en compte des principes de protection des données et de la vie privée dans ces contextes.

Principe de la prise en compte du respect de la vie privée dès la conception

44. L'idée d'intégrer des garanties technologiques en matière de protection des données dans les technologies de l'information et de la communication (« TIC ») n'est pas entièrement nouvelle. La directive 95/46/CE contient déjà plusieurs dispositions qui prévoient expressément que les responsables du traitement des données doivent mettre en œuvre des garanties technologiques lors de la conception et l'utilisation des TIC. C'est le cas de l'article 17 qui leur impose d'appliquer des mesures techniques et d'organisation appropriées. Le considérant 46 demande que de telles mesures soient prises tant au moment de la conception du système de traitement qu'à celui de la mise en œuvre du traitement lui-même. L'article 16 instaure la confidentialité du traitement, règle reprise et complétée dans les règlements sur la sécurité informatique. Outre ces articles, les principes relatifs à la qualité des données, tels que visés à l'article 6 (traitement loyal et licite, limitation des finalités, pertinence, exactitude, durée de conservation limitée, responsabilité), s'appliquent également.

45. Si les dispositions susmentionnées de la directive contribuent à promouvoir la prise en compte du respect de la vie privée dès la conception, elles n'ont, en pratique, pas suffi à garantir l'intégration du respect de la vie privée dans les TIC. Les utilisateurs de services TIC, à savoir les entreprises, le secteur public et plus encore les personnes physiques, ne sont pas en mesure de prendre eux-mêmes les mesures de sécurité appropriées pour protéger leurs propres données à caractère personnel ou celles d'autres personnes. Par conséquent, ces services et technologies devraient être conçus avec un paramétrage par défaut favorable au respect de la vie privée.

46. Aussi le nouveau cadre juridique doit-il prévoir une disposition qui traduise les prescriptions ponctuelles actuelles en un principe plus large et cohérent de prise en compte du respect de la vie privée dès la conception. Ce principe devrait être contraignant pour les concepteurs et producteurs de technologies ainsi que pour les responsables du traitement des données chargés de l'achat et de l'utilisation des TIC. Ils devraient avoir l'obligation de prendre en compte la protection technologique des données dès la phase de planification des procédures et des systèmes technologiques d'information. Les fournisseurs de tels systèmes ou services et les responsables du traitement des données devraient démontrer qu'ils ont pris toutes les mesures requises pour remplir ces obligations.

47. Un tel principe devrait requérir la mise en œuvre de la protection des données dans les TIC (prise en compte du respect de la vie privée dès la conception) conçues ou utilisées pour le traitement des données à caractère personnel. Il devrait impliquer que les TIC doivent non seulement assurer la sécurité mais également être conçus et développés de sorte à éviter ou à limiter la quantité de données à caractère personnel traitées. Cette approche est conforme à la jurisprudence allemande récente.13[73]

48. L'application de ce principe soulignerait la nécessité de mettre en œuvre des technologies qui améliorent la protection de la vie privée, un paramétrage par défaut favorable au respect de la vie privée et des outils indispensables aux utilisateurs pour mieux protéger leurs données à caractère personnel (par exemple, les contrôles d'accès ou le cryptage).

73 Récemment, la Cour constitutionnelle allemande (arrêt du 27 février 2008 - 1 BvR 370/07; 1 BvR 595/07 –) a créé un droit constitutionnel à la confidentialité et à l'intégrité des systèmes informatiques. Les systèmes capables de créer, de traiter ou de stocker des données sensibles à caractère personnel requièrent une protection particulière. Le champ de protection du droit fondamental à la confidentialité et à l'intégrité des systèmes d'informations s'étend aux systèmes qui, seuls ou du fait de leur interconnectivité technique, peuvent contenir des données à caractère personnel sur la personne concernée, à un degré et dans une diversité tels que l'accès aux systèmes fournit des informations sur des éléments importants de la vie de cette personne ou dresse un portrait révélateur de sa personnalité. Ces systèmes sont par exemple les ordinateurs personnels et les ordinateurs portables, les téléphones portables et les agendas électroniques.

Les produits et services fournis aux tiers et aux clients particuliers (par exemple les routeurs Wifi, les réseaux sociaux et les moteurs de recherche) devraient être soumis à l'obligation d'appliquer ce principe. Quant aux autorités chargées de la protection des données, elles auraient davantage de pouvoir pour mettre en œuvre efficacement de telles mesures.

49. Ce principe devrait être défini de manière *neutre sur le plan technologique* pour qu'il puisse durer longtemps dans un contexte technologique et social en constante mutation. Il devrait également être assez *souple* pour permettre aux responsables du traitement des données et aux autorités chargées de leur protection, de le convertir, au cas par cas, en mesures concrètes garantissant la protection des données.

50. Il devrait également souligner, comme le fait l'actuel considérant 46, la nécessité d'une application *dès que possible*, « tant au moment de la conception qu'à celui de la mise en œuvre du traitement ». Les garanties mises en œuvre tardivement ne sont pas cohérentes ni suffisantes au regard des exigences d'une protection efficace des droits et des libertés des personnes concernées.

51. Des normes technologiques devraient être développées et prises en compte lors de la phase d'analyse du système par des ingénieurs en logiciels et matériel informatique, de sorte à limiter les difficultés liées à la définition et à la fixation des obligations découlant du principe de prise en compte du respect de la vie privée dès la conception. De telles normes pourraient être générales ou spécifiques, en fonction des finalités et des technologies de traitement.

52. Les exemples suivants montrent comment la prise en compte du respect de la vie privée dès la conception peut contribuer à une meilleure protection des données:

- les identificateurs biométriques devraient être conservés dans des dispositifs contrôlés par les personnes concernées (c'est-à-dire via des cartes à puces) plutôt que dans des bases de données externes;
- les systèmes de vidéosurveillance des transports publics devraient être conçus de sorte que le visage des personnes enregistrées ne soit pas reconnaissable ou que d'autres mesures soient prises pour réduire les risques pour les personnes concernées. Bien entendu, des exceptions doivent être prévues pour des circonstances exceptionnelles, par exemple lorsque la personne est suspectée d'avoir commis une infraction pénale;
- les noms des patients et d'autres identificateurs personnels conservés dans les systèmes d'information des hôpitaux devraient être séparés des données relatives à l'état de santé et au traitement médical. Ces éléments devraient être combinées uniquement en cas de nécessité, pour des raisons médicales ou d'autres raisons valables, dans un environnement sécurisé;
- si nécessaire, une fonctionnalité devrait être intégrée pour permettre à la personne concernée d'annuler son consentement, ce qui aurait pour effet de supprimer ses données de tous les serveurs concernés (y compris les serveurs proxy et miroirs).

53. En pratique, la mise en œuvre du principe de prise en compte du respect de la vie privée dès la conception exigera l'évaluation de plusieurs éléments ou objectifs concrets. En particulier, avant de décider de la conception d'un système de traitement, de son achat et de son utilisation, les éléments/objectifs généraux suivants devraient être pris en compte:

- limitation autant que possible des données: les systèmes de traitement des données doivent être conçus et choisis en accord avec la finalité de ne collecter, traiter ou exploiter aucune donnée à caractère personnel ou une quantité aussi faible que possible de ce type de données;
- capacité de contrôle: un système informatique devrait fournir aux personnes concernées des moyens de contrôle efficaces de leurs données à caractère personnel. Les possibilités d'autorisation et de refus devraient être facilitées par les moyens technologiques;

- transparence: les développeurs et gestionnaires de systèmes informatiques doivent s'assurer que les personnes concernées sont suffisamment informées du mode opératoire des systèmes. L'accès électronique / l'accès aux informations devrait être assuré;
- systèmes conviviaux: les fonctions et dispositifs associés au respect de la vie privée devraient être conviviaux, autrement dit proposer une aide suffisante et des interfaces simples, susceptibles d'être également utilisées par des personnes peu expérimentées;
- confidentialité des données: les systèmes informatiques doivent être conçus et sécurisés de sorte que seules des entités autorisées aient accès aux données à caractère personnel;
- qualité des données: les responsables du traitement des données doivent assurer la qualité des données par des moyens techniques. Les données pertinentes devraient être accessibles, le cas échéant, à des fins licites.
- restriction d'emploi: les systèmes informatiques, affectés à différentes finalités ou fonctionnant dans un environnement multi-utilisateurs (à savoir les systèmes virtuellement connectés tels que les entrepôts de données, l'informatique dématérialisée, les identificateurs numériques), doivent garantir que les données et processus servant à différentes tâches ou finalités puissent être isolés les uns des autres de manière sécurisée.

