Commission Nationale
pour la Protection
des Données

Rapport annuel 2011

Commission Nationale
pour la Protection
des Données

Rapport annuel **2011**

Table des matières

Mission

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

Superviser et assurer la transparence par :

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

Informer et guider avec :

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

Conseiller et coopérer à travers :

- Les avis relatifs aux projets de loi et 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

Participations aux travaux européens

1 Avant-propos

Le collège :
Pierre WEIMERSKIRCH, Gérard LOMMEL, Thierry LALLEMANG

Les textes légaux en matière de protection des données au niveau de l'Union européenne, du Conseil de l'Europe, et de l'OCDE sont actuellement en cours de révision pour tenir compte de l'évolution technologique rapide et des effets de la mondialisation qui ont modifié en profondeur notre quotidien.

Madame Viviane Reding, Vice-présidente de la Commission européenne, chargée de la justice, des droits fondamentaux et de la citoyenneté, a dressé les grandes lignes de la réforme initiée au niveau communautaire dans un discours à Bruxelles le 16 mars: « *Alors que les sites de réseaux sociaux et les services de partages de photos ont apporté d'importants changements dans notre façon de vivre, les nouvelles technologies ont également suscité de nouveaux défis. Des outils sophistiqués permettent la*

Chiffres clés de la CNPD en 2011

- 14 avis formels
- 401 notifications reçues
- 653 demandes d'autorisation préalable
- 1831 demandes de renseignement
- 115 plaintes et demandes de vérification de licéité

collecte automatique de données et il est souvent difficile pour l'utilisateur de détecter quand ses données personnelles sont collectées. Après la collecte, ces données sont utilisées par les entreprises pour mieux cibler les individus ». Les entreprises privées ne sont pas les seules à être concernées: « *Les autorités publiques utilisent de plus en plus de données personnelles pour de nombreuses raisons, notamment la prévention et la lutte contre le terrorisme et les faits criminels graves* ».

La Commission européenne a préparé un projet de réforme ambitieux combinant le renforcement des droits et recours des individus avec une responsabilisation accrue des acteurs qui collectent et traitent davantage encore que par le passé des renseignements de plus en plus variés et détaillés sur les citoyens et consommateurs. Les moyens des autorités de contrôle dans les différents Etats membres doivent être renforcés à leur tour, afin d'assurer une réelle transparence et davantage de contrôle des personnes concernées sur l'utilisation de leurs données et, le cas échéant, de pouvoir sanctionner des violations ou abus.

Plusieurs exemples récents ont montré qu'un cadre légal mieux harmonisé et une protection plus efficiente étaient nécessaires pour faire face aux nouveaux défis.

Un exemple est l'atteinte majeure à la sécurité des bases de données de Sony, qui a compromis les comptes de 77 millions de consommateurs avec leurs noms, adresses de courrier électronique et adresses postales, dates de naissance, informations de connexion, mots de passe, historiques des achats et informations relatives aux cartes de crédit. Les utilisateurs ont été avertis beaucoup trop tard, près d'une semaine après le vol des données.

Un autre exemple concerne Google Street View. La découverte de la collecte des données privées sur les réseaux Wi-Fi non sécurisés a suscité des réactions énergiques, mais pas toujours similaires de la part des autorités de contrôle. Cette approche divergente d'une même situation démontre la nécessité de mettre en place une stratégie plus cohérente pour appréhender ce type de violations susceptibles de porter atteinte aux droits et protections des citoyens.

Nous pouvons encore évoquer la manière dont les géants de l'internet collectent les données à caractère personnel de leurs utilisateurs. Que ce soit pour une modification des paramètres de confidentialité ou pour l'introduction d'une nouvelle fonctionnalité, il ne se passe guère une semaine sans que des entreprises comme Facebook, Google ou Apple ne se trouvent au cœur de l'actualité relatée par les médias pour mettre en lumière des risques nouveaux au niveau de l'application des principes de la protection des données. Face à ces entreprises, les autorités de contrôle rencontrent souvent des difficultés à faire respecter certaines règles européennes, compte tenu de la globalisation.

La Commission nationale est ainsi confrontée à un énorme défi en termes de sensibilisation de la population et surtout des jeunes. En janvier, elle a organisé une conférence sur la protection de la vie privée sur Internet avec le Dr Alexander Dix (Commissaire à la protection des données

1 Avant-propos

et à l'accès à l'information du Land de Berlin) et le directeur européen de Facebook, Richard Allan. La conférence au Cercle Cité a connu un grand succès avec une salle comble. D'autres évènements et formations ponctuels ont contribué à informer un public plus spécialisé des enjeux de la protection des données.

Une nouvelle mission a été introduite par la loi du 28 juillet 2011, qui est entrée en vigueur le 1er septembre. Celle-ci oblige les fournisseurs de services de communications électroniques à notifier les failles de sécurité à la Commission nationale et d'en informer les personnes concernées.

Parmi les temps forts de l'année, citons encore la conclusion du partenariat de la Commission nationale avec le Centre Interdisciplinaire pour la Sécurité, la Fiabilité et la Confiance (SnT) de l'Université du Luxembourg. Le programme commun de recherche comporte trois principaux domaines d'analyse : les nouveaux développements de la législation européenne en matière de protection des données, les défis technologiques tels que le cloud computing et leurs répercussions pour les acteurs publics et privés du pays, ainsi que le concept de « privacy by design ».

La Commission nationale a également avisé un certain nombre de projets de loi et de mesures réglementaires, dont le projet de loi n°6284 visant la création et l'exploitation d'une nouvelle base de données à caractère personnel des élèves par le Ministère de l'Education nationale et de la Formation professionnelle qui a suscité de vives réactions dans l'opinion publique. Elle a poursuivi la concertation avec le Ministère de la Santé sur le dossier de soins partagé et le médecin référent. De plus, elle a accompagné les projets publics ayant un impact sur la vie privée des citoyens comme, par exemple, la réforme du casier judiciaire, l'introduction du nouveau titre de séjour biométrique, la vidéosurveillance dans les lieux publics et privés et l'initiative citoyenne européenne.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

2 Les activités en 2011

Le travail de la Commission nationale durant l'année 2011 était centré sur les activités suivantes :

- Le conseil et la guidance d'acteurs publics et privés ;
- La supervision de l'application de la loi ;
- L'information et la sensibilisation du public ;
- 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'État et les organismes publics

La Commission nationale a poursuivi et renforcé le dialogue avec les organisations représentatives sectorielles, les principaux acteurs économiques, l'Etat et les organismes publics. Lors de 140 réunions (69 avec le secteur public et 71 avec le secteur privé) elle a été consultée au sujet des aspects soulevant des questions de protection des données.

En 2011, elle était notamment en lien avec les ministères, administrations et organes publics suivants :

- Le Ministère de la Justice : réforme du casier judiciaire, procédure de dépôt de la liasse comptable auprès du gestionnaire du registre de commerce, coopération en matière d'obligations alimentaires ;
- La Direction de l'Immigration : introduction du nouveau titre de séjour biométrique ;
- Le Ministère de la Santé : mise en œuvre du plan national « e-santé » et projet médecin-référent ;
- Le Ministère des Transports : identification des menues embarcations, permis de conduire ;
- L'Inspection de la Police : caméras dans les cellules de détention ;
- Le Ministère des Affaires étrangères : cartes diplomatiques ; initiative citoyenne européenne ;
- La Ville de Luxembourg : projet AVTAX (avertissements taxés), destruction des formulaires de l'enquête logement, intégration d'un système de géolocalisation au système d'exploitation du réseau public d'autobus ;
- La Police judiciaire : vidéosurveillance de l'ambassade des Etats-Unis ;
- Le Médiateur du Grand-Duché de Luxembourg : caméras cellules de détention ;
- L'Université du Luxembourg : partenariat avec le Centre

Interdisciplinaire pour la Sécurité, la Fiabilité et la Confiance (SnT) ;
- Le Ministère de l'Enseignement Supérieur et de la Recherche : demande d'échange des données au sujet des aides financières ;
- Le Ministère de la Famille et de l'Intégration : surendettement ;
- L'Office luxembourgeois de l'Accueil et de l'Intégration (OLAI) : contrat d'accueil et d'intégration ;
- Le Ministère de l'Education nationale et de la Formation professionnelle : exploitation d'une base de données à caractère personnel relative aux élèves ;
- Le Ministère des Classes Moyennes : réglementation de l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales;
- Le Ministère de l'Economie et du Commerce Extérieur (Direction de l'Energie) : sécurité et confidentialité des données de consommation d'électricité et de gaz ;
- Le Ministère du Logement : statistiques annuelles sur les prix des terrains à bâtir.

Dans le domaine de la santé, la Commission nationale a collaboré avec de nombreux acteurs, dont le Comité National d'Ethique et de Recherche (CNER), le CRP-Santé, la Biobanque de Luxembourg (IBBL), le Collège médical, l'Association des Médecins et Médecins-Dentistes (AMMD), l'Entente des Hôpitaux (EHL), la Caisse Nationale de Santé (CNS) et le laboratoire d'analyses médicales Ketterthill.

Par ailleurs, la Commission nationale a rencontré des entreprises multinationales implantées au Luxembourg. Elle a notamment eu des entrevues avec iTunes (Apple) sur la collecte de données de localisation, le profilage des utilisateurs à travers les applications mobiles sur l'iPhone et l'iPad et l'utilisation de données à caractère personnel pour la publicité comportementale en ligne. Elle a été en contact régulier avec eBay/Paypal pour discuter de divers sujets, dont le partage de données entre eBay et Paypal ou le traitement des plaintes qu'elle a reçues concernant leurs services. Des échanges de vues ont encore eu lieu avec Google concernant le service « Street View » et avec les entreprises Amazon, Innova ou encore Microsoft.

La Commission nationale est aussi intervenue périodiquement dans les travaux de la Commission Consultative des Droits de l'Homme (CCDH) et du Comité National pour la Simplification Administrative en faveur des Entreprises (CNSAE).

2.1.2 Demandes de renseignements

La Commission nationale a reçu 1831 demandes de renseignements en 2011, dont 1634 par téléphone.

Plus de la moitié des demandes provenaient d'entreprises privées. Les autres requêtes émanaient d'administrations publiques (17%), d'avocats (14%) et de citoyens (12%).

Il s'agissait le plus souvent de questions sur les formalités à accomplir pour pouvoir mettre en œuvre un traitement de données ou de questions juridiques.

Le sujet le plus fréquemment abordé était la vidéosurveillance. D'autres questions concernaient les demandes de coopération des autorités de protection des données des autres pays, le domaine de la recherche et des études scientifiques, la surveillance informatique, le droit à l'image et les enregistrements téléphoniques.

2 Les activités en 2011

2.2 Supervision de l'application de la loi

2.2.1 Formalités préalables

Le législateur luxembourgeois prévoit que tout traitement de données à caractère personnel doit en principe être notifié à la Commission nationale. Cette obligation repose sur deux considérations principales: d'abord, le régime général de la déclaration préalable assure à la Commission nationale une vision des réalités sur le terrain; puis, le caractère public des déclarations, consultables sur le site web www.cnpd.lu, contribue à la transparence en offrant aux personnes concernées la possibilité de s'informer sur les caractéristiques de tel ou tel traitement. Le régime de la déclaration préalable constitue ainsi une sorte de corollaire à l'obligation des détenteurs de fichiers d'informer les personnes concernées sur le sort de leurs données.

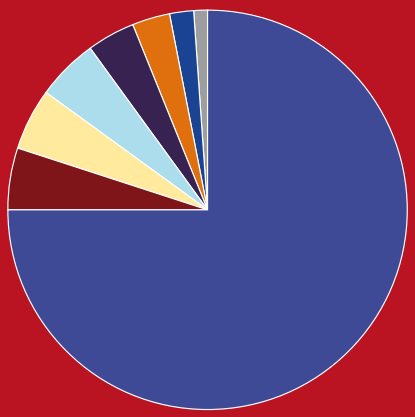
En 2007, de larges exceptions ont été introduites au devoir de notification pesant sur les responsables du traitement. D'abord, il exempte de déclaration les traitements les plus courants, comportant un risque négligeable pour la vie privée ou bien couverts par des garanties légales particulières en matière de protection des données.

En revanche, il demande des garanties supplémentaires pour certains traitements à caractère « sensible » dont la mise en œuvre requiert l'accord préalable de la CNPD (une simple déclaration n'étant donc pas suffisante). Parmi ces traitements, limitativement énumérés par la loi, figurent par exemple les systèmes de caméras vidéo, les surveillances au moyen d'appareils informatiques ou de télécommunications, les traitements de données génétiques dans le cadre de recherches, les géolocalisations de véhicules, les transferts de données hors Union européenne ou encore les contrôles d'accès par radiocommunication ou par procédés biométriques.