Règlements relatifs aux contextes technologiques spécifiques

54. Le principe de la prise en compte du respect de la vie privée dès la conception peut ne pas suffire à garantir, en toutes circonstances, que les principes appropriés de protection des données technologiques sont correctement pris en compte par les TIC. Dans certains cas, une approche pragmatique plus concrète pourra être nécessaire. Pour faciliter la mise en œuvre de telles mesures, un nouveau cadre juridique devrait contenir une disposition permettant l'adoption de règlements spécifiques en cas de contexte technologique particulier, exigeant la prise en compte des principes de protection de la vie privée dans ce contexte.

55. Il n'y a là aucune nouveauté: l'article 14, paragraphe 3, de la directive relative à la vie privée et aux communications électroniques prévoit une disposition similaire: « Au besoin, des mesures peuvent être adoptées afin de garantir que les équipements terminaux seront construits de manière compatible avec le droit des utilisateurs de protéger et de contrôler l'utilisation de leurs données à caractère personnel, conformément à la directive 1999/5/CE et à la décision 87/95/CEE du Conseil du 22 décembre 1986 relative à la normalisation dans le domaine des technologies de l'information et des télécommunications ».

56. Cette disposition faciliterait l'adoption, dans des cas particuliers, de mesures législatives spécifiques intégrant le concept de « prise en compte du respect de la vie privée dès la conception » et garantissant que les spécifications adéquates sont fournies. Cela pourrait par exemple être le cas de la technologie RFID, des réseaux sociaux, de la publicité comportementale, etc.

Conclusion

57. L'importance croissante de la protection des données lors de la création et de l'exécution de systèmes informatiques soumet les informaticiens à de nouvelles obligations. Pour cette raison, la protection des données doit impérativement être intégrée dans la formation des personnels informatiques.

58. Les principes de la protection des données technologiques et les critères concrets qui en résultent devraient servir de base à l'attribution de labels de qualité (systèmes de certification) dans le cadre d'un audit de la protection des données[74].

74 C'est par exemple le cas avec le projet EuroPriSe.

5. Habilitation des personnes concernées

59. Toutes les possibilités associées à la place de la personne concernée dans la directive 95/46/CE n'ont pas été exploitées. En outre, tant le comportement des citoyens que le rôle des personnes concernées au regard de la protection des données ont changé, sous l'effet, notamment, des évolutions sociologiques et des nouvelles méthodes de collecte des données (par exemple à des fins de profilage). Il arrive que les personnes concernées fassent preuve de négligence en ce qui concerne la protection de leur propre vie privée, et elles sont parfois prêtes à y renoncer pour obtenir des avantages réels ou imaginaires. Et pourtant, elles attendent toujours beaucoup des entités avec lesquelles elles sont en relation commerciale. En outre, elles jouent elles-mêmes un rôle de plus en plus actif dans le traitement des données à caractère personnel, en particulier sur l'internet.

60. L'évolution du comportement et du rôle de la personne concernée, ainsi que l'expérience acquise grâce à la directive 95/46/CE imposent d'accorder aux personnes une place plus importante dans la protection des données[75]. Il est essentiel de donner à la personne concernée les moyens de jouer un rôle plus actif.

Amélioration des voies de recours

61. Pour habiliter la personne concernée, il faut lui donner davantage de possibilités d'exercer et de faire valoir ses droits. La procédure judiciaire réservant parfois de nombreuses difficultés et comportant un risque financier, la possibilité d'une procédure de recours collectif devrait être introduite dans la directive 95/46/CE[76].

62. En outre, les responsables du traitement des données devraient prévoir des procédures de plainte plus aisément accessibles, plus efficaces et moins coûteuses (voir également le chapitre 6). Si ces procédures ne permettent pas de régler le litige entre le responsable du traitement des données et la personne concernée, cette dernière devrait avoir la possibilité de recourir à des modes alternatifs de règlement des litiges, essentiellement prévus par l'industrie[77]. Ces possibilités devraient être incluses dans le nouveau cadre législatif.

Transparence

63. La transparence est une autre condition fondamentale, car elle permet à la personne concernée d'intervenir dans le traitement des données à caractère personnel en amont de celui-ci. Avec le profilage, l'extraction de données et les évolutions technologiques qui facilitent l'échange des données à caractère personnel, il est encore plus important pour la personne concernée de savoir qui traite les données, sur quelles bases, à partir de quel lieu, à quelles fins et avec quels moyens techniques. Il est important que ces informations soient compréhensibles. Toutefois, l'obligation d'information de la personne concernée (articles 10 et 11 de la directive 95/46/CE) n'est pas toujours correctement mise en pratique. Un nouveau cadre juridique devrait prévoir des solutions alternatives, pour une plus grande transparence. Par exemple, de nouvelles modalités d'information des personnes concernées pourraient être élaborées en ce qui concerne la publicité comportementale.

64. En outre, la transparence impose une information des personnes concernées en cas de violation de la vie privée susceptible de nuire à leurs données à caractère personnel ainsi qu'à leur vie privée. Elles pourraient de cette manière tenter de limiter le préjudice qu'elles ont subi (dans certains cas, les autorités devraient également être informées, voir aussi le chapitre 6). La notification générale de violation de la vie privée devrait être introduite dans le nouveau cadre juridique (voir également le chapitre 6)[78].

75 C'est notamment le cas en ce qui concerne les enfants. Au moment de prendre des décisions concernant leurs données à caractère personnel, leur intérêt supérieur doit être une considération primordiale, comme le prévoit la Convention des Nations Unies relative aux droits de l'enfant (http://www2.ohchr.org/french/law/crc.htm), d'autres instruments internationaux spécifiques et la législation nationale.

76 Des recours collectifs existent, par exemple, en droit environnemental.

77 Ce type de procédure ne peut bien entendu pas empêcher une personne de former un recours approprié auprès d'un tribunal ou d'une autorité chargée de la protection des données.

78 Dans l'« Avis 1/2009 concernant les propositions modifiant

Consentement

65. Dans la directive, le consentement de la personne concernée constitue un motif légitime de traitement des données (articles 7 et 8 de la directive 95/46/CE). Ce consentement est et demeure un motif important de traitement, qui pourrait, dans certaines circonstances, donner plus de pouvoir à la personne concernée. Toutefois, le consentement doit être une manifestation de volonté, libre, spécifique et informée [article 2, point h), de la directive 95/46/CE].

66. Dans de nombreux cas, le consentement ne peut être accordé librement, notamment en cas de déséquilibre évident entre la personne concernée et le responsable du traitement des données (par exemple, dans le contexte du travail ou lorsque les données à caractère personnel doivent être transmises aux pouvoirs publics).

67. En outre, l'exigence selon laquelle le consentement doit être informé présuppose que la personne concernée comprenne pleinement les conséquences de sa décision de consentir à un traitement de ses données. Toutefois, la complexité des pratiques de collecte des données, des modèles commerciaux, des relations entre fournisseurs et des applications technologiques dépassent, bien souvent, la capacité ou la volonté d'une personne de décider, par un choix actif, de contrôler l'utilisation et le partage d'informations[79].

68. Dans les deux hypothèses, si le consentement constitue un motif inapproprié de traitement, il est néanmoins souvent invoqué à tort comme le motif applicable. Les évolutions technologiques invitent également à un examen attentif du consentement. En pratique, l'article 7 de la directive 95/46/CE n'est pas toujours correctement appliqué, en particulier dans le contexte de l'internet, où un consentement implicite ne conduit pas toujours à un consentement non équivoque [comme le prévoit l'article 7, point a), de la directive]. Pour permettre aux personnes concernées de s'exprimer davantage en amont du traitement de leurs données à caractère personnel, il faut que le consentement soit donné explicitement (il faut par conséquent un accord préalable) pour l'ensemble du traitement basé sur le consentement[80].

69. Le nouveau cadre juridique devrait prévoir cette obligation de consentement, compte tenu des observations ci-dessus.

Harmonisation

70. À l'heure actuelle, l'habilitation des personnes concernées est limitée par l'absence d'harmonisation entre les législations nationales transposant la directive 95/46/CE. Plusieurs éléments de la directive qui sont essentiels pour la place des personnes concernées, tels que la disposition sur la responsabilité et la possibilité d'introduire une demande en indemnité pour préjudice immatériel[81], n'ont pas été transposés par l'ensemble des États membres. Outre ces différences de transposition de la directive 95/46CE, son interprétation dans les États membres n'est pas toujours homogène. À l'heure où la mondialisation s'intensifie, ces différences affaiblissent de plus en plus le rôle de la personne concernée. Par conséquent, il est essentiel d'améliorer l'harmonisation (voir également le chapitre 7b), en précisant si nécessaire les dispositions législatives.

la directive 2002/58/CE sur la protection de la vie privée dans le secteur des communications électroniques (directive « vie privée et communications électroniques ») », le groupe de travail 29 a relevé une approche recommandée sur la question des notifications spécifiques de violation de la vie privée reprises dans la directive relative à la vie privée et aux communications électroniques. Les mêmes recommandations s'appliquent à l'introduction de notifications générales de violation de la vie privée.

79 Voir « Data Protection Accountability: The essential Elements – A Document for Discussion », Centre for Information Policy Leadership, qui assure le secrétariat du projet Galway, octobre 2009, p. 4.

80 En ce qui concerne le consentement et le consentement préalable (opt-in)/l'option de refus (opt-out), voir également le chapitre 2, où il est indiqué que la confusion entre consentement préalable et option de refus doit être évitée, de même que le recours au consentement lorsqu'il ne constitue pas la base juridique adéquate.

81 Dans la plupart des cas où la personne concernée a subi un dommage, il s'agit de préjudice immatériel tel que le sentiment de ne plus pouvoir évoluer librement dans les secteurs public et privé sans être observé. Ce problème est encore plus vif dans l'actuelle « société de la surveillance ».

Le rôle des personnes concernées sur l'internet

71. Les personnes téléchargent de plus en plus leurs propres données à caractère personnel sur l'internet (dans le cadre de réseaux sociaux, de services informatiques dématérialisés, etc.). Néanmoins, la directive 95/46/CE ne s'applique pas à la personne qui télécharge les données « pour l'exercice d'activités exclusivement personnelles ou domestiques »[82]. On peut estimer qu'elle ne s'applique pas non plus à l'entité qui fournit le service, c'est-à-dire qui héberge et met à disposition les informations téléchargées par la personne physique (à moins que l'entité ne traite les données à ses propres fins) dans la mesure où le prestataire de services peut ne pas être considéré comme un responsable du traitement23[83]. Il en résulte une absence de garanties à laquelle il faudra peut-être remédier, notamment du fait que ces situations sont de plus en plus fréquentes. Dans ces circonstances, quiconque propose des services à une personne privée devrait être tenu de fournir certaines garanties en matière de sécurité et, si nécessaire, de confidentialité des informations téléchargées par les utilisateurs, que son client soit ou non un responsable du traitement des données. En outre, il conviendrait de s'intéresser à la question de savoir si les personnes concernées devraient se voir accorder davantage de moyens pour faire valoir leurs droits sur l'internet, y compris la protection des droits de tiers dont les données à caractère personnel peuvent faire l'objet d'un traitement (par exemple sur les réseaux sociaux). De nombreuses autres questions restant encore sans réponse[84], le rôle de la personne concernée sur l'internet devrait être davantage précisé, dans la perspective d'un nouveau cadre juridique.

6. Renforcement de la responsabilité des responsables du traitement des données

72. Au titre de la directive 95/46/CE, le responsable du traitement des données est l'acteur clé qui veille au respect des principes et obligations visant à garantir la protection des données à caractère personnel des personnes physiques. La directive, de manière implicite mais également explicite en de nombreux points, impose au responsable du traitement de respecter les principes de protection des données et de se conformer à certaines obligations spécifiques25[85]. Il doit par exemple adresser une notification aux autorités nationales et vérifier préalablement auprès d'elles la légalité des opérations de traitement des données[86]. En outre, le respect des droits des personnes physiques en matière de protection des données implique d'imposer au responsable du traitement les obligations correspondantes, telles que la transmission d'informations[87].

73. Ces obligations s'appliquent aussi, de manière directe ou indirecte, aux sous-traitants si les responsables du traitement des données leur confient tout ou partie des opérations de traitement. Soucieux de préciser les notions de responsable du traitement des données et de sous-traitant des données, le groupe de travail 29 prépare actuellement un avis interprétatif sur la question, qu'il devrait rendre prochainement à la Commission. Cet avis pourrait comprendre de nouvelles recommandations pour un futur cadre juridique.

82 Pour mieux comprendre si une activité est couverte ou non par cette « exemption domestique », voir l'Avis 5/2009, sur les réseaux sociaux en ligne (WP 163).

83 Le problème ne se pose pas dans les organisations (du secteur public ou privé) utilisant des applications informatiques dématérialisées, car la directive s'applique à ces dernières, ainsi qu'à leurs opérations de traitement lorsqu'elles « [sont effectuées] dans le cadre des activités d'un établissement du responsabledu traitement » dans l'UE [voir l'article 4, paragraphe 1, point a)]. Le chapitre 5 s'applique donc à ces organisations, que le prestataire de services soit ou non établi dans l'UE.

84 Cela concerne, par exemple, le consentement des enfants et/ou de leurs parents, les demandes d'accès des autorités policières et judiciaires, les droits d'accès aux comptes internet de personnes décédées par leurs héritiers, et les demandes de tiers.

85 L'article 6, paragraphe 2, dispose explicitement qu' « [il] incombe au responsable du traitement d'assurer le respect du paragraphe 1 » (qui renvoie aux principes généraux relatifs à la qualité des données).

86 Voir les articles 18 à 21 de la directive 95/46/CE.

87 D'autres exemples des droits des personnes concernées comprennent le droit d'accès, de rectification, d'effacement et de blocage, et d'opposition au traitement des données à caractère personnel (articles 10 à 12 et article 14). Ces droits impliquent pour le responsable du traitement l'obligation de les respecter.

Intégration de la protection des données dans les organisations

74. Les dispositions pertinentes de la directive 65/46/CE forment une base incontestablement solide pour la protection des données à caractère personnel et devraient être maintenues. Néanmoins, le respect des obligations juridiques existantes est souvent insuffisamment intégré dans les pratiques internes des organisations. Il est fréquent que la protection de la vie privée ne soit pas prise en compte par les technologies et systèmes de traitement de l'information. En outre, la direction, notamment les cadres supérieurs, n'est généralement pas suffisamment au fait des pratiques en matière de traitement des données appliquées dans l'organisation et n'en est donc pas activement responsable. Les scandales liés à la protection des données qui ont éclaté dans certains États membres ces quelques dernières années témoignent de ce constat préoccupant.