2.2.1.1 Déclarations préalables : les chiffres

En 2011, 401 traitements ont été notifiés à la Commission nationale, la moitié de ces notifications provenant d'acteurs du secteur financier et les traitements se plaçant le plus souvent dans le cadre de la gestion du personnel. De plus, la Commission nationale a reçu 653 demandes d'autorisation en 2011, dont la majorité concernait l'exploitation de caméras de surveillance, les transferts de données hors UE et, plus généralement, les surveillances sur le lieu de travail.

Catégories des demandes d'autorisation



De manière générale, on peut observer que le nombre des notifications va décroissant depuis quelques années, tandis que celui des demandes d'autorisations et des requêtes connexes demeure à un niveau constamment élevé.

2.2.1.2 Aspects de simplification administrative

Bien consciente de la lourdeur inhérente au régime de l'autorisation préalable, la Commission nationale met en œuvre certaines mesures visant à protéger la vie privée des personnes concernées, tout en tenant compte des efforts de simplification administrative du gouvernement. Ainsi, la CNPD s'éloigne des sentiers battus administratifs en favorisant les « chemins courts » et la simplicité lors de la communication avec les requérants, qu'elle ne considère point comme administrés, mais plutôt comme clients qu'elle doit s'efforcer d'aider et de satisfaire. Les collaborateurs de la CNPD sont toujours à l'écoute des différents acteurs impliqués dans la procédure d'autorisation et ils les assistent dans l'accomplissement des obligations légales en la matière. Ceci faisant, la CNPD ne met non seulement un accent particulier sur les nouvelles technologies de la communication et de l'information, mais également sur le contact direct et les visites sur place. D'un point de vue plus formel, la procédure allégée de l'autorisation unique, la mise à disposition de formulaires et de guides, et le nombre croissant de personnes agréées et encadrées en tant que chargés de la protection des données contribuent encore à réduire au mieux la charge administrative.

2.2.1.3 Les autorisations préalables

Les décisions de la CNPD visent à établir un juste équilibre entre les différents intérêts en jeu, à savoir d'un côté le droit des personnes concernées à jouir d'une vie privée intacte et de l'autre l'intérêt légitime que peut avoir l'exploitant à mettre en œuvre un traitement soumis à autorisation. Il ne s'agit donc nullement d'un « mécanisme d'estampillage » se bornant à distribuer des « cartes blanches », mais au contraire d'une mise en balance – parfois bien délicate – d'intérêts différents (et parfois divergents) selon des critères pertinents tels que nécessité, proportionnalité, loyauté et légitimité. Cette différenciation peut même se faire au sein d'un même traitement de données, de sorte que certains aspects du traitement sont admissibles, alors que d'autres ne sauraient pas être autorisés par la CNPD (sans que cela entraîne automatiquement un refus intégral pour le traitement en question).

A. Vidéosurveillance

La vidéosurveillance, qui connaît depuis quelques années un essor assez spectaculaire, est un moyen de traitement invasif dont les possibilités de

graduation sont a priori limitées. Ainsi, la surveillance d'un local commercial visant à détecter les vols aux étalages entraîne notamment que le personnel se retrouve souvent sur les images, même si la surveillance du personnel n'est pas la finalité poursuivie par l'exploitant. La CNPD considère donc que toute personne captée (que ce soit de manière intentionnelle ou incidente) est à considérer comme personne concernée. S'il faut néanmoins remarquer que les développements récents permettent p.ex. de déterminer avec précision le degré de détail des images ou de voiler certaines portions de l'image, il n'en reste pas moins que la seule présence de caméras peut déjà suffire à créer un climat de pression.

La CNPD prévoit des restrictions afin d'alléger le caractère intrusif des dispositifs de vidéosurveillance. Elle estime ainsi que les caméras ne doivent filmer que le strict nécessaire. La surveillance ne doit pas porter sur des terrains privés ou publics autres que ceux de l'exploitant. La surveillance des voies publiques est en principe considérée comme disproportionnée (même si des impératifs de configuration ou de sécurité peuvent, dans des cas tout à fait exceptionnels, entraîner l'autorisation pour le captage d'une bande restreinte de voie publique adjacente à l'enceinte).

À l'intérieur de l'enceinte filmée, l'exploitant n'est pas non plus « maître absolu » de sa vidéosurveillance dans la mesure où il s'agit de lieux accessibles au public (y inclus les membres du personnel). Ainsi la vidéosurveillance à l'intérieur d'un restaurant ou d'un café n'est-elle pas autorisée. Plus généralement, elle ne doit pas porter en outre sur des lieux à usage privé (toilettes, douches, vestiaires, cabines d'essayage,...).

La CNPD met par ailleurs un accent particulier sur la protection de la vie privée sur le lieu de travail. Les caméras ne doivent pas capter en permanence certains postes de travail. Un captage exceptionnel de postes de travail avec floutage d'images est admis lorsque les intérêts légitimes de l'exploitant, comme p.ex. des impératifs de sécurité, priment sur la vie privée (p.ex. guichets d'une banque, lieux de production industrielle de matières dangereuses,...). La vidéosurveillance ne doit pas servir en outre à contrôler les déplacements, comportements ou performances des membres du personnel.

La Commission nationale accorde encore une protection particulière aux personnes mineures pouvant se trouver dans le champ de vision des caméras. Elle n'approuve généralement pas la présence de caméras à l'intérieur

des écoles, qui sont susceptibles d'habituer les enfants à la vidéosurveillance dès leur plus jeune âge. Les vidéosurveillances dans les écoles et les lycées doivent dès lors rester limitées au strict nécessaire et ne peuvent, pour certaines zones, se faire qu'en temps réel.

La durée de conservation des images doit rester limitée au strict nécessaire (la Commission nationale impose à cet égard des délais assez restreints). Une importance particulière est attachée à l'information en bonne et due forme des personnes concernées, notamment par le biais de pancartes ou de pictogrammes, ceci nonobstant les droits dont disposent les individus en vertu des articles 26 et 28 de la loi modifiée du 2 août 2002. Les pictogrammes prémentionnés sont encore complétés par des vignettes délivrées par la CNPD comportant le numéro de la décision; ceci permet aux intéressés de se renseigner, dans le registre public consultable sous www.cnpd.lu, sur les caractéristiques principales de la vidéosurveillance en question.

B. Surveillance des outils informatiques

Il s'agit ici d'assurer la protection de la vie privée des usagers d'appareils électroniques ou informatiques. On peut considérer qu'une surveillance a lieu dès que le traitement vise principalement la personne et non pas la machine, p. ex. lorsque l'employeur s'intéresse de près aux sites Internet que visitent ses employés identifiés. Les champs d'action d'une telle surveillance sont toutefois strictement délimités par la loi.

De manière générale, la CNPD préconise une graduation de l'emploi des moyens de surveillance; une surveillance informatique devrait donc se faire en premier lieu de manière générale ou statistique; l'identification de la personne concernée ne devrait se faire que dans un deuxième stade où il s'agirait de déceler l'origine d'incidents concrets, sur base d'indices objectifs et spécifiques. L'enregistrement et la prise de connaissance de correspondances ne doivent pas porter sur des contenus à caractère personnel ou privé.

La consultation de contenus doit en principe se faire a posteriori, c'est-à-dire suite à un incident ou à un évènement rendant nécessaire l'accès à des informations spécifiques et bien déterminées. Une prise de connaissance généralisée et a priori (p.ex. pour déceler d'une manière générale la qualité des prestations des employés) est considérée comme disproportionnée.

Une importance particulière revient ici encore à l'information préalable du salarié, qui doit savoir à l'avance qu'une surveillance a lieu.

C. Contrôles de déplacements et d'accès

Un contrôle des déplacements peut être envisagé dans certains cas bien déterminés, p.ex. pour

Les activités en 2011

la coordination en temps réel des véhicules de service d'une entreprise (géolocalisation) ou encore pour la protection de certaines personnes vulnérables (p.ex. surveillance par radio-identification de nouveau-nés dans les maternités, afin d'éviter des kidnappings). L'exploitant peut encore être amené à vouloir contrôler les accès à son enceinte, par des procédés de radio-identification ou de biométrie. Il est toutefois bien entendu que de tels contrôles devront être accompagnés des garanties appropriées et que la personne concernée devra être parfaitement renseignée sur l'utilisation qui sera faite des données.

Les géolocalisations dans les véhicules professionnels sont limitées à des finalités considérées comme légitimes (p.ex. coordination de la flotte de véhicules, protection contre les vols, constitution de la preuve d'un travail exécuté en vue de la facturation au client). Le dispositif de géolocalisation doit pouvoir être désactivé lors d'un usage non professionnel du véhicule (dans la mesure où un tel usage est permis).

Pour la mise en œuvre d'une surveillance des nouveau-nés dans les maternités, l'accord préalable des ayants droit est obligatoire. De manière générale, l'usage d'une telle technologie ne peut être que complémentaire aux mesures de surveillance humaines déjà en place.

Quant aux contrôles des accès, une procédure d'autorisation allégée (autorisation unique) est en place pour les contrôles à radio-identification (badges). Ceci n'est pas le cas pour les systèmes biométriques qui restent soumis à la procédure d'autorisation ordinaire.

D. Etudes et recherches scientifiques

Les recherches comportant des données génétiques ou la réutilisation de données collectées auparavant doivent répondre à des critères très stricts. Les données ne doivent pas être collectées et utilisées de manière déloyale. La collecte doit se limiter au strict nécessaire, et l'anonymisation des données doit se faire au plus tôt et autant que possible.

La conservation des données doit en principe rester strictement limitée à la durée nécessaire pour mener à bien le projet de recherche; la constitution d'une banque de données « utiles » (p.ex. pour des recherches postérieures) peut uniquement avoir lieu si aucune identification directe ou indirecte n'est possible, une simple codification n'étant pas suffisante.

E. Transferts de données hors Union européenne

a) Autorisation en cas de transferts de données vers des pays tiers

Un organisme qui souhaite transférer des données à caractère personnel du Luxembourg vers un pays tiers n'assurant pas un niveau de protection adéquat au vu de sa législation sur la protection des données, doit demander une autorisation préalable de la Commission nationale. En 2011, elle a été saisie de 48 demandes de ce type.

Les deux tiers des autorisations accordées en 2011 reposaient sur des demandes d'entreprises du secteur financier. Le pays de destination des données était le plus souvent les Etats-Unis.

Ces transferts sont souvent opérés dans le cadre de l'externalisation du stockage, de l'hébergement et du support informatique (« outsourcing ») en ce qui concerne les ressources humaines, les clients, les fournisseurs, les relations publiques, le marketing ou la comptabilité.

Les pays de l'Espace économique européen (Union européenne, Islande, Liechtenstein et Norvège) ont transposé la directive 95/46/CE du 24 octobre 1995 en droit national et garantissent ainsi un même niveau élevé de protection des données. Le principe d'interdiction de transférer des informations de nature personnelle vers un destinataire établi hors de cette « sphère de sécurité » comporte trois exceptions :

- les personnes physiques et morales établies aux Etats-Unis ayant adhéré aux conditions des accords de la sphère de sécurité (« Safe Harbor ») conclus entre la Commission européenne et les autorités américaines et figurant sur la liste afférente tenue par la Federal Trade Commission ;

- les situations correspondant aux conditions énumérées à l'article 19 (1) de la loi modifiée du 2 août 2002 qui constituent des dérogations légales prévues également dans le texte de la directive (consentement de la personne concernée, nécessité pour l'exécution d'un contrat conclu dans l'intérêt de la personne concernée, intérêt public important…) ;

- les accords conventionnels passés entre les exportateurs et les destinataires des données ou autres mesures de protection qui constituent des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes concernées. Aux termes du paragraphe (3) de l'article 19 de la loi, il appartient à la Commission nationale de vérifier si les sauvegardes et garanties sont suffisantes, ces dernières pouvant résulter notamment de l'application des clauses contractuelles types approuvées par la Commission européenne.

b) Approbation de règles d'entreprise contraignantes

Les règles d'entreprise contraignantes (« Binding Corporate Rules ») représentent une alternative juridique intéressante pour les groupes de sociétés qui se voient amenés

2 Les activités en 2011

Avantages des « BCR » pour un groupe d'entreprises multinationales

- Conformité avec la directive 95/46/CE
- Limitation des obligations administratives pour chaque transfert
- Uniformisation des pratiques relatives à la protection des données au sein d'un groupe
- Guide interne en matière de protection des données personnelles
- Moyen plus flexible et adapté à la culture d'entreprise
- Possibilité de placer la protection des données au rang de « préoccupation éthique du groupe »

à transférer régulièrement des données à caractère personnel à partir de leurs sociétés établies sur le territoire de l'UE vers d'autres entités du groupe situées dans les pays tiers.

De telles règles ne sont pas expressément prévues par la directive 95/46/CE, mais elles se sont créées dans la pratique entre autorités chargées de la protection des données, avec le soutien du groupe de travail « Article 29 ». Elles peuvent constituer des garanties suffisantes exigées par la directive 95/46/CE pour exporter des données vers des pays hors UE n'assurant pas un niveau de protection adéquat, à condition qu'elles soient approuvées par les autorités de contrôle des Etats membres où le groupe est implanté. Avec la réforme de la protection des données au niveau européen qui est en cours actuellement, cet instrument va prendre encore de l'importance.

Les « chartes » ou « codes de conduite » doivent revêtir un caractère contraignant et doivent être respectés par l'ensemble des entités d'un groupe de sociétés ainsi que par leurs salariés.

L'année passée, le groupe sidérurgique mondial Arcelor Mittal a soumis pour analyse un projet de leur charte BCR à la Commission nationale. Celle-ci travaille de manière intensive sur le projet du groupe ayant

son siège social au Luxembourg et des entrevues ont déjà eu lieu pour préparer la procédure d'approbation.

2.2.1.4 Les chargés de la protection des données

En 2011, 10 personnes ont été désignées par un responsable du traitement pour accomplir le rôle de chargé de la protection des données. Cette fonction peut être occupée par un salarié du responsable du traitement ou une personne externe, physique ou morale. Parmi les 57 organismes ayant désigné un chargé depuis 2005, plus de 90% sont des entreprises du secteur privé.

Les motivations pour lesquelles les entreprises, associations et organismes publics désignent un chargé sont multiples. D'abord, le responsable du traitement est exempté de l'obligation de notifier ses traitements. Seuls les traitements soumis à autorisation continuent à faire l'objet de formalités.

De plus, le chargé dispose d'un pouvoir d'investigation et assure la surveillance du respect des dispositions légales par le responsable du traitement.

Pour devenir chargé de la protection des données, certaines conditions doivent être remplies. La Commission nationale n'accepte que la désignation de personnes avec les qualités visées à l'article 40 de la loi de 2002, et dont la fonction principale dans l'organisme n'engendre pas de conflits d'intérêts avec celle de chargé.

Avant de pouvoir être désigné par le responsable du traitement, le chargé doit recevoir l'agrément de la Commission nationale. Il doit également justifier de ses efforts de formation continue par la suite. Un chargé est tenu, par ailleurs, d'assurer de manière indépendante l'application des dispositions légales en la matière et de soumettre à la CNPD un registre des traitements effectués par le responsable du traitement.

2.2.2 Demandes de vérification de licéité et plaintes

En 2011, la Commission nationale a reçu 115 plaintes et demandes de vérification de licéité. Si un citoyen ne réussit pas à faire valoir ses droits auprès d'une administration, entreprise ou association, ou si une réclamation reste sans suite ou s'avère difficile, il peut s'adresser à la Commission nationale.

Les catégories les plus concernées par les plaintes en 2011 étaient : les demandes d'effacement ou de rectification de données non respectées, la vidéosurveillance, la transmission de données à des tiers, l'opposition à la prospection ou au SPAM ou le refus d'accéder aux données.

Plus de la moitié des dossiers ont été clôturés avec succès auprès du responsable visé et la CNPD a répondu directement au plaignant après analyse. Dans quelques cas, les plaignants se sont désistés ou voulaient juste s'informer. Dans d'autres cas, la plainte a été transmise à une autorité étrangère compétente.

Services en ligne

Au cours des deux dernières années, la Commission nationale a reçu un nombre croissant de plaintes concernant les services en ligne offerts par des grandes entreprises internationales.

Cela est dû au fait que ces entreprises ont choisi d'établir leur siège social européen au Luxembourg. La plupart des plaintes concernant ces services provenaient d'autres pays européens et avaient été transmises à la CNPD par des autorités étrangères de protection des données.

De nombreux utilisateurs se sont plaints du non-respect de leurs demandes d'effacement de données. D'une part, la Commission nationale a constaté régulièrement une inobservation des conditions générales ou des

Les activités en 2011

règles relatives à la protection des données de ces entreprises par les utilisateurs eux-mêmes.

D'autre part, certaines réponses données par ces entreprises étaient des lettres standard non personnalisées. Pour ces raisons, la clôture d'un compte et l'effacement des données pouvait parfois conduire à des procédures inutilement longues.

En conséquence, la Commission nationale a recommandé à ces entreprises de donner des réponses personnalisées à leurs clients. Certaines entreprises ont réagi en désignant un chargé de la protection des données qui est en contact direct avec la CNPD et qui garantit à chaque plaignant une analyse détaillée et une réponse personnalisée et motivée.

Dans le même sens, la CNPD s'est vu adresser des plaintes par des personnes rencontrant des difficultés lorsqu'elles voulaient supprimer leur compte auprès d'un service en ligne et toutes les données les concernant. Dans certains cas, cela n'était pas possible parce qu'il ne faut non seulement respecter la législation sur la protection des données, mais également celle sur les réglementations financières.

Pour chaque demande de fermeture d'un compte, ces sociétés seront ainsi obligées de vérifier l'identité du détenteur en lui demandant de transmettre des documents officiels, si la fermeture ne peut pas se faire en ligne.

De plus, pour être conforme aux lois et réglementations financières (p.ex. lois contre le financement du terrorisme, blanchiment d'argent, etc.), elles ne peuvent pas effacer immédiatement les données de transactions lors de la fermeture du compte, mais elles doivent archiver ces données pour des besoins de preuve et de conformité avec la législation sectorielle et les bonnes pratiques prônées par l'autorité de surveillance prudentielle.

La Commission nationale a également été contactée pour assister les utilisateurs de ces services lorsqu'ils ont rencontré des difficultés avec la gestion de leurs comptes, notamment concernant leur droit d'accès.

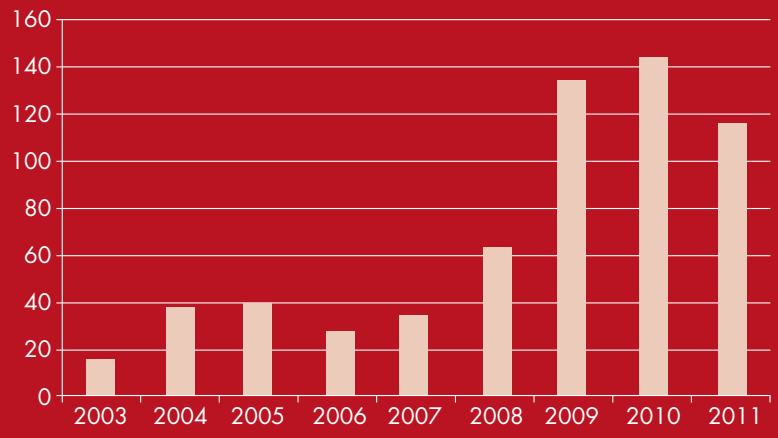
Autres exemples

Voici quelques exemples de traitement de plaintes, demandes et questions du public permettant d'illustrer l'action de la Commission nationale face aux difficultés rencontrées par les particuliers.

Opposition à des courriers non sollicités

Suite à son inscription à un concours organisé par une

Evolution du nombre de plaintes



société, Monsieur X a reçu des courriers électroniques publicitaires non sollicités et sans relation avec l'organisation du concours. Après avoir rencontré des difficultés pour faire supprimer son adresse électronique des fichiers de prospection commerciale de cette société, il a saisi la Commission nationale.

Les règles en droit luxembourgeois en matière de prospection par e-mail sont claires (article 11 paragraphe (2) de la loi modifiée du 30 mai 2005). L'abonné doit préalablement consentir à cette prospection (principe de l'« opt-in ») à moins que le fournisseur ait préalablement obtenu les données de son client dans le cadre d'une vente d'un produit ou d'un service. Même dans ce cas, l'abonné peut toujours et en tout état de cause s'opposer à toute sorte de prospection ultérieure (principe de l'« opt-out »).

Après l'intervention de la Commission nationale auprès de la société en question, celle-ci a respecté le droit d'opposition du plaignant en désinscrivant son adresse de courrier électronique de ses fichiers de prospection.

Dans un autre cas, en raison d'une publicité qu'il a reçue par voie postale de la société A, Monsieur Z a saisi la Commission nationale d'une plainte pour voir supprimer son adresse postale des fichiers de prospection commerciale de ladite société. La publicité envoyée au plaignant était une invitation à un évènement organisé conjointement par deux sociétés commerciales. Bien que le plaignant ait été en possession d'une carte de fidélité de la société B – co-organisatrice de l'évènement – il n'a jamais sollicité les services de l'autre.

Compte tenu des faits constatés, la Commission nationale a informé la société A que si la prospection par courrier postal ne nécessite pas le consentement préalable des personnes prospectées, l'article 30 paragraphe (1) lettre (b) de la loi modifiée du 2 août 2002 confère néanmoins aux personnes concernées le droit « de s'opposer, sur demande et gratuitement, au traitement la concernant envisagé par le responsable du traitement des données à des fins de prospection ».

Par ailleurs, il incombe au responsable du traitement de porter l'existence de ce droit à la connaissance de la personne concernée et d'informer celle-ci avant que les données la concernant ne soient utilisées pour la première fois à des fins de prospection.

Après l'intervention de la Commission nationale, la société A a confirmé la suppression définitive de l'adresse de Monsieur Z.

2 Les activités en 2011

Données collectées dans le cadre du recrutement

À la recherche d'un emploi, Monsieur Y a envoyé un dossier de candidature à une entreprise pour un poste vacant. Suite à une réponse négative, il a prié la société de bien vouloir effacer toutes les données le concernant.

Comme sa demande était restée sans réponse, il a saisi la Commission nationale. Etant donné que chaque personne dispose d'un droit d'accès, de rectification et, le cas échéant, de suppression de ses données personnelles en vertu de l'article 28 de la loi modifiée du 2 août 2002, la Commission nationale a demandé à la société de transmettre, dans les meilleurs délais, une réponse écrite au plaignant.

En effet, l'article 4 paragraphe (1) lettre (d) de la loi modifiée du 2 août 2002 oblige les responsables du traitement de s'assurer que les données qu'ils traitent soient « 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 ».

À cet égard, la Commission nationale a également demandé à ladite société de l'informer sur la durée de conservation des données personnelles contenues dans leurs dossiers de recrutements, et des pratiques mises en œuvre relatives à la suppression des données.

Suite à cette intervention de la Commission nationale, la société a confirmé que les données étaient bien effacées.

Usurpation d'identité et création d'un faux profil sur un réseau social

Madame Y a découvert qu'elle a été victime d'une usurpation d'identité sur un réseau social. En effet, quelqu'un avait créé un profil en utilisant des photos de la plaignante et en y ajoutant des informations personnelles et insultantes.

Une plainte auprès du réseau social étant restée sans suites, Madame Y a fait appel à la Commission nationale. Celle-ci a demandé au réseau social de lui communiquer le procédé appliqué lorsqu'une personne leur signale un abus de ses données à caractère personnel, et les mesures qu'ils envisagent de prendre afin de mieux se prémunir contre les cas d'usurpation à venir.

La Commission nationale a pu constater que quelques jours après la plainte, la page Internet affichant la photo de Madame Y avec un faux profil n'était plus en ligne. Etant donné que toute

usurpation d'identité constitue un délit pénal au sens de l'article 231 du Code pénal, ces faits ont également été signalés à la police afin de connaître le nom de l'usurpateur et de pouvoir le poursuivre en justice.

Publication de résultats scolaires en ligne

La Commission nationale a été saisie d'une demande de vérification de licéité quant à la publication de résultats scolaires en ligne, accessibles à tout le monde et qui mentionnaient non seulement les noms et prénoms d'élèves ayant été admis, mais également ceux des élèves ayant été ajournés.

Après intervention de la CNPD auprès du responsable du site Internet en question, celui-ci a déclaré ne plus procéder à un affichage de ces résultats en ligne.

Vidéosurveillance

La Commission nationale a constaté une légère hausse de plaintes concernant des caméras de surveillance installées par des particuliers dans leur domicile.