75. Tant que la protection des données ne fera pas partie des valeurs et des pratiques communes d'une organisation et que les responsabilités n'en sont pas clairement attribuées, le respect effectif du principe de protection sera compromis et les incidents liés à la protection des données perdureront. Par ailleurs, une telle situation risque de fragiliser la confiance du public dans les entreprises comme dans les administrations publiques. En outre, l'intégration de la protection des données dans les cultures des organisations aidera les autorités chargées de la protection des données à mener à bien leurs missions de contrôle et de lutte contre la criminalité, comme il est expliqué au chapitre 7, ce qui aura pour effet d'accroître l'efficacité des mesures de protection de la vie privée.

76. Les principes et obligations énoncés dans la directive 95/46/CE devraient être au cœur même de la culture des organisations, à tous les niveaux, au lieu d'être considérés comme un ensemble d'obligations juridiques à valider par le service juridique. Les exigences énoncées par la directive devraient correspondre à des mesures concrètes de protection des données appliquées quotidiennement. Les contrôles en matière de protection de la vie privée devraient être pris en compte dès la conception des technologies et systèmes d'information (voir également le chapitre 4). En outre, au sein des organisations des secteurs public et privé, la responsabilité interne de la protection des données devrait être suffisamment reconnue, renforcée et attribuée de manière spécifique.

77. L'efficacité des dispositions de la directive 95/46/CE repose sur les efforts que déploient les responsables du traitement des données pour atteindre ces objectifs. Elle passe par les mesures proactives suivantes:

- *l'adoption par les responsables du traitement des données de politiques et processus internes* mettant en œuvre les exigences de la directive en ce qui concerne les opérations de traitement spécifiques réalisées par le responsable du traitement. Ces processus et politiques internes devraient être approuvés au plus haut niveau de l'organisation et par conséquent être imposés à l'ensemble du personnel;
- *la mise en place de mécanismes de mise en œuvre des politiques et processus internes, notamment le traitement des plaintes (voir également le chapitre 5),* afin de garantir l'efficacité pratique de ces politiques. Il pourra s'agir notamment de sensibiliser le personnel à la protection des données, de le former et de lui donner des instructions à ce sujet;
- *la rédaction de rapports de conformité et la réalisation d'audits, la certification par des organismes tiers* pour contrôler et évaluer si les mesures internes adoptées pour garantir le respect des obligations permettent de gérer efficacement, de protéger et d'assurer la sécurité des données à caractère personnel (voir également le chapitre 4);
- la conduite d'*études d'impact sur la vie privée*, notamment pour certaines opérations de traitement des données réputées présenter des risques spécifiques pour les droits et libertés des personnes concernées, par exemple en raison de leur nature, de leur portée ou de leur finalité;
- *l'attribution de la responsabilité de la protection des données* à des personnes désignées, directement

chargées du respect par leur organisation de la législation sur la protection des données;

- *la certification de la conformité par les cadres supérieurs de l'organisation*, confirmant qu'ils ont mis en place des garanties appropriées pour protéger les données à caractère personnel;
- *la transparence de ces mesures adoptées* vis-à-vis des personnes concernées et du public en général. Les obligations de transparence contribuent à la responsabilisation des personnes en charge du traitement des données (par exemple, publication des politiques de protection de la vie privée sur l'internet, transparence du traitement interne des plaintes et publication dans les rapports annuels).

78. L'article 17, paragraphe 1, de la directive 95/46/CE, impose déjà dans une certaine mesure aux responsables du traitement des données de mettre en œuvre les mesures techniques et d'organisation (le responsable du traitement des données doit « mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre [...] toute autre forme de traitement illicite »). Ces mesures peuvent comprendre certaines des recommandations susmentionnées. Toutefois, en pratique, l'article 17, paragraphe 1, n'a pas permis de rendre la protection des données suffisamment efficace dans les organisations en raison, notamment, de la diversité des approches adoptées par les mesures nationales de mise en œuvre.

Principe de responsabilité[88]

79. Pour résoudre ce problème, il conviendrait d'introduire un principe de responsabilité dans le cadre global aux termes duquel les responsables du traitement des données seraient contraints de prendre les mesures nécessaires pour veiller au respect des obligations et principes essentiels de la directive actuelle lors du traitement des données à caractère personnel. Une telle disposition renforcerait la nécessité de mettre en place des politiques et des mécanismes permettant la mise en œuvre effective des principes et obligations essentiels de la directive actuelle. Elle confirmerait la nécessité de prendre des mesures efficaces donnant lieu à une application interne efficace des obligations et principes essentiels actuellement consacrés dans la directive. En outre, le principe de responsabilité exigerait des responsables du traitement des données qu'ils mettent en place les mécanismes internes nécessaires pour démontrer leur conformité aux parties prenantes externes, notamment aux autorités nationales chargées de la protection des données. Au final, la nécessité de prouver que les mesures appropriées ont été prises pour assurer la conformité facilitera considérablement l'exécution des règles applicables.

80. En tout état de cause, les mesures attendues des responsables du traitement des données devraient être modulables et prendre en compte, entre autres critères, le type de la société (sa taille, son statut de société à responsabilité limitée), ainsi que le type, la nature et la quantité de données à caractère personnel qui lui sont confiées.

Autres solutions proactives ou réactives

81. Certaines des mesures décrites précédemment peuvent être considérées comme de bonnes pratiques, qui satisfont par conséquent au principe de responsabilité si elles sont mises en œuvre. La législation pourrait prévoir un système de récompense pour inciter les organisations à appliquer ces mesures.

82. Une autre solution pourrait être plus normative. Par exemple, l'article 17, paragraphe 1, pourrait être rédigé de sorte à proposer d'autres mesures proactives, comme celles évoquées précédemment, que les responsables du traitement des données seraient tenus de mettre en œuvre. Ces mesures devraient viser des objectifs spécifiques et être neutres sur le plan technologique.

83. D'autres mesures seraient de nature plus réactive. Appliquées en cas de traitement illicite des données à caractère personnel, elles pourraient notamment prévoir:

- *une obligation de notification en cas de violation de la sécurité* des données (voir également les chapitres 2 et 5)

88 Voir également le point 39 sur la responsabilité.

- *le renforcement des compétences des autorités chargées de la protection des données en matière de lutte contre la criminalité*, notamment l'adoption d'obligations concrètes pour garantir une protection efficace des données (voir également le chapitre 7a).

Simplification des notifications

84. Les notifications des opérations de traitement aux autorités nationales chargées de la protection des données pourraient être simplifiées ou réduites. Dans ce contexte, il convient d'examiner le lien entre le respect des exigences susmentionnées et la possibilité de préciser plus avant les obligations administratives, en particulier la notification d'activités de traitement des données aux autorités nationales chargées de la protection des données.

85. La notification contribue à sensibiliser le personnel des organisations aux opérations de traitement de données et aux pratiques liées à leur protection[89]. Elle donne également aux autorités chargées de la protection des données une vision des activités de traitement. Néanmoins, un renforcement des obligations en matière de gouvernance des données et de responsabilité pourrait permettre d'atteindre les mêmes objectifs. Ces mécanismes pourraient contribuer à la mise en œuvre des mesures nécessaires pour respecter les principes et obligations essentiels actuellement consacrés dans la directive et produire les preuves d'un tel respect.