Elle aimerait rappeler à ce sujet que même si la loi nationale sur la protection des données ne s'applique pas à un traitement mis en œuvre par une personne physique « dans le cadre exclusif de ses activités personnelles et domestiques », le champ de vision des caméras privées ne doit en aucun cas capter la voie publique, ni les abords, entrées, accès et intérieurs d'autres maisons ou immeubles avoisinants.

2.2.3 Contrôles et investigations

Pour accomplir sa mission de contrôle, la Commission nationale peut procéder à des investigations en vue de vérifier le respect des obligations légales.

Ces investigations :
- sont liées à un dossier de plainte ou de vérification ponctuelle de licéité ;
- ou bien elles se font sur initiative de la Commission nationale menée à des fins dissuasives et pédagogiques.

La Commission nationale a effectué plusieurs visites de lieux pour vérifier la licéité de systèmes de vidéosurveillance. La loi modifiée du 2 août 2002 lui attribue ce pouvoir d'investigation, grâce auquel elle dispose d'un accès direct aux locaux (autres que les locaux d'habitation) où a lieu le traitement ainsi qu'aux données faisant l'objet du traitement.

En général, elle se concentre tous les deux ans sur une investigation de taille, dans un domaine qui donne lieu à des traitements de données d'envergure ou particulièrement sensibles. Les années précédentes, elle avait mené ce type d'investigations, dans le secteur des télécommunications.

Depuis 2011, elle intervient également lorsqu'apparaissent des failles de sécurité dans le secteur des communications électroniques, notamment pour garantir la confidentialité des utilisateurs (Voir point 3.3.1. pour plus d'informations à ce sujet).

À la fin de l'année, la presse internationale avait fait état d'inquiétudes concernant la collecte et la transmission de données sur certains smartphones. Un logiciel spécial développé par la société Carrier IQ, fournissant aux opérateurs des informations sur la manière dont les propriétaires utilisent leur téléphone portable, avait été particulièrement mis en cause.

La Commission nationale est immédiatement intervenue auprès des opérateurs de téléphonie mobile nationaux pour savoir si cette application était installée sur des portables commercialisés au Luxembourg.

2 Les activités en 2011

2.3 Information du public

2.3.1 Actions de sensibilisation du public

Dans le cadre de la Journée européenne de la protection des données et du 30e anniversaire de la Convention du Conseil de l'Europe sur la protection des données, la Commission nationale a organisé une conférence avec le commissaire à la protection des données et à l'accès à l'information du Land de Berlin, le Dr Alexander Dix, intitulée « Y a-t-il encore une vie privée sur Internet ? ». Cette conférence, à laquelle participait également le porte-parole européen de Facebook, Richard Allan, était suivie d'une table ronde avec des représentants du monde politique et de la protection de la jeunesse (Voir point 3.4. pour plus d'informations à ce sujet).

La Commission nationale a également participé au Safer Internet Day célébré à travers de nombreuses initiatives ayant pour but de promouvoir une utilisation plus sûre et plus responsable de l'Internet fixe et mobile par les jeunes. La 8e édition de cette journée s'est déroulée le 8 février 2011, elle est organisée chaque année par la Commission européenne dans plus de 60 pays. Au Luxembourg, BEE SECURE est l'interlocuteur du réseau Insafe. Le thème de la journée était l'importance du rôle des pratiques virtuelles dans la vie des enfants et des adolescents que ce soit dans les mondes virtuels et dans les jeux vidéo en ligne ou sur les réseaux sociaux.

La brochure avec des conseils sur la protection des données intitulée « Voici comment sécuriser tes données sur Internet », qui a été réalisée dans le cadre du projet BEE SECURE avec le soutien de la Commission nationale, a été rééditée cette année dans un format plus maniable.

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

La Commission nationale est apparue régulièrement dans les médias à propos de sujets très variés. Plus de 30 interviews ont généré 101 citations de la CNPD dans la presse.

Les interviews ont porté sur des sujets différents, dont la conférence « Y a-t-il encore une vie privée sur Internet ? » organisée par la CNPD en janvier, le recensement général de la population, la base de données relative aux élèves, la collecte de données de localisation par Apple, le programme « Origin » du jeu vidéo « Battlefield 3 » d'Electronic Arts, le dossier de soins partagé, Google Street View et Facebook.

Le site Internet de la Commission nationale : www.cnpd.lu

Parmi les thèmes traités par les médias dans le domaine de la protection des données et de la vie privée, citons les suivants : la surveillance de l'ambassade des Etats-Unis au Luxembourg, la vidéosurveillance dans les lieux publics, le vol de données dans le Sony Playstation Store, l'installation du logiciel Carrier IQ sur les smartphones et la réaction de la CNPD suite à un article sur le site Internet de RTL sur les groupes Facebook.

2.3.3 Outil de communication : le site Internet

Le site web de la Commission nationale est un vecteur de communication privilégié destiné aussi bien au grand public qu'aux responsables du traitement.

Pour le grand public, le site constitue une source privilégiée d'informations concernant les sujets qui ont dominé l'actualité dans le domaine de la protection des données et de la vie privée. Il offre aussi une information de base sur la protection des données et sur les droits et obligations des citoyens en la matière. Les internautes intéressés peuvent élargir leurs connaissances par la consultation de dossiers thématiques.

Pour les responsables du traitement, le site constitue une plate-forme interactive pour l'accomplissement en ligne des formalités prescrites par la Loi. En 2011, 43% des notifications ont été envoyées sous forme électronique.

Le grand public et les responsables du traitement peuvent encore utiliser le site pour consulter le registre public des traitements et contacter la Commission nationale pour toute question et demande de renseignement.

2.3.4 Formations et conférences

En 2011, les membres de la Commission nationale ont tenu 15 conférences, séminaires, formations ou ateliers. Ces évènements représentent une alternative à la presse ou au site Internet pour informer un public plus spécialisé des enjeux de la protection des données.

Le Président de la Commission nationale, Monsieur Gérard Lommel, a participé à la conférence « La protection des données personnelles : défis, enjeux et limites », organisée par la Chambre de Commerce dans le cadre de ses activités d'« Enterprise Europe Network-Luxembourg ». L'objectif de cette conférence était de sensibiliser le public, et d'accroître la vigilance des entreprises en matière de traitement des données personnelles face à l'utilisation accrue des nouvelles technologies

Les activités en 2011

de communication électronique. La présentation de M. Lommel portait sur l'établissement d'une bonne gouvernance au sein de l'entreprise et la mise en pratique du principe d' « accountability ». Les exposés de Gérard Lommel et Nicolas Dubois (Administrateur, Direction Générale Justice, Unité protection des données, Commission européenne) étaient suivis de témoignages des entreprises eBay Inc. (M. Steve Kenny, Head EU Privacy) et Microsoft Europe (M. Thierry Frommes, General Manager, Microsoft Luxembourg), ainsi que d'un exposé de Me Elisabeth Guissart (Associé, Cabinet Allen & Overy) sur la responsabilité des entreprises.

La conférence s'est achevée par deux ateliers de travail sur les nouveaux défis du secteur financier et la sécurisation des données.

La 6e journée des Juristes Européens a eu lieu du 18 au 20 mai 2011 à Luxembourg. Gérard Lommel a participé à une table ronde sur la protection des données à caractère personnel avec M. Jean-Claude Bonichot (Juge, Cour de justice de l'Union européenne, Luxembourg), Prof. Paul de Hert (Université Libre de Bruxelles, Belgique), Dr Thomas Petri (Contrôleur bavarois de la protection des données, Allemagne), M. Reinhard Priebe (Directeur, DG Affaires Intérieures, Commission européenne, Bruxelles) et Mme Isabelle Falque-Pierrotin (Présidente de la Commission nationale de l'informatique et des libertés, France). L'accord entre les Etats-Unis et l'Union européenne sur les principes de protection des données dans le domaine du droit pénal et de la coopération policière, ainsi que la directive sur la conservation des données de télécommunications du point de vue du droit constitutionnel ont fait partie des sujets traités.

Le 12 octobre 2011, Deloitte et l'Entente des Hôpitaux Luxembourgeois (EHL) ont organisé une journée d'échange sur les modifications dans le système des soins de santé suite à la réforme. Gérard Lommel a donné une présentation intitulée: « Qui a accès à nos données médicales ? Les données des patients seront-elles suffisamment protégées ? Quels droits et quelles restrictions et garanties un cadre légal doit-il prévoir ? ». Suite aux exposés des différents intervenants, une table ronde a eu lieu avec des médecins, des représentants de l'EHL et de la CNPD.

Messieurs Pierre Weimerskirch et Thierry Lallemang, membres effectifs de la CNPD, ont tenu une journée de formation sur le sujet « La protection de la vie privée et des données sur le lieu de travail » pour les

Gérard LOMMEL à la conférence « La protection des données personnelles : défis, enjeux et limites »

délégués du LCGB-SESF le 4 mai 2011. La présentation a plus particulièrement porté sur la cybersurveillance sur le lieu de travail, l'enregistrement des conversations téléphoniques, la vidéosurveillance, la biométrie et le rôle de la représentation du personnel.

Le 7 février 2011, Monsieur Pierre Weimerskirch a tenu un cours de formation au Lycée Technique de Bonnevoie (LTB). Les classes avaient préalablement préparé un recueil de questions au sujet de la protection des données personnelles touchant les domaines les plus variés: caméras de surveillance, réseaux sociaux, Google Street View, droits et devoirs de la police, commerce en ligne, publication de photos sur Internet, etc.

Plusieurs cours de formation ont également été destinés à l'Institut National d'Administration Publique (INAP) et à l'Institut National des Langues.

Outre les exposés précités, la Commission nationale a aussi fait des présentations au Rotary Club Luxembourg-Kiem et au Lions Club Fort Vauban sur la protection des données à caractère personnel sur Internet et sur l'éducation aux médias.

2 Les activités en 2011

2.4 Avis et recommandations

En 2011, la Commission nationale a émis 14 avis dans le cadre de projets de loi ou de règlements grand-ducaux :

1. Avis relatif au projet de loi n°5949 concernant les registres communaux des personnes physiques (Délibération n°11/2011 du 14 février 2011)
2. Avis relatif au projet de règlement grand-ducal modifiant :

   1. le règlement grand-ducal modifié du 5 septembre 2008 portant exécution de certaines dispositions relatives aux formalités administratives prévues par la loi du 29 août 2008 sur la libre circulation des personnes et l'immigration ;

   2. le règlement grand-ducal du 26 septembre 2008 portant création des traitements de données à caractère personnel nécessaires à l'exécution de la loi du 29 août 2008 sur la libre circulation des personnes et l'immigration et déterminant les données à caractère personnel auxquelles le ministre ayant l'immigration dans ses attributions peut accéder aux fins d'effectuer les contrôles prévus par la loi (Délibération n°124/2011 du 12 avril 2011)
3. Avis relatif à l'article 32 du projet de loi n°6158 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales (Délibération n°125/2011 du 15 avril 2011)
4. Avis concernant l'avant-projet de loi portant sur l'exploitation d'une base de données à caractère personnel relative aux élèves et à l'avant-projet de règlement grand-ducal pris en exécution de la loi du … portant sur l'exploitation d'une base de données à caractère personnel relative aux élèves (Délibération n°126/2011 du 15 avril 2011)
5. Avis concernant le projet de règlement grand-ducal fixant les conditions d'application et modalités d'exécution relatives au contrat d'accueil et d'intégration (Délibération n°145/2011 du 6 mai 2011)
6. Avis concernant l'avant-projet de règlement grand-ducal déterminant la procédure de dépôt de la liasse comptable auprès du gestionnaire du registre de commerce et des sociétés, les conditions de contrôles arithmétiques

et logiques concernant les comptes annuels et portant modification du règlement grand-ducal modifié du 23 février 2003 portant exécution de la loi du 19 décembre 2002 concernant le registre de commerce et des sociétés ainsi que la comptabilité et les comptes annuels des entreprises (Délibération n°158/2011 du 3 juin 2011)

7. Avis relatif au projet de loi no 6237 relatif à la mise en application du Règlement (CE) no 4/2009 du 18 décembre 2008 relatif à la compétence, la loi applicable, la reconnaissance et l'exécution des décisions et la coopération en matière d'obligations alimentaires et modifiant : a) le Nouveau Code de procédure civile et b) la loi modifiée du 10 août 1991 sur la profession d'avocat (Délibération n°159/2011 du 10 juin 2011)
8. Avis complémentaire concernant le projet de règlement grand-ducal fixant les conditions d'application et modalités d'exécution relatives au contrat d'accueil et d'intégration (Délibération n°160/2011 du 10 juin 2011)
9. Avis concernant le projet de règlement grand-ducal portant exécution de l'article 3 de la loi du 3 août 2011 relative à la mise en application du Règlement (CE) no 4/2009 du 18 décembre 2008 relatif à la compétence, la loi applicable, la reconnaissance et l'exécution des décisions et la coopération en matière d'obligations alimentaires, modifiant le nouveau Code de procédure civile (Délibération n°161/2011 du 17 juin 2011)
10. Avis relatif au projet de loi n°6021 sur le surendettement et modifiant certaines dispositions légales (Délibération n°168/2011 du 17 juin 2011)
11. Avis concernant l'avant-projet de règlement grand-ducal modifiant le règlement grand-ducal du 17 février 1987 sur l'identification des menues embarcations (Délibération n°181/2011 du 1er juillet 2011)
12. Avis au sujet d'une demande d'échanges de données relatives aux enfants de fonctionnaires du Parlement européen soumise par cette institution communautaire au Ministère de l'Enseignement Supérieur et de la Recherche (Délibération n°270/2011 du 3 août 2011)
13. Avis concernant l'avant-projet de loi relatif aux droits et obligations du patient et aux droits et obligations correspondants du professionnel de la santé, relatif à la médiation dans le domaine de la santé et portant modification de la loi du 28 août 1998 sur les établissements hospitaliers (Délibération n°357/2011 du 28 octobre 2011)
14. Avis concernant le projet de loi n°6325 relatif à la mise en application du règlement (UE) No 211/2011 du Parlement européen et du Conseil du 16 février 2001 relatif à l'initiative citoyenne (Délibération n°378/2011 du 11 novembre 2011)

2.5 Participation aux travaux européens

La Commission nationale, représentée par un ou plusieurs de ses membres, a participé en 2011 à 37 réunions et à différents groupes de travail au niveau européen.