86. Il convient d'examiner si et dans quelle mesure la notification pourrait être limitée aux cas de menace grave contre la protection de la vie privée, ce qui permettrait aux autorités chargées de la protection des données d'être plus sélectives et de concentrer leurs efforts sur ces situations. Même dans de tels cas, la notification pourrait être rationalisée, par exemple, par la communication des résultats des études d'impacts sur la vie privée ou des audits réalisés par des tiers. Elle pourrait être associée à un système d'enregistrement qui imposerait l'inscription de tous les responsables du traitement des données dans un registre tenu par l'autorité chargée de la protection des données, ce qui permettrait d'identifier aisément les organisations en vue d'une application efficace et efficiente de la loi, si nécessaire.

7. Les autorités chargées de la protection des données devraient avoir un rôle plus important et plus précis, et renforcer leur coopération au sein de l'UE

7a. Les autorités chargées de la protection des données

87. À l'heure actuelle, il existe d'importantes disparités entre les 27 États membres en ce qui concerne le rôle des autorités chargées de la protection des données. Ces disparités sont le fruit de l'histoire, de la jurisprudence, de la culture et de l'organisation interne qui varient d'un État membre à l'autre, mais également, à maints égards, de l'imprécision de la directive 95/46/CE. De plus, cette directive a, dans une certaine mesure, été transposée de manière incomplète dans certains pays, créant d'importantes disparités entre les États membres en ce qui concerne, notamment, le rôle, les ressources et les pouvoirs des autorités chargées de la protection des données.

88. Les nouveaux défis en matière de protection des données (la mondialisation et les évolutions technologiques, voir les chapitres 3 et 4) nécessitent un contrôle ferme, plus homogène et efficace des autorités chargées de la protection des données. Dès lors, le nouveau cadre devrait garantir l'application de normes homogènes en ce qui concerne l'indépendance, les pouvoirs réels et le rôle consultatif de ces autorités dans le processus législatif, mais également leur capacité à définir leur propre programme de travail, notamment en fixant les priorités en matière de traitement des plaintes. De telles normes devraient être adoptées à un haut niveau par des instances qui font autorité.

89 Ce point de vue est confirmé par le rapport du groupe de travail sur l'obligation de notification aux autorités nationales de contrôle, sur la meilleure utilisation des dérogations et des simplifications et sur le rôle des détachés à la protection des données dans l'Union européenne (WP 106), adopté le 18 janvier 2005.

89. Les autorités chargées de la protection des données doivent être pleinement et réellement indépendantes. L'actuel article 28, paragraphe 1, de la directive 95/46/CE manque de clarté à cet égard, comme le démontre l'affaire C-584/07 (Commission/Allemagne), actuellement examinée par la Cour de justice des Communautés européennes. Dans le nouveau cadre juridique, les autorités chargées de la protection des données devraient bénéficier:

- d'une indépendance institutionnelle totale et ne pas être subordonnées à une quelconque autre autorité gouvernementale;
- d'une indépendance fonctionnelle et ne pas être soumises aux instructions de l'entité contrôlée en ce qui concerne le contenu et l'étendue de ses activités;
- d'une indépendance matérielle. Elles devraient disposer d'une infrastructure adaptée à la conduite ininterrompue de leurs activités, notamment d'un financement suffisant. Les autorités chargées de la protection des données devraient se voir affecter des ressources suffisantes.

90. Les autorités chargées de la protection des données jouent un rôle de plus en plus important dans la lutte contre la criminalité. Elles doivent être en mesure d'agir avec fermeté, audace et stratégie en matière d'intervention et de lutte contre la criminalité. La formulation actuelle de l'article 28 de la directive 95/46/CE a donné lieu à une grande disparité des pouvoirs de lutte contre la criminalité. Le nouveau cadre devrait inviter les États membres à adopter une approche plus homogène, qui dote les autorités chargées de la protection des données des pouvoirs nécessaires, et devrait être plus précis à cet égard que la directive 95/46/CE. Parmi les pouvoirs indispensables, citons la faculté d'infliger des sanctions financières aux responsables du traitement des données et à leurs sous-traitants.

91. Le rôle consultatif des autorités chargées de la protection des données dans le processus législatif est indispensable, car les connaissances acquises par ces autorités lors d'enquêtes et d'actions de contrôle est souvent nécessaire pour améliorer la législation (sur la protection des données). Ce rôle consultatif devrait concerner toutes les mesures et tous les règlements liés à la protection des droits et des libertés des personnes à l'égard du traitement de données à caractère personnel, et pas uniquement les « mesures réglementaires ou administratives »[90]. L'avis des autorités chargées de la protection des données devrait donc être sollicité avant que le projet de loi ne soit adopté. En outre, le nouveau cadre devrait veiller à ce que ces autorités remplissent un rôle consultatif auprès de leurs parlements nationaux et/ou autres institutions nationales compétentes, lorsque ces derniers participent à la rédaction d'une nouvelle législation de l'UE.

92. Elles devraient être en mesure d'établir leur propre programme de travail, en fixant, notamment, les priorités et les modalités de traitement des plaintes[91]. Elles devraient, en tout état de cause, pouvoir évaluer dans quelle mesure le traitement d'une plainte donnée peut contribuer suffisamment à la protection des données à caractère personnel[92]. Le nouveau cadre devrait permettre aux autorités chargées de la protection des données d'« être sélectives pour être efficaces ».

93. Par ailleurs, les autorités chargées de la protection des données doivent assumer la responsabilité de l'usage qu'elles font de leur pouvoir de contrôle accru. Elles devraient être transparentes à cet égard et rendre compte publiquement de leurs modalités d'action et des priorités qu'elles se fixent. La formulation actuelle de l'article 28, paragraphe 5, de la directive 95/46/CE devrait être précisée à cet égard dans le nouveau cadre.

90 Article 28, paragraphe 2, de la directive 95/46/CE.

91 La capacité de choix peut être mise en pratique de différentes manières, par exemple par l'établissement de procédures accélérées pour le traitement des plaintes mineures.

92 Les critères applicables pour déterminer si une plainte doit être traitée consistent par exemple à vérifier si celle-ci décrit une situation qui concerne un grand nombre de personnes, une violation de la législation sur la protection des données de faible importance et probablement pas un phénomène isolé, et si le traitement de la plainte donnera vraisemblablement lieu à une issue favorable et ne nécessite pas d'efforts disproportionnés.

7b. Coopération entre les autorités chargées de la protection des données

Le cadre juridique actuel

94. L'article 29 de la directive 95/46/CE institue le groupe de protection des personnes à l'égard du traitement des données à caractère personnel (groupe de travail 29) en tant qu'organisme institutionnel chargé de la coopération entre les autorités nationales chargées de la protection des données. Le groupe de travail 29 est un organe consultatif et indépendant. Conformément à l'article 30, paragraphe 1, de la directive, il a pour mission de contribuer à la mise en œuvre homogène de la directive, par l'examen de toute question portant sur l'application des dispositions nationales, de donner des avis sur le niveau de protection dans la Communauté et dans les pays tiers, et de conseiller (y compris de sa propre initiative) la Commission sur tout projet de législation communautaire ayant une incidence sur la protection des données ou sur tout autre sujet lié à la protection des personnes physiques à l'égard du traitement des données à caractère personnel dans la Communauté. La Commission est membre du groupe de travail 29 et en assure le secrétariat.

95. Le groupe de travail 29 remplit sa mission dans le cadre de la directive 95/46/CE, comme le prévoit son article 3, paragraphe 2. Dans le domaine de la coopération policière et judiciaire, les autorités européennes chargées de la protection des données ont créé en 2007 le groupe de travail « Police et justice » qui remplit une fonction similaire à celle du groupe de travail 29, mais sans base juridique ni secrétariat assuré par une institution de l'UE. La décision-cadre 2008/977/JAI, qui introduit les principes de protection des données dans ce domaine, ne prévoit aucune coopération institutionnalisée entre les autorités chargées de la protection des données.