Il s'agit notamment :

- du groupe de travail « Article 29 » (établi en vertu de l'article 29 de la directive 95/46/CE), qui regroupe toutes les

Les activités en 2011

autorités 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 » ;
- « Health Data » ;
- « Règles d'entreprise contraignantes » ;
- « Financial Matters » ;
- « Biometrics and E-government »;
- « Future of Privacy »
- « Key provisions of directive 95/46/CE ».

- du Comité consultatif de la Convention 108 du Conseil de l'Europe (T-PD) ;
- du « Groupe de Berlin », dédié à la protection des données dans le secteur des communications électroniques ;
- du séminaire européen d'échanges d'expériences dans le traitement des cas pratiques (« Case Handling Workshop »).

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.

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 (ci-après le groupe « Article 29 » ou « G29 »), est un organe consultatif indépendant. Son objectif est d'examiner les questions relatives à la protection des données et de promouvoir une application harmonisée de la directive dans les 27 États membres de l'Union européenne.

Parmi les sujets traités par le groupe de travail en 2011, citons : les puces RFID, la géolocalisation, l'accord TFTP et la lutte contre le financement du terrorisme, les données des dossiers passagers, la publicité comportementale en ligne, la définition du consentement et les compteurs intelligents.

2.5.1.1 Puces RFID : signature d'un accord destiné à protéger la vie privée des consommateurs

Le mercredi 6 avril 2011, la Commission européenne a annoncé la signature d'un accord avec l'industrie pour protéger la vie privée des consommateurs lors de l'usage de puces RFID (systèmes d'identification par radiofréquence) au sein de l'Union européenne. Cet accord volontaire vise à étudier les effets de l'utilisation des puces intelligentes sur la vie privée des citoyens avant leur mise sur le marché. Des représentants de la société civile, l'ENISA (Agence européenne chargée de la sécurité des réseaux et

Les puces RFID, qu'est-ce que c'est ?

Les tags RFID (Radio Frequency Identification) sont des petites puces à radiofréquence grosses comme une tête d'épingle et de plus en plus répandues. Intégrées dans des étiquettes « intelligentes », elles sont utilisées pour reconnaître ou identifier à plus ou moins grande distance et dans un laps de temps très court, un objet, un animal ou une personne. Ces puces quasiment invisibles sont capables de lire et de stocker des informations uniquement par transmission d'ondes radio sans nécessiter un contact physique. Contrairement aux codes-barres, les tags RFID ne nécessitent pas de contact physique pour que l'identification s'opère.

de l'information) ainsi que des organes européens de surveillance du respect de la vie privée et de la protection des données figurent également parmi les signataires.

Les domaines dans lesquels les puces intelligentes sont utilisées sont en constante évolution. Elles sont installées sur les cartes d'abonnement pour le bus ou au péage pour éviter l'arrêt des voitures lors de leur passage.

Dans le domaine logistique, elles sont utilisées pour gérer les marchandises. En outre, elles peuvent servir à localiser des personnes en cas d'urgence, tracer des livres dans les librairies et les bibliothèques ou identifier des animaux domestiques ou sauvages (marqueur posé en sous-cutané). Même les implantations sous la peau humaine sont possibles, comme cela a déjà été effectué sur des clients de discothèques pour le paiement des consommations.

Selon les chiffres de la Commission européenne, environ 2,8 milliards de puces ont été vendues en 2011, dont environ un tiers en Europe. Selon l'industrie, ce nombre pourrait augmenter jusqu'à 50 milliards d'ici 2020. Ces dispositifs microélectroniques peuvent être intégrés dans un grand nombre d'objets de la vie courante et nous faciliter la vie à bien des égards, mais ils peuvent également représenter un risque potentiel pour la vie privée.

Ainsi, la Commission note qu'« il devient possible pour un tiers d'accéder à vos données personnelles (concernant votre localisation par exemple) sans votre permission ».

Avec ce texte intitulé « Privacy and Data Protection Impact Assessment Framework for RFID Applications », la Commission européenne cherche à anticiper les risques pour la protection des données et de la vie privée.

En vertu de l'accord, les entreprises effectueront une évaluation complète des risques et prendront les mesures nécessaires pour y remédier avant qu'une nouvelle application RFID ne soit mise sur le marché. Pour la première fois en Europe, une méthode claire et exhaustive d'évaluation des risques, pouvant être appliquée dans tous les secteurs industriels utilisant des puces, a été établie.

L'absence d'une telle méthodologie avait amené le groupe de travail « Article 29 » à rejeter la proposition de cadre en 2010 (WP 175) avant de l'approuver dans son avis du 11 février 2011 (WP 180).

Pour Neelie Kroes, vice-présidente de la Commission européenne, chargée de la stratégie numérique, cet accord constitue également « *un bon exemple de réponse pratique aux questions de respect de la vie privée en Europe pour d'autres industries et technologies* ».

2 Les activités en 2011

2.5.1.2 *Géolocalisation des dispositifs mobiles intelligents*

Dans son avis 13/2011 relatif aux services de géolocalisation sur les téléphones et autres appareils mobiles, le groupe « Article 29 » a affirmé que les données de localisation sont des informations personnelles et qu'elles doivent être protégées en conséquence. De plus, il a clarifié le cadre légal applicable à ces services disponibles sur les « smartphones » et générés par ceux-ci.

Un nombre croissant d'appareils portables (smartphones, tablettes tactiles, etc.) permettent de localiser leur utilisateur. Une telle fonction peut présenter de nombreux avantages. Ainsi, elle permet à l'usager de s'orienter dans une ville inconnue, de découvrir un nouveau restaurant, d'avoir des informations sur la météo ou encore d'indiquer à ses « amis » où il se trouve à travers des services en ligne comme Facebook ou Foursquare. Mais ces services de géolocalisation permettent aussi d'espionner une personne à son insu en la suivant à la trace, ou de dresser un profil à partir de ses déplacements, notamment à des fins publicitaires.

Les risques sont nombreux, comme l'ont montré les polémiques autour d'Apple (iOs) et de Google (Android). Début 2011, une étude avait révélé que l'iPhone et l'iPad

conservaient un fichier collectant des données de géolocalisation. Ces informations non cryptées étaient stockées dans la mémoire du téléphone et transférées sur l'ordinateur lors de chaque synchronisation. Apple avait expliqué que ce n'était pas à proprement parler la localisation de l'iPhone qui était stockée, mais une base de données sur les points d'accès Wifi et les tours de téléphonie mobile autour du lieu où le détenteur du mobile se trouve.

Suite à cette étude, la société américaine Google avait à son tour confirmé qu'elle stockait des informations de localisation à travers les smartphones sous Android. Elle a justifié l'usage de ces données en expliquant qu'elles sont indispensables à certaines de ses applications de cartographie et de recherche, tout en soulignant que ces services étaient optionnels.

Dans son avis, le G29 a estimé que les services de localisation devaient être désactivés par défaut. C'est à l'utilisateur de décider quand il veut activer ces services en donnant son autorisation préalable à l'usage des données enregistrées. En pratique, ce consentement est souvent caché dans les conditions générales d'utilisation. C'est la raison pour laquelle le groupe de travail a insisté sur le caractère « spécifique » du consentement et sur une information transparente de la personne concernée sur l'utilisation de ses données. De plus, cette autorisation devrait être renouvelable au moins une fois par an et facile à annuler. Enfin, les données stockées devraient être effacées après une période donnée.

2.5.1.3 L'accord « TFTP » et la lutte contre le financement du terrorisme

Le « Terrorist Finance Tracking Program » (ci-après TFTP), plus communément appelé accord « SWIFT », permet aux autorités américaines d'accéder aux données financières européennes stockées sur le réseau de la société SWIFT.

Le TFTP américain est le résultat des négociations entre l'Union européenne et les autorités américaines pour trouver une solution juridique concernant l'échange de données à caractère personnel dans le cadre de la lutte contre le financement du terrorisme. Ses répercussions sur les droits fondamentaux des citoyens ont suscité de sérieuses préoccupations.

Celles-ci proviennent essentiellement du fait que l'application de l'accord TFTP UE-USA entraîne la communication d'importants volumes de données à caractère personnel (« transfert de données en masse ») aux autorités américaines, dont la grande majorité concerne des citoyens qui n'ont aucun rapport avec le terrorisme ou son financement.

Inspection de l'autorité commune de contrôle d'Europol

Depuis l'adoption de cet accord en août 2010, l'autorité commune de contrôle d'Europol (ci-après ACC) a la tâche de contrôler si Europol respecte les dispositions de l'accord lorsqu'il est décidé de la recevabilité des demandes des États-Unis pour l'accès à SWIFT. Selon l'accord, Europol doit vérifier à chaque requête américaine si le transfert de données est nécessaire, et doit donc approuver ou rejeter ce transfert de données vers les États-Unis.

En mars 2011, l'ACC a fait sa première inspection auprès d'Europol concernant l'accord et a critiqué le manque de respect des standards européens de protection des données personnelles. Le rapport a montré que les demandes des Etats-Unis étaient souvent abstraites et pas assez spécifiques pour permettre à Europol de prendre une décision sur le transfert des données. Cela n'a pourtant pas empêché Europol d'accepter toutes les requêtes.

Le G29 a critiqué la manière dont l'accord TFTP a été mis en œuvre

En juin 2011, les commissaires européens à la protection des données ont adressé une lettre commune au Département du Trésor des Etats-Unis, dans laquelle ils réclamaient une

meilleure prise en compte des principes de la protection des données dans la mise en œuvre de l'accord TFTP. La lettre contenait un catalogue de dix points avec des questions, qui s'étaient posées en pratique et qui avaient rendu difficile le respect des droits des personnes concernées jusqu'à ce moment-là.

Le chargé allemand de la protection des données, Monsieur Peter Schaar, a déclaré qu'il n'était toujours pas garanti que chaque citoyen européen était informé sans délai lorsque les autorités américaines avaient accédé à ses données, et sous quelles conditions cela avait eu lieu. Conjointement avec les autorités de protection des données européennes, il voulait s'assurer que les droits contenus dans l'accord SWIFT, notamment les droits d'accès et de rectification, ainsi que l'effacement ou le blocage de données incorrectes, étaient respectés.

Vers un « Terrorist Finance Tracking System » européen ?

En septembre 2011, le G29 a réagi par une lettre à la communication (COM (2011)429) de la Commission européenne sur les options envisageables pour la création d'un système européen de surveillance du financement du terrorisme. Il était prévu que le « Terrorist Finance Tracking System » (ci-après TFTS) serait l'équivalent européen du TFTP américain.

Le groupe « Article 29 » n'est toujours pas convaincu que l'adoption d'un TFTS européen soit nécessaire et proportionnée à la menace existante. Les problématiques des transferts de données en masse, des types de données traitées et partagées, du temps de rétention et des droits des personnes concernées étaient également soulevées dans la lettre.