Le fonctionnement du groupe de travail 29

96. Actif depuis plus de 10 ans, le groupe de travail 29 a largement contribué à la réalisation des objectifs de l'article 30 de la directive 95/46/CE. Les résultats d'un grand nombre de ses activités sont présentés sur son site[93].

97. Le groupe de travail 29 cherche constamment à renforcer son efficacité et devrait continuer à prêter une attention particulière à son fonctionnement. Il devrait notamment s'interroger sur la manière:

- de contribuer efficacement à la mise en oeuvre homogène de la législation de l'UE et des lois nationales ainsi qu'à l'application homogène de la législation nationale;
- d'améliorer son efficacité vis-à-vis des institutions de l'UE et en particulier de la Commission, en tenant également compte du rôle hybride de celle-ci en tant que membre, secrétariat et destinataire de la plupart des avis du groupe.

Conséquences pour l'avenir

98. La première priorité consiste à s'assurer que toutes les questions liées au traitement des données à caractère personnel, en particulier dans le domaine de la coopération policière et judiciaire en matière pénale, seront couvertes par les activités du groupe de travail actuel. Un cadre juridique global devrait prévoir un conseiller général et une coopération efficace entre les autorités de contrôle. Pendant une période transitoire, tant qu'aucune modification législative ne sera entrée en vigueur, des modalités appropriées de collaboration étroite devront être trouvées entre le groupe de travail 29 et le groupe de travail « Police et justice ».

99. D'autres améliorations ne nécessitent aucune modification législative.

- L'application homogène de la législation nationale transposant la directive 95/46/CE peut être assurée au sein du cadre juridique actuel, par le renforcement des méthodes de travail du groupe et, le cas échéant, par une volonté accrue de ses membres d'inscrire les points de vue du groupe de travail dans la pratique nationale.
- Conformément à l'article 29 de la directive 95/46/CE, le secrétariat du groupe de travail 29 est assuré

93 http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_fr.htm

par la Commission. Le secrétariat devrait travailler en étroite collaboration avec la présidence du groupe de travail 29 et son personnel. Les tâches du secrétariat et de la présidence sont complémentaires. Tous deux devraient travailler en étroite collaboration pour permettre au groupe de travail 29 de mener à bien ses missions aussi efficacement que possible. Le secrétariat gère tous les aspects logistiques des activités du groupe de travail et l'aide à préparer ses avis et documents. La présidence (et la viceprésidence) se consacre essentiellement au processus décisionnel et à la stratégie du groupe de travail 29.

- Les relations entre le groupe de travail et la Commission peuvent encore être améliorées par une description des fonctions essentielles des deux acteurs dans un protocole d'accord. Celui-ci devrait également porter sur les ressources mises à la disposition du groupe de travail 29 pour lui permettre d'exploiter pleinement ses capacités au service de sa mission. Enfin, il devra s'intéresser au fonctionnement du secrétariat, pour veiller à ce que ce dernier et le groupe de travail 29 disposent des ressources suffisantes pour préparer les avis et les documents de travail du groupe. Le groupe de travail 29 lancera une consultation avec la Commission sur l'ensemble de ces points en 2010.

8. Les défis de la protection des données dans le domaine de la police et de la lutte contre la criminalité

100. La protection des données dans le domaine de la police et de la justice est un sujet spécifique qui requiert une attention particulière, compte tenu de la relation complexe entre les activités de l'État visant à garantir la sécurité et la protection des données à caractère personnel des personnes physiques. La spécificité de cette question résulte non seulement de l'ancienne structure en piliers des précédents traités européens, mais est également plus largement reconnue (voir par exemple les exceptions de l'article 13 de la directive 95/46/CE et la déclaration 21 annexée au traité de Lisbonne).

Évolution du contexte communautaire

101. L'entrée en vigueur du traité de Lisbonne offrira de nouvelles perspectives pour le travail législatif dans le domaine de la protection des données. La structure en piliers sera supprimée, et l'article 16 du TFUE crée une base juridique unique pour la protection des données dans presque tous les domaines du droit de l'Union (voir le chapitre 2). Cela ne signifie pas nécessairement que la mise en oeuvre des principes de la protection des données en matière policière et judiciaire devrait être identique aux règles applicables aux autres secteurs de la société. La déclaration 21, annexée au traité de Lisbonne, prévoit que des règles spécifiques en matière de lutte contre la criminalité « pourraient s'avérer nécessaires ».

102. La protection et l'échange des données seront des thèmes importants du programme de Stockholm. Le processus décisionnel reposera sur la notion de juste équilibre entre les besoins qu'exige la lutte contre la criminalité et ceux liés à la protection des données. De nouvelles mesures ne devraient être adoptées qu'après évaluation adéquate du cadre juridique actuel.

103. La décision-cadre 2008/977/JAI relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale doit être transposée par les États membres avant le 27 novembre 2010. Elle peut être considérée comme un premier pas vers la création d'un cadre général relevant de l'ancien troisième pilier, mais est loin d'être complète. En effet, elle ne s'applique qu'aux situations transfrontalières. Il semble qu'elle ne prévoie pas d'éléments ni d'outils essentiels pour réagir efficacement à l'évolution des méthodes de travail en matière de lutte contre la criminalité.

Changement des priorités dans la lutte contre la criminalité

104. On a assisté ces dernières années à un changement des priorités dans les méthodes de travail des autorités policières et judiciaires, en ce qui concerne l'utilisation des informations (à caractère personnel). Ce changement résulte des besoins croissants

d'utilisation de ces informations pour combattre les nouvelles menaces résultant du terrorisme et de la criminalité organisée, mais également des progrès technologiques de ces dernières années.

105. Ce changement des priorités revêt plusieurs aspects:

- l'utilisation d'informations est orientée sur les premières étapes de la chaîne: outre l'utilisation habituelle à des fins d'enquête et de détection d'un crime spécifique, les informations sont recueillies et échangées pour prévenir d'éventuels actes criminels (« police préventive »);
- l'utilisation d'informations concerne un groupe plus large de personnes. Des informations sont collectées et échangées, non seulement sur les personnes directement liées à un crime telles que les suspects ou les témoins, mais aussi sur des groupes plus larges de personnes qui ne font pas l'objet d'une enquête (par exemple, les voyageurs, les utilisateurs de services de paiement, etc.);
- les informations utilisées sont de plus en plus associées aux technologies, qui permettent même d'assembler des éléments disparates pour prédire le comportement futur des personnes au moyen d'outils automatisés (extraction de données, profilage);
- les informations utilisées sont de nature différente: elles proviennent non seulement de données obtenues de façon objective (données vérifiées) mais également d'évaluations et d'analyses réalisées dans le cadre d'une enquête (données non vérifiées). Par ailleurs, la distinction entre ces deux types d'informations peut varier selon les États membres;
- l'utilisation accrue, à des fins préventives, d'informations à caractère personnel issues du secteur privé, comme les données bancaires/financières, et les données sur les passagers recueillies par les transporteurs aériens et le SIR;
- les informations collectées dans un but précis et légitime sont de plus en plus exploitées à des fins différentes, parfois incompatibles, et la tendance à leur recoupement est croissante. L'interopérabilité entre les systèmes est un élément important mais n'est pas une question purement technique, compte tenu notamment des risques d'interconnexion des bases de données aux finalités différentes;
- de plus en plus d'autorités participent à l'utilisation de ces données: les autorités policières et judiciaires, au sens strict, mais également d'autres autorités publiques telles que celles chargées du contrôle aux frontières, l'administration fiscale et les services en charge de la sécurité nationale.

106. Ce changement de priorités en matière de lutte contre la criminalité a accru fortement le stockage et l'échange de données à caractère personnel liés aux activités policières et judiciaires. Les possibilités technologiques permettant de combiner aisément les informations peuvent avoir une incidence profonde sur la protection de la vie privée et des données de tous les citoyens et sur leur capacité même de jouir pleinement de leurs droits fondamentaux et de les exercer, notamment dès lors que la liberté de circulation, la liberté de parole et la liberté d'expression sont en jeu.

Défis de la protection des données

107. Dans ce contexte, les défis posés par la protection des données sont immenses. Le futur cadre juridique devrait, en tout état de cause, prendre en compte les facteurs suivants:

- les tendances actuelles peuvent conduire à une surveillance plus ou moins permanente de l'ensemble des citoyens, souvent qualifiée de « société de la surveillance ». À titre d'exemple, citons l'utilisation combinée de caméras vidéo intelligentes et d'autres technologies, telles que la reconnaissance automatique des plaques minéralogiques, permettant d'enregistrer les entrées et sorties de tous les véhicules dans une zone donnée;
- les bases de données peuvent servir à l'extraction de données, et des évaluations des risques peuvent être réalisées sur la base du profilage des personnes physiques, ce qui peut conduire à stigmatiser les personnes issues de certains milieux;
- les analyses réalisées sur la base de critères généraux engendrent le risque d'inexactitudes importantes,

conduisant à un nombre élevé de faux négatifs et de faux positifs;

- le traitement des données à caractère personnel de personnes non suspectes prend de plus en plus d'ampleur. Des conditions et des garanties spécifiques sont indispensables pour évaluer leur légitimité et leur proportionnalité, et pour éviter toute atteinte aux personnes qui ne sont pas (activement) impliquées dans un délit;
- les données biométriques sont de plus en plus utilisées, notamment l'ADN, ce qui présente des risques spécifiques.

Conditions pour le processus législatif et l'élaboration des politiques

108. Le nombre croissant d'initiatives sectorielles adoptées ou programmées peut facilement conduire au double emploi ou même à des distorsions. Il peut donc s'avérer judicieux de fonder l'échange d'informations sur une stratégie cohérente, à condition que la protection des données soit pleinement prise en compte et intégrée à cette stratégie[94].

109. Il est primordial d'évaluer les instruments juridiques actuels et leur application, en tenant compte des coûts induits par la protection de la vie privée. L'évaluation des mesures actuelles devrait être effectuée avant que de nouvelles mesures ne soient prises. En outre, un examen périodique des mesures existantes devrait être réalisé.

110. La transparence est un élément essentiel. Les personnes concernées devraient disposer d'informations précises sur l'utilisation des informations collectées et sur la logique sous-jacente au traitement. Cette collecte d'informations devrait uniquement être limitée, si nécessaire, à des cas individuels, pour ne pas compromettre les enquêtes et pour une durée limitée. Les droits d'accès et de rectification des personnes concernées devraient être pris en compte dans un contexte transfrontalier pour éviter que ces personnes ne perdent le contrôle de leurs données.

111. Une attention particulière doit être accordée à la transparence et au contrôle démocratique du processus législatif. Une place importante devrait être accordée aux études d'impacts sur la vie privée, à des modes appropriés de consultation des autorités chargées de la protection des données et à un débat parlementaire efficace, aux niveaux national et européen.

112. L'architecture de tout système de stockage et d'échange de données à caractère personnel devrait être bien élaborée. On prendra note des quelques considérations générales suivantes:

- la prise en compte du respect de la vie privée dès la conception et les technologies améliorant la protection de la vie privée (système de certification) devraient déterminer cette architecture; en matière de liberté, de sécurité et de justice, domaines dans lesquels les autorités publiques jouent un rôle prépondérant et où chaque initiative visant à une surveillance accrue des personnes et à un renforcement de la collecte et de l'utilisation des informations à caractère personnel pourrait avoir une incidence directe sur le droit fondamental de ces personnes à la protection de leur vie privée et de leurs données, ces exigences pourraient être rendues obligatoires;
- la limitation des finalités et du nombre de données collectées devrait rester un principe directeur;
- l'accès à d'importantes bases de données doit être configuré de sorte à interdire, de manière générale, la consultation directe en ligne des données stockées, et un système « trouvé/non trouvé » ou dispositif d'indexation est généralement jugé préférable;
- le choix entre des modèles mettant en oeuvre un stockage central, à savoir des systèmes dotés d'une base de données centrale au niveau de l'UE et d'un stockage décentralisé, devrait être effectué sur la base de critères transparents et, en tout état de cause, s'accompagner de dispositions strictes prévoyant une définition claire du rôle et des obligations des responsables du traitement, et s'assurer d'un contrôle approprié par les autorités compétentes chargées de la protection des données;

94 Une stratégie européenne de gestion des informations, en cours d'élaboration par le Conseil, pourra, si elle est correctement mise en place, s'avérer utile dans ce contexte.

- les données biométriques devraient être utilisées uniquement si le recours à d'autres dispositifs moins intrusifs ne permet pas d'obtenir les mêmes résultats.

113. La dimension extérieure. Il conviendra d'éviter que le système rigoureux d'échange de données à caractère personnel au sein de l'UE soit contourné. Les relations avec les États tiers devraient s'appuyer sur un cadre précis, contraignant pour toutes les parties et reposant sur la notion de niveau de protection adéquat. Le système d'évaluation du caractère adéquat de la protection devrait être apprécié à la suite d'une évaluation par les autorités nationales chargées de la protection des données, si nécessaire réalisée au moyen de mécanismes communs assurant une mise en oeuvre cohérente et une grande efficacité.

114. Une attention particulière doit être accordée aux systèmes d'informations à grande échelle dans l'UE et, si nécessaire, des garanties spécifiques pourront être adoptées pour assurer la protection des données.

115. Un contrôle indépendant, de même qu'un contrôle judiciaire et des voies de recours devraient être prévus. En tout état de cause, un contrôle indépendant implique la mobilisation de ressources et de compétences appropriées.

116. La coopération entre les autorités chargées de la protection des données, qui doivent veiller à la licéité du traitement des données, devrait être renforcée à tous égards et être intégrée dans le cadre juridique. Elle devrait également prévoir des mécanismes stables, similaires à ceux actuellement à l'oeuvre pour les questions liées au premier pilier, afin de promouvoir une approche harmonisée dans toute l'UE et au-delà.

Pour le groupe de travail « Article 29 »

Le président
Alex TÜRK

Pour le groupe de travail « Police et justice »

Le président
Francesco PIZZETTI

Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel [STE 108] (T-PD) – Programme de travail du T-PD pour 2009 et les années à venir

Tel qu'approuvé par le T-PD lors de sa 25e réunion plénière

(2-4 septembre 2009, Strasbourg)

1 Amendements à la Convention 108[95]

En s'appuyant sur l'exemple du Protocole additionnel (STE No. 181), plusieurs amendements ayant trait aux différentes questions pourraient être traités simultanément. Dans cette optique il convient de définir les priorités de travail parmi les sujets proposés dans ce chapitre.