Enfin, le G29 a formulé 44 recommandations concernant la protection de la vie privée et des données dans le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme dans son avis 14/2011.

2.5.1.4 Les données des dossiers passagers

Dans son avis 10/2011, le groupe « Article 29 » a critiqué la nouvelle proposition de la Commission européenne visant à imposer aux transporteurs aériens de fournir aux États membres de l'Union les données des dossiers passagers (« Passenger Name Record » ou « PNR ») de vols à destination ou en provenance du territoire de l'Union européenne, afin de lutter contre les infractions graves et le terrorisme. Il a cependant constaté des

améliorations relatives à la protection des données par rapport à la proposition de 2007.

Ce groupe de travail a noté que la nécessité d'un système PNR propre à l'UE n'a pas encore été établie et que les autres mesures proposées ne sont pas conformes au principe de proportionnalité.

En effet, ce système envisage la collecte et la conservation de l'ensemble des données de tous les voyageurs sur la totalité des vols. La collecte et le traitement des données PNR aux fins de lutte contre le terrorisme et les formes graves de criminalité ne devraient pas permettre de surveiller l'ensemble des voyageurs sans distinction.

Le G29 a également de sérieux doutes sur la proportionnalité de la mise en concordance systématique des données de l'ensemble des passagers avec des critères préétablis.

De plus, les catégories de données sont les mêmes que les dix-neuf éléments d'information figurant dans les accords PNR conclus entre l'UE et les Etats-Unis et entre l'UE et le Canada. Concernant celles-ci, le G29 maintient sa position selon laquelle aucun élément de preuve satisfaisant ne permet de connaître les données qui se sont avérées nécessaires, de sorte qu'une telle liste est disproportionnée.

Bien que la durée de conservation ait été clairement réduite par rapport à la proposition précédente, le groupe de travail est d'avis qu'il n'a pas été démontré de manière suffisamment convaincante que les données de l'ensemble des voyageurs doivent être conservées pendant cinq ans.

Accords PNR entre la Commission européenne et des pays tiers

Parallèlement au système PNR européen, la Commission européenne a également renégocié les accords PNR avec l'Australie, le Canada et les Etats-Unis en 2011.

La résistance du Parlement européen contre l'enregistrement de données concernant les passagers aériens s'était intensifiée en 2011. Selon les parlementaires, la Commission européenne n'a pas pu prouver la nécessité d'une conservation à grande échelle de ces données pendant une durée atteignant 15 ans.

Les députés ont encore critiqué que des standards différents soient appliqués aux accords PNR avec des pays tels que les Etats-Unis, le Canada ou l'Australie. Un autre point de critique était le fait que les PNR ne contenaient non seulement des données d'identification (noms et adresses des passagers), mais également des informations telles que le numéro de la carte de crédit, l'adresse IP ou certaines préférences des passagers, par exemple les types de repas préférés (végétariens, kasher, etc.).

Nouvel accord PNR entre la Commission européenne et les Etats-Unis

Après de longues négociations, la Commission européenne et les Etats-Unis ont pu trouver un accord, en novembre 2011, concernant l'échange de données des dossiers passagers.

Selon Cecilia Malmström, commissaire européenne en charge des Affaires intérieures, le projet d'accord contient quelques améliorations en matière de protection des données par rapport à celui signé en 2007:

- les données doivent être anonymisées au bout de 6 mois;
- la durée de conservation est passée de 15 à 10 ans;
- les compagnies d'aviation transmettent désormais les données aux autorités américaines (auparavant, celles-ci pouvaient accéder elles-mêmes aux ordinateurs des compagnies d'aviation);
- après 5 ans, les données PNR sont transférées dans une

base de données avec des règles d'accès plus strictes (précédemment 7 ans).

En général, les autorités américaines peuvent avoir accès aux données pour prévenir ou poursuivre des infractions terroristes pour lesquelles on encourt 3 ans de détention au moins.

Cet accord doit encore être approuvé par le Conseil de l'Union européenne et par le Parlement européen.

2.5.1.5 Publicité comportementale en ligne

La directive 2009/136/CE, modifiant la directive 2002/58/CE, a été transposée en droit national par la loi du 28 juillet 2011 portant modification de la loi modifiée du 30 mai 2005 concernant la vie privée dans le secteur des communications électroniques. Une des innovations importantes de cette loi a trait aux témoins de connexions sur Internet (généralement appelés « cookies ») et à d'autres technologies permettant de collecter des informations sur les utilisateurs.

Initialement, les cookies étaient utilisés pour faciliter l'interaction entre le navigateur et le serveur. Sous la direction des industriels de la publicité, ils étaient employés à d'autres fins: gestion publicitaire, profilage, traçage, etc. Pour cette raison, de nombreux citoyens, politiciens, autorités de protection des données et organisations de défense des consommateurs ont exprimé leurs inquiétudes quant à la publicité comportementale en ligne (« Online Behavioural Advertising ») et l'utilisation de cookies.

Depuis la révision de la directive « e-Privacy » (2002/58/CE), les régies publicitaires doivent obtenir le consentement préalable actif (principe de l'opt-in) des utilisateurs avant d'installer des cookies sur l'ordinateur ou d'y accéder. Le principe de l'« opt-out » n'est plus applicable. Cette mesure devrait augmenter la transparence pour les utilisateurs, qui souvent ne sont pas conscients que les données les concernant sont collectées et utilisées par les régies publicitaires.

Dans son avis 2/2010, le groupe « Article 29 » avait déjà demandé aux réseaux publicitaires et aux fournisseurs de navigateurs de développer et d'implémenter des mécanismes simples et effectifs pour recueillir le consentement actif des utilisateurs pour la publicité comportementale en ligne.

En avril 2011, les acteurs du secteur de la publicité

comportementale en ligne, représentés à la fois par l'EASA (European Advertising Standards Alliance) et l'IAB (Internet Advertising Bureau Europe), ont adopté un code de conduite autorégulateur. En août 2011, le groupe « Article 29 » a adressé une lettre ouverte à l'EASA et à l'IAB faisant valoir ses craintes, en matière de protection des données, à l'égard de l'approche de l'« opt-out » proposée dans le code.

Si le groupe de travail se félicite des initiatives prises par le secteur de la publicité comportementale en matière d'autorégulation, il doit néanmoins constater que ce code, tel qu'il est complété par le site Internet www.youronlinechoices.eu est insuffisant pour assurer la conformité avec la directive « e-Privacy ». Selon le groupe, on a l'impression qu'il est possible de choisir de ne pas être tracé lors de la navigation sur Internet.

Cette impression peut être nuisible aux utilisateurs, mais également à l'industrie si elle pense que ce code répond aux exigences de la directive. Le groupe « Article 29 » a en outre montré dans son avis qu'il est possible d'envisager des solutions pratiques assurant un bon niveau de protection des données sans rendre la navigation difficile et les sites non fonctionnels.

2.5.1.6 La définition du consentement

L'avis 15/2011 du groupe « Article 29 » porte sur le cadre juridique relatif à la notion de « consentement », en application des directives 95/46/CE et 2002/58/CE. Il tend à clarifier les exigences légales existantes et à illustrer leur fonctionnement dans la pratique à l'aide de nombreux exemples de consentement valable et non valable. Il précise aussi certains aspects de la notion de consentement, comme le moment où celui-ci doit être obtenu ou la différence entre le droit d'opposition et le consentement.

Le consentement de la personne concernée a toujours été une notion clé en matière de protection des données. Cependant, il n'est pas toujours aisé de déterminer quand un consentement est nécessaire et quelles sont les conditions qui doivent être remplies pour qu'un consentement soit valable. Ce manque de clarté peut conduire à des divergences de vues sur les bonnes pratiques entre États membres. Il peut également affaiblir la position des personnes concernées.

S'il est utilisé à bon escient, le consentement est un instrument qui permet à la personne concernée de contrôler le traitement de ses données. S'il est, par contre, mal utilisé, le contrôle pour la personne concernée devient illusoire et le consentement constitue une base inappropriée pour le traitement de données.

Actuellement, les conditions du consentement font l'objet d'interprétations diverses, allant de l'obligation systématique d'obtenir un consentement écrit à l'acceptation d'un consentement implicite. C'est pour cette raison que la Commission européenne avait demandé un avis dans le cadre de la révision de la directive 95/46/CE. Il a pour but de clarifier la situation afin de garantir une compréhension commune du cadre juridique existant.

2.5.1.7 Les compteurs intelligents

La problématique de la sécurité et de la confidentialité des données de consommation d'électricité et de gaz a également été abordée par le groupe « Article 29 ».

Le comptage intelligent consiste à installer chez les particuliers des compteurs de gaz et d'électricité pouvant communiquer de façon bidirectionnelle avec un système informatique central de collecte et de gestion des données situé chez les gestionnaires de réseaux. Les compteurs intelligents informent les clients de la quantité d'énergie qu'ils consomment et ces informations peuvent aussi être transmises aux fournisseurs

Les activités en 2011

d'énergie et à d'autres parties désignées. Ils offrent de nouvelles fonctionnalités, comme la production d'information détaillée sur la consommation d'énergie, la possibilité d'effectuer des relevés à distance, l'élaboration de nouveaux tarifs et services sur la base de profils énergétiques, et la possibilité d'interrompre la fourniture à distance.

Ils revêtent une importance particulière dans la mesure où ils peuvent avoir une incidence sur la vie de tous les citoyens susceptibles de recevoir un approvisionnement en électricité et en gaz. L'objectif de l'Union européenne est d'atteindre une couverture de 80% des consommateurs d'ici 2020.

Les avantages de l'utilisation intelligente de l'énergie sont notamment la possibilité pour les consommateurs de réduire leurs factures en changeant leurs habitudes, par exemple en utilisant l'énergie à des moments différents de la journée pour profiter de tarifs plus bas, ainsi que des possibilités pour l'industrie de prévoir de façon plus précise la demande et donc d'éviter des coûts élevés de stockage de l'électricité.

Si ces programmes offrent de nombreux avantages, ils permettent aussi de traiter de plus en plus de données à caractère personnel et de rendre ces données aisément accessibles à un cercle d'utilisateurs plus large qu'avec un compteur « traditionnel ». Le risque d'intrusion dans la vie privée est plus grand dans la mesure où les fournisseurs ont un aperçu des habitudes personnelles de consommation.

Dans son avis 12/2011, le groupe « Article 29 » a démontré que des données à caractère personnel étaient traitées par les compteurs et que, par conséquent, les législations relatives à la protection des données s'appliqueraient.

Il a également préconisé que le responsable du traitement devait être clairement identifié et avoir connaissance des obligations que lui impose la législation, notamment du point de vue de la prise en compte du respect de la vie privée dès la conception, de la sécurité et des droits des personnes concernées.

Celles-ci devaient être correctement informées de la façon dont sont traitées leurs données et avoir conscience des différences fondamentales dans les modes de traitement pour être en mesure de donner valablement leur consentement.

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

La Commission nationale a participé aux travaux du Comité consultatif de la Convention STE n°108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD) et de son bureau.

2.5.2.1 Modernisation de la Convention 108

En 2011, le Conseil de l'Europe a fêté le 30e anniversaire de sa Convention sur la protection des données (généralement appelée « Convention 108 »), qui a influencé la législation en la matière dans plus de 40 pays européens.

La Convention 108 fait actuellement l'objet d'une révision afin de tenir compte des réalités d'aujourd'hui qui, avec le développement des nouvelles technologies et les effets de mondialisation, nous posent de nouveaux défis en matière de protection des données.

Le T-PD est en charge des travaux de modernisation de la Convention qui ne font que commencer. À l'occasion de la 5e Journée de la protection des données (le 28 janvier 2011), le Conseil de l'Europe a lancé une consultation publique sollicitant les personnes et organisations intéressées à envoyer au Secrétariat leurs commentaires, réflexions et idées au sujet de la révision de la Convention 108.

Des orientations générales ont été élaborées lors des discussions menées pendant les réunions du T-PD à l'aide des contributions provenant d'experts scientifiques et d'observateurs associés aux travaux. Il a été proposé:

- de maintenir les dispositions de la Convention, avec des textes sectoriels plus détaillés au moyen de recommandations du Comité des Ministres du Conseil de l'Europe ;
- d'assurer la cohérence et la compatibilité avec le cadre juridique de l'Union européenne ;
- de maintenir des dispositions technologiquement neutres ;
- de réaffirmer la vocation universelle et le caractère ouvert de la Convention.

À l'occasion de la 33e Conférence internationale des Commissaires à la vie privée et à la protection des données, qui s'est tenue les 2 et 3 novembre 2011 à Mexico, le Conseil de l'Europe a fait une campagne en faveur de la reconnaissance, à l'échelle mondiale, de sa Convention 108 comme seule option réaliste et prête à l'emploi pour l'établissement de normes internationales en matière de respect de la vie privée.

« La vie privée est un droit qui s'applique à tous, qu'il s'agisse de contrôler la collecte, l'utilisation ou la communication d'informations nous concernant. Ce droit est le fondement d'autres libertés qui définissent les sociétés ouvertes, en particulier la liberté d'expression », a affirmé Maud de Boer-Buquicchio, secrétaire générale adjointe du Conseil de l'Europe.

Pour le Conseil de l'Europe, l'approche ouverte qui est la sienne est incontournable pour traiter ce problème au niveau planétaire. : « *Le cyberespace ouvre des possibilités infinies, mais cela ne devrait pas se faire au détriment de la dignité humaine, ni au détriment des droits de l'homme. Nous sommes convaincus que ces valeurs ne sont pas seulement propres à l'Europe : elles sont universelles et doivent être préservées dans le monde entier. C'est en cela que réside l'importance de la Convention pour la protection des données* », a expliqué la secrétaire générale adjointe.

2.5.2.2 Autres travaux du T-PD

À côté des travaux sur la modernisation de la Convention 108, le T-PD est également en train de réviser deux recommandations.

Les activités en 2011

Il s'agit notamment de la recommandation (89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi et de la recommandation (87) 15 visant à réglementer la protection des données à caractère personnel dans le secteur de la police.

La Comité consultatif a par ailleurs préparé un projet d'avis sur les projets de textes préparés par le Comité d'experts sur les nouveaux médias (MC-NM) au sujet des réseaux sociaux et des moteurs de recherche ainsi qu'un projet de document de consultation sur la prédictivité, les tests génétiques et l'assurance.

2.5.3 Le « Groupe de Berlin »

Le Groupe de travail international sur la protection des données dans les télécommunications, mieux connu sous le nom de « Groupe de Berlin » se penche surtout sur la problématique de la protection de la vie privée dans les services de télécommunication et sur Internet.

Lors de deux réunions en 2011 à Montréal et à Berlin, le groupe a adopté trois documents de travail.

2.5.3.1 Enregistreurs de données routières

Les enregistreurs de données routières (EDR - Event Data Recorders on Vehicles) peuvent apporter des bénéfices notables en matière de sécurité routière. Leur rôle est de mémoriser les paramètres de conduite, comme la boîte noire d'un avion. Ils peuvent enregistrer des données avant, pendant et après un accident, concernant la vitesse et l'accélération du véhicule, le déploiement du coussin gonflable, ainsi que d'autres variables relatives aux occupants.

Le Groupe de Berlin a constaté dans son document de travail qu'en raison du développement rapide des nouvelles technologies, le traitement de données dans les véhicules (à usage privé ou professionnel) a augmenté considérablement. Sans garanties appropriées en matière de protection des données, les passagers de ces « voitures intelligentes » n'ont pas la possibilité de contrôler la collecte des données et n'en sont souvent même pas conscients. Les données transmises peuvent être intéressantes pour un nombre croissant de parties prenantes, notamment les constructeurs de voitures, la police, les compagnies d'assurance, les chercheurs et les annonceurs.

Afin d'éviter que les enregistreurs de données routières soient utilisés pour des raisons déloyales, le groupe de travail a fait appel dans son document de

travail aux acteurs responsables pour mettre en place un cadre législatif approprié et de promouvoir l'adoption de standards technologiques.

2.5.3.2 « Privacy by Design » et compteurs intelligents

« Compteurs intelligents » (en anglais « smart meters ») est le terme employé pour désigner une nouvelle génération de compteurs d'électricité. Ceux-ci disposent de technologies avancées qui identifient de manière plus détaillée et éventuellement en temps réel la consommation énergétique d'une habitation. Les compteurs « intelligents » permettent également une communication dans les deux sens, l'établissement de factures en temps réel et le repérage des postes qui coûtent le plus cher au client.

Même si cette notion renvoie le plus souvent aux compteurs d'électricité, cette technologie commence également à être appliquée pour la mesure des consommations de gaz et d'eau. Un rapport de Pike Research[1] suppose que 250 millions de foyers seront équipés de compteurs intelligents en 2015.

Avec son document de travail, le Groupe de Berlin a attiré l'attention sur les atteintes potentielles à la vie privée que permettent les compteurs intelligents. En collectant les informations toutes les 10 à 30 minutes, ils génèrent une masse de données dont on peut déduire des informations très personnelles sur les habitudes des usagers. De plus, si on connaît la consommation d'électricité d'une maison, il est possible de savoir dans quelle pièce se trouvent les habitants, quand ils sont présents et quand ils dorment.

Le Groupe de Berlin a également noté que le « smart metering », qui se trouve encore à ses débuts, est particulièrement bien adapté à l'application des principes du « Privacy by Design ». Le respect de la vie privée dès la conception signifie prendre en compte dès le début du développement des compteurs intelligents les exigences en matière de protection des données et intégrer les outils de protection directement dans le produit, au lieu de les ajouter ultérieurement sous forme de compléments. Idéalement, aucune action du consommateur ne devrait être nécessaire pour protéger sa vie privée (« Privacy by Default »).
En outre, seulement les données strictement nécessaires à la finalité de ces compteurs devraient sortir de la maison du consommateur par un « smart meter » (principe de minimisation des données). Enfin, le Groupe a insisté sur le fait que les consommateurs ne devraient pas être contraints de choisir entre la protection de leur sphère privée et l'efficacité énergétique.

2.5.3.3 Micropaiement sur Internet

Un nombre croissant de services en ligne, gratuits auparavant, sont devenus payants. Contre une petite somme d'argent, l'utilisateur peut consulter un article en ligne ou un clip vidéo. Même Facebook a commencé à offrir sa propre monnaie, les « Facebook Coins », qui permettent aux internautes d'acheter des applications tierces. Celles-ci deviennent de plus en plus populaires sur le réseau social.

Ces développements peuvent conduire à des atteintes à la vie privée des utilisateurs. Les fournisseurs de systèmes de micropaiement pourraient en effet utiliser les données collectées lors de l'enregistrement à des fins publicitaires. Un autre risque consiste dans le fait que les opérations de micropaiement pourraient générer des traces sur qui a consulté quel média et à quel moment.

Selon le Groupe de Berlin, il doit rester possible d'effectuer des paiements anonymes en ligne, surtout s'il s'agit de petites sommes. De ce fait, le Groupe fait appel aux régulateurs pour ne pas interdire le paiement anonyme et intégrer ces dispositions dans leur législation nationale.

[1] Pike Research (Nov. 2, 2009) "Smart Meter Installations to Reach 250 Million Worldwide by 2015", online : http://www.pikeresearch.com/newsroom/smart-meter-installations-to-reach-250-million-worldwide-by-2015.

Les activités en 2011

De plus, le Groupe veut rendre les utilisateurs attentifs au fait que leur choix de méthode de paiement peut avoir un effet direct sur le niveau de protection de la vie privée.

2.5.4 Le séminaire européen « Case Handling Workshop »

L'autorité de protection des données polonaise a organisé le 23e séminaire européen « Case Handling Workshop » du 4 au 5 octobre à Varsovie.

Cet atelier présente l'opportunité pour les employés des autorités de protection des données européennes d'échanger leurs expériences pratiques en matière de traitement des plaintes.

En 2011, les thèmes suivants ont été abordés :

- réseaux sociaux et Internet;
- protection de la vie privée au lieu de travail;
- traitements de cas transfrontaliers;
- méthodologie d'audit/ inspection.

3 Les temps forts de 2011

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

3.1 Conclusion d'un partenariat avec le Centre Interdisciplinaire pour la Sécurité, la Fiabilité et la Confiance (SnT) de l'Université du Luxembourg

La Commission nationale et le Centre Interdisciplinaire pour la Sécurité, la Fiabilité et la Confiance (SnT) de l'Université du Luxembourg ont lancé un programme commun de recherche intitulé « Legal issues in Data protection, Cloud Computing and Privacy ».

Ce programme comporte trois principaux domaines d'analyse :

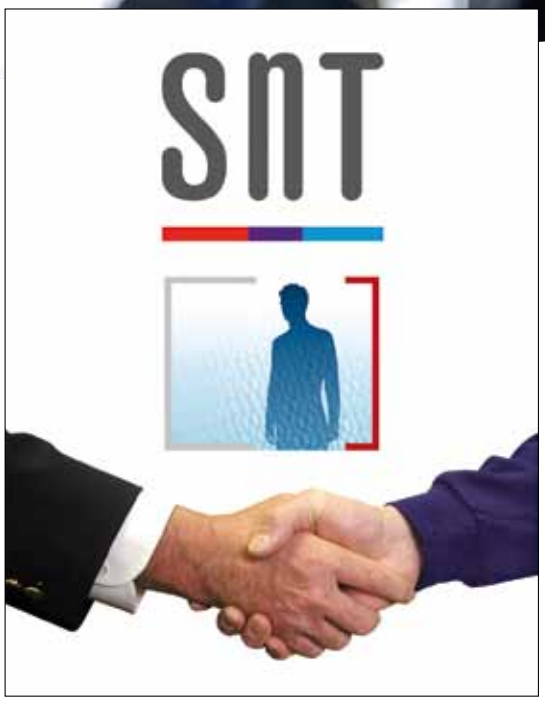
- les nouveaux développements de la législation européenne en matière de protection des données ;
- les défis technologiques tels que le cloud computing et leurs répercussions pour les acteurs publics et privés du site luxembourgeois ;
- le concept de « privacy by design ».

La protection des données personnelles joue un rôle de plus en plus significatif tant à l'échelle internationale qu'au Luxembourg. La conformité à la législation en la matière devient d'autant plus importante pour les différents acteurs traitant des données. Compte tenu de l'évolution rapide des technologies de l'information et de la communication (TIC) et de la réglementation dans ce domaine, les sociétés privées et les pouvoirs publics ont besoin d'un savoir-faire juridique et technique particulier, afin de garantir que leurs activités répondent aux requis des lois en vigueur.

En tant qu'autorité de contrôle, la CNPD est chargée de vérifier la légalité des traitements des données à caractère personnel des acteurs privés et publics. Elle s'occupe des demandes et plaintes des citoyens et avise les projets de loi. Lors de ses appréciations et investigations, elle se penche sur des questions juridiques et techniques. Le SnT mène des recherches scientifiques dans le contexte des services TIC tels que les réseaux de communication et les systèmes logiciels pour en améliorer la sécurité et la fiabilité, et afin de renforcer la confiance des utilisateurs en ces services. Dans

Centre Interdisciplinaire pour la Sécurité, la Fiabilité et la Confiance (SnT)

Créé en 2009 par l'Université du Luxembourg, le SnT est une plate-forme de recherche de renommée internationale qui, avec des partenaires externes, agit en sorte que le Luxembourg devienne un centre européen d'excellence et d'innovation en matière de systèmes et services TIC (Technologies d'information et de communication) sécurisés, fiables et dignes de confiance. Le SnT propose une plate-forme d'interaction et de collaboration entre les chercheurs universitaires et les partenaires extérieurs.



ces domaines, la CNPD et le SnT entendent réunir leur savoir-faire dans le cadre de leur partenariat stratégique.

La coopération entre la CNPD et le SnT sur le plan scientifique contribuera par son analyse conceptuelle et l'identification des aspects critiques à une approche approfondie et orientée vers l'avenir. Une attention particulière sera attachée à l'incidence des évolutions constatées sur les acteurs du site luxembourgeois. La coopération a commencé au 1er novembre 2011 et durera dans une première phase jusqu'au 31 décembre 2014.

Le partenariat entre les deux institutions se concrétise avec une chercheuse qui travaille à mi-temps auprès de la CNPD et auprès du SnT. Elle facilite l'échange entre les deux institutions et coordonne le travail au quotidien. Une des premières tâches sera d'accompagner les nouveaux développements de la législation européenne en matière de protection des données.

Analyse des conséquences de la refonte du cadre législatif européen

Il importe d'avoir une compréhension rapide de la future législation européenne dans le domaine et d'en analyser les répercussions. Si cette législation correspondait bien à l'état de l'art en 1995, elle requiert aujourd'hui une refonte face à l'essor de nouveaux services en ligne tels que les réseaux sociaux. Dans ce contexte, le cadre législatif existant est actuellement réexaminé. La mise en œuvre de ces règles modernisées nécessitera, outre leur transposition en droit luxembourgeois, des travaux de recherche sur les répercussions qu'elles auront à la fois sur l'utilisation des données à caractère personnel et sur le travail des autorités de contrôle (voir point 4. pour plus d'informations à ce sujet).