1.1 Convention 108 et les développements technologiques

Objectif : évaluer le besoin de compléments réglementaires nécessaires pour répondre aux défis posés à la protection des données par les développements technologiques liés à l'internet

1.2 Décision individuelle automatisée

Objectif : insertion d'une disposition régissant les décisions individuelles automatisées

1.3 Information obligatoire à fournir à la personne concernée par le responsable du traitement

Objectif : insertion d'une disposition définissant l'étendue de l'information à fournir par le responsable du traitement à la personne concernée relative au traitement de ses données personnelles

1.4 Contrôle de la mise en œuvre de la Convention 108 par les Etats contractants

Objectif : Doter le Comité Consultatif d'une compétence de contrôle de la mise en œuvre par les Etats membres de la Convention 108 et son Protocole additionnel, ainsi que, éventuellement, l'examen préalable du niveau de protection des données à caractère personnel des Etat candidats à l'adhésion à la Convention 108 et son Protocole Additionnel

Méthodes de travail : le Bureau du T-PD envisagera la création de plusieurs groupes de travail relatifs aux sujets retenus. Ces groupes de travail seront composés des membres du T-PD et des représentants des Etats contractants, des organisations et des Etats observateurs et seront coordonnés par un rapporteur (membre du T-PD). Les groupes doivent être constitués d'un nombre suffisant de membres pour pouvoir apporter l'expertise nécessaire sans toutefois compromettre l'efficacité du travail. La participation des experts peut être envisagée sous condition d'un financement suffisant. Les groupes travailleront par email. Les projets d'amendements ainsi rédigés feront l'objet d'une discussion lors des réunions du Bureau en présence des rapporteurs des groupes concernés. Le Secrétariat se chargera de la préparation du document final qui incorporerait des projets d'amendements et constituerait un projet du protocole additionnel.

Partenaire(s) : CRID, experts du CoE
Calendrier : le premier projet du protocole additionnel pourrait être présenté lors de la réunion plénière de 2012.
Ordre des priorités : supérieur

95 Activités menées en application de l'article 21 de la Convention 108

2. Révision des « anciennes » et rédaction de « nouvelles » Recommandations[96]

2.1 Recommandation N° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police

Objectif : le développement de nouveaux procédés automatisés, concepts et techniques utilisés pour le traitement des données à caractère personnel nécessaires pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière, ou l'exécution de sanctions pénales appellent à la mise à jour de la Recommandation (87) 15 ou à la rédaction d'un nouveau document juridiquement contraignant.

Méthodes de travail : le T-PD engagera une étude générale de la Recommandation (87)15 afin de déterminer les principes à approfondir pour couvrir de façon adéquate les nouvelles questions de protection des données dans le domaine de la prévention et de la détection des infractions pénales, des enquêtes et des poursuites en la matière, ou de l'exécution de sanctions pénales. L'utilisation d'un questionnaire adressé aux Etats contractants concernant la législation et pratiques internes peut être envisagée. Sur la base de l'information reçue le groupe de travail formé au sein du T-PD se chargera de la préparation du projet préliminaire présenté ensuite lors des réunions du Bureau et les réunions plénières. Après l'examen, si le T-PD l'estime nécessaire, la réglementation de l'utilisation de données à caractère personnel dans le secteur « police » pourrait faire l'objet d'un instrument juridiquement contraignant.

Partenaire(s) : experts du CoE, des autorités européennes de protection des données
Calendrier : 2 ans, le premier projet de la Recommandation pourrait être présenté pendant la réunion plénière de 2012
Ordre des priorités : supérieur

2.2 La Recommandation (89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi

Objectif : la mise à jour de la Recommandation (89) 2 à la lumière des développements technologiques et autres textes du Conseil de l'Europe contenant des dispositions sur le traitement de données dans le domaine de l'emploi

Méthodes de travail : le T-PD engagera une étude générale de la Recommandation (89) 2 afin de déterminer les principes à approfondir pour couvrir de façon adéquate les nouvelles questions de protection des données dans le domaine de l'emploi. L'utilisation d'un questionnaire adressé aux Etats contractants concernant la législation et pratiques internes peut être envisagée. Sur la base de l'information reçue le groupe de travail formé au sein du T-PD se chargera de la préparation du projet préliminaire présenté ensuite lors des réunions du Bureau et la réunion plénière.

Partenaire(s) : expert du CoE, le Secrétariat de la Chartre Sociale Européenne
Calendrier : 2 ans, le premier projet de la Recommandation pourrait être présenté pendant la réunion plénière de 2014
Ordre des priorités : supérieur

3. Autres travaux

3.1 Statut et compétences des autorités de contrôle de protection des données

Objectif : rédiger un document explicatif exposant un « modèle » de l'autorité de contrôle telle qu'elle ressort du Protocole additionnel

Méthodes de travail : dans un premier temps, le Bureau et le T-PD concevront et distribueront un questionnaire aux Etats contractants relatif à l'organisation et aux compétences des autorités de contrôle. Le Bureau se chargera

96 Les activités mentionnées sous ce chapitre nécessitent un mandat préalable au T-PD de la part du CDCJ.

ensuite de préparer un document de compilation en esquissant un modèle d'accompagnement à la mise en œuvre du Protocole additionnel.

Partenaire(s) :
Calendrier : travaux à poursuivre après que l'arrêt dans l'affaire C-518/07 de la Cour de justice des Communautés européennes soit rendu.

3.2 Le réseau social en ligne

Objectif : préparer une étude des instruments existants tendant à renforcer les droits des utilisateurs devant l'expansion du phénomène des réseaux sociaux en ligne

Méthodes de travail : Le T-PD, en collaboration avec les représentants du CDCJ, ainsi que du Comité directeur sur les médias et les nouveaux services de communication (CDMC) explorera des pistes de réflexion relatives aux méthodes de travail et au financement du projet de la recommandation.

Partenaire(s) : CDMC, experts du CoE
Ordre des priorités : secondaire

3.3 Droit fondamental à la protection des données

Objectif : engager une étude pour évaluer la nécessité et la valeur ajoutée d'un droit fondamental à la protection des données indépendant de l'article 8 de la CEDH

Partenaire : Comité directeur pour les Droits de l'Homme (CDDH)
Calendrier : travaux à poursuivre après l'entrée en vigueur du Traité de Lisbonne.

3.4 Avis sur la compatibilité avec les instruments de protection des données du Conseil de l'Europe

Objectif : le suivi constant des développements au sein et à l'extérieur du Conseil de l'Europe avec les instruments de protection des données du Conseil de l'Europe.

Méthodes de travail : le Secrétariat du T-PD se chargera de mettre constamment à jour les documents « Réalisation du Conseil de l'Europe dans le domaine de la protection des données » et « La jurisprudence de la Cour européenne des Droits de l'Homme relative à la protection des données à caractère personnel ».

Partenaire(s) : Secrétariat du T-PD
Ordre des priorités : à suivre régulièrement

3.5 Préparation de la célébration à l'occasion du 30ème anniversaire de la signature de la Convention 108

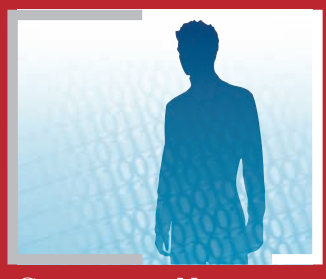
Objectif: recueillir les propositions en vue de l'organisation de la célébration transfrontalière du 30ème anniversaire de la signature de la Convention 108

Méthodes de travail : Le Bureau se chargera de préparer un questionnaire à soumettre aux Etats membres. La compilation des propositions, préparée par le Secrétariat, sera discutée pendant la réunion plénière en vue de l'adoption du plan commun d'action.

Calendrier: Questionnaire à approuver pendant la réunion du Bureau des 19-20 Novembre 2009, le plan commun d'action à discuter pendant la réunion plénière de 2010
Partenaire(s) : Secrétariat du T-PD
Ordre de priorité: à suivre régulièrement

Le 10 avril 2009, Monsieur le Ministre des Communications Jean-Louis Schiltz a procédé à l'assermentation de trois nouveaux juristes. MM. Michel Sinner, Georges Weiland et Christian Welter ont ainsi rejoint les rangs des fonctionnaires de l'Etat dans la carrière supérieure de l'attaché de direction.

Table ronde "Mesurer les diversitées" du 9 avril 2009 à l'Hôtel Royal avec avec le Président de la CNIL Alex Türk, des représentants du Commissariat aux Etrangers (aujourd'hui OLAI), du Centre de l'égalité de traitement et les responsables d'instituts statistiques et d'organismes de recherche dans le domaine social et de la population.



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