L'exemple du cloud computing et de la protection des données

L'harmonisation du cloud computing et de la confidentialité des données constitue un autre point d'intérêt commun entre la CNPD et le SnT.

L'utilisation de plus en plus fréquente du cloud computing (où les utilisateurs accèdent aux ressources informatiques à distance, plutôt que de les stocker localement) pour traiter les données à caractère personnel soulève des problèmes juridiques et techniques.

3 Les temps forts de 2011

Privacy by design : les 7 principes fondamentaux

1. Prendre des mesures proactives et non réactives; des mesures préventives et non correctives
2. Assurer la protection implicite de la vie privée
3. Intégrer la protection de la vie privée dans la conception des systèmes et des pratiques
4. Assurer une fonctionnalité intégrale selon un paradigme à somme positive et non à somme nulle
5. Assurer la sécurité de bout en bout, pendant toute la période de conservation des renseignements
6. Assurer la visibilité et la transparence
7. Respect de la vie privée des utilisateurs

Source : www.privacybydesign.ca

Avec le cloud computing, des données peuvent être traitées au Luxembourg, stockées à Bombay et consultées à Los Angeles. À l'ère numérique, les données sont communément transférées d'un pays à l'autre, tant à l'intérieur qu'en dehors de l'Union. Mais tous les pays ne garantissent pas le même niveau de protection des données à caractère personnel.

La compréhension des aspects techniques et réglementaires du cloud computing et de sa portée particulière pour le Luxembourg représentera un défi important pour les deux institutions.

Privacy by design

Le troisième domaine d'analyse du programme de recherche porte sur le concept de « privacy by design ». Celui-ci garantit que la protection de la vie privée est intégrée dans les nouvelles pratiques technologiques et commerciales dès leur conception, au lieu de les ajouter ultérieurement sous forme de compléments. Ce concept joue un rôle essentiel dans la révision de la directive de 1995.

Des solutions « made in Luxembourg »

« Au cours des dernières années, de nouveaux services tel que Google Street View, mis en œuvre dans un délai assez bref, ont constitué de réels enjeux pour le cadre législatif actuel et ont exigé une réponse rapide sur la manière de traiter ces services », a déclaré le Prof. Björn Ottersten, directeur du SnT. Gérard Lommel, président de la CNPD, a ajouté que « notre programme de recherche commun répondra à ces questions fondamentales de la protection des données dans un environnement technologique moderne. Nos résultats contribueront à sensibiliser le public et aideront à définir des solutions 'made in Luxembourg' qui pourront servir d'exemples pour faire face aux nouveaux défis dans ce domaine dès le début ».

3.2 Base de données relative aux élèves

Le projet de loi n°6284 vise la création et l'exploitation d'une nouvelle base de données à caractère personnel des élèves par le Ministère de l'Education nationale et de la Formation professionnelle (ci-après désigné le « Ministère »). La base de données comportera tout leur suivi scolaire mais aussi des informations sur leur milieu socioculturel et familial. Elle a comme finalité un meilleur suivi administratif et pédagogique des élèves, ainsi qu'une optimisation de la qualité de l'enseignement à travers des analyses et recherches statistiques approfondies.

Le projet de loi règle aussi la question de la collecte des données, l'accès aux données, la communication des données à des tiers et définit des règles concernant leur confidentialité et sécurité.

Dans un premier temps, il avait été envisagé de créer et d'organiser la nouvelle base de données par voie de règlement grand-ducal autorisé par la loi du 6 février 2009 sur l'obligation scolaire. Or, à la suite du premier avis de la Commission nationale, en date du 26 juillet 2010 (délibération n° 238/2010), au sujet du projet de ce règlement grand-ducal, il s'était avéré que les bases légales existantes étaient trop faibles. C'est donc sur recommandation de la Commission nationale que le projet de loi n°6284 et son projet de règlement grand-ducal d'exécution ont vu le jour. Elle s'est prononcée une seconde fois à ce sujet dans son avis du 15 avril 2011 (délibération n° 126/2011).

Avis du 26 juillet 2010

Dans sa prise de position du 26 juillet 2010, la Commission nationale a noté que la nouvelle base de données intègre deux bases de données déjà existantes, le « Scolaria élèves » et le « Fichier élèves », et qu'il est envisagé d'englober davantage de données que ne le permet le règlement grand-ducal du 20 juin 2001 (autorisant la création et l'exploitation d'une banque de données nominative relative

3 Les temps forts de 2011

aux élèves), mais aussi et surtout, davantage d'acteurs que ne le permet le cadre tracé par l'article 20 de la loi du 6 février 2009.

La Commission nationale a reconnu l'intérêt de la base de données en tant que telle, en vue notamment d'une meilleure planification et évaluation de la qualité de l'enseignement. Toutefois, elle a relevé que l'accroissement du nombre de données collectées et l'augmentation de transferts de données entre les différents protagonistes soulèveraient des interrogations quant à la protection de la vie privée et des données à caractère personnel des élèves et de leurs représentants légaux.

Devant le constat du manque d'une base légale suffisante, mais également dans un souci de transparence et de prévisibilité, la Commission nationale a insisté sur le fait que la création d'un fichier d'une telle envergure nécessiterait une loi propre qui devrait se consacrer aux principes généraux relatifs au traitement en cause et définir clairement les finalités du traitement afin de pouvoir vérifier l'existence de fins d'intérêt public.

Sur base de ces recommandations, le Ministère

a décidé d'ancrer la nouvelle base de données dans une loi, accompagnée d'un règlement grand-ducal. Ce dernier énumère limitativement les données pouvant être enregistrées dans la base de données. Selon l'exposé des motifs du projet de loi, cette démarche doit permettre de fermer la porte à des dérives menant vers l' « élève transparent ».

Dans ce premier avis, la Commission nationale s'est encore exprimée sur les problématiques suivantes :

L'origine des données à caractère personnel
La Commission nationale a estimé utile qu'une loi vienne préciser auprès de qui sont collectées les données. Pour permettre une vérification du caractère légitime, compatible et non excessif par rapport aux finalités du fournisseur et du fichier dont elles proviennent, il faudrait indiquer plus précisément au sein du règlement grand-ducal quel organisme fournit quelles données. Ces recommandations ont été intégrées dans le projet de loi.

La nature des données à caractère personnel
En ce qui concerne les informations relatives à la catégorie socioprofessionnelle des personnes exerçant la responsabilité parentale, la Commission nationale s'est demandé si cette notion n'était pas trop large et imprécise. Pour elle, il aurait été préférable de collecter ces informations ponctuellement dans le cadre d'études statistiques plutôt que dans une base de données conservée pendant une longue période et accessible à un nombre important de personnes. Dans son avis du 6 décembre 2011, le Conseil d'Etat s'est rallié à ces vues de la CNPD.

L'accès aux données à caractère personnel
Le nombre important de données en jeu et le caractère sensible de certaines d'entre elles rendent la réglementation de leur accès nécessaire. La Commission nationale n'a émis aucun doute quant à l'intérêt légitime des utilisateurs autorisés d'accéder aux données, mais s'est demandé si cet accès n'était pas trop large et donc susceptible de faciliter des abus. Selon elle, l'accès ne pourra être autorisé que pour les seules données nécessaires à l'exécution des missions confiées aux utilisateurs autorisés, ceci en vertu des principes de proportionnalité et de nécessité établis à l'article 4 de la loi modifiée du 2 août 2002.

La communication des données à caractère personnel à des tiers
Le législateur a fait suite aux recommandations de la Commission nationale, d'établir, d'une part, des groupes parmi les destinataires et d'identifier au sein de la loi les finalités pour lesquelles ces groupes sont voués à recevoir les données. D'autre part, elle a conseillé de déterminer les listes de données concrètes pouvant faire l'objet d'une collecte ou d'un échange au sein d'un règlement grand-ducal, ceci dans un souci de flexibilité, pour permettre une évolution ultérieure de cette liste tout en respectant la nature des données telle que définie dans la loi.

Le traitement de données à caractère personnel à des fins de recherche statistiques ou scientifiques
La loi modifiée du 2 août 2002 autorise un traitement ultérieur de données à des fins d'analyses et de recherches statistiques ou scientifiques qui n'est pas jugé incompatible avec les finalités pour lesquelles les données ont été collectées. Selon l'exposé des motifs du projet de loi, les données alimentant les analyses et études afférentes seront rendues anonymes au départ lorsque des tiers en seront chargés. De même, lorsque le Ministère souhaite effectuer lui-même une telle recherche, il ne devrait le faire qu'à l'aide de données préalablement anonymisées. Néanmoins, si cette technique ne permet pas d'atteindre les finalités

Les temps forts de 2011

escomptées, le Ministère pourra alors recourir à des données codées. En tout état de cause, la Commission nationale est d'avis que seules les données nécessaires pour effectuer la recherche pourront être utilisées.

Les mesures de sécurité
La Commission nationale était satisfaite de voir intégré un chapitre particulier traitant des mesures de sécurité. Toutefois, elle a suggéré de préciser les mesures techniques d'accessibilité et organisationnelles. Cette recommandation a été suivie par le législateur dans le projet de loi.

La durée de conservation
L'avant-projet de règlement grand-ducal soumis à l'avis de la Commission nationale a entendu autoriser la conservation des données durant une période de cent ans. La Commission nationale a considéré cette durée difficilement justifiable au vu des finalités exposées, à savoir la scolarité des élèves.

Selon elle, une période de conservation de dix ans après le cursus scolaire devrait être suffisante. Au-delà, les données devraient être anonymisées de façon irréversible. Le gouvernement a finalement opté pour une destruction des données 15 ans après la fin du cursus scolaire dans le projet de loi n°6284.

Avis du 15 avril 2011

Dans son second avis du 15 avril 2011, la Commission nationale s'est félicitée que le législateur ait repris dans une large mesure les observations formulées dans sa prise de position du 26 juillet 2010.

Toutefois, elle a réitéré ses réserves à l'égard de la communication de données non dépersonnalisées à l'Université du Luxembourg dont elle estimait le libellé trop général et pas assez restrictif en vue d'éviter tout risque d'abus. Elle a également formulé quelques remarques au sujet de la nouvelle disposition relative aux partenariats pour la recherche.

3.3 Protection de la vie privée dans le secteur des communications électroniques

3.3.1 Les violations de sécurité doivent être signalées par les opérateurs

Le 1er septembre 2011 est entrée en vigueur la loi du 28 juillet 2011 portant modification de la loi modifiée du 30 mai 2005 concernant la vie privée dans le secteur des communications électroniques. Elle transpose certaines dispositions de la

directive 2009/136/CE modifiant la directive 2002/58/CE concernant le traitement de données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

La nouvelle législation entend mieux protéger les utilisateurs de services de télécommunications en cas de « pannes » de sécurité et de violations de données personnelles.

Désormais, les fournisseurs de services de communications électroniques accessibles au public, comme les entreprises de téléphonie fixe ou mobile ou les fournisseurs d'accès à Internet, doivent avertir immédiatement la Commission nationale en cas de survenance d'une violation de la sécurité et de la confidentialité de données à caractère personnel et d'informer de surcroît leurs abonnés dès lors que l'incident constaté est susceptible d'affecter défavorablement le niveau de la protection de leur vie privée et des données les concernant.

La loi définit la violation de données à caractère personnel comme une « violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés de données à caractère personnel transmises, stockées ou traitées d'une autre manière en relation avec la fourniture de services de communications électroniques accessibles au public ».

Il peut s'agir de toutes sortes de « pannes », comme par exemple des hypothèses suivantes:

- Des personnes externes ont, par le biais d'Internet, accès aux serveurs contenant toutes les données de clients en raison de failles dans la sécurité du système informatique du fournisseur de services concerné.
- A un moment donné, tout le monde peut avoir accès aux comptes client en ligne sans mot de passe alors que seulement les clients donnant le mot de passe devraient avoir accès à leurs comptes respectifs.
- Un salarié d'un fournisseur de services perd un CD-ROM ou une clé USB avec des données de clients.

Dans ce cas de violation, le fournisseur de services de communications électroniques notifie sans retard la Commission nationale de la violation. La notification décrit notamment la nature de la violation de données à caractère personnel, les conséquences de la violation de données à caractère personnel, les mesures proposées ou prises par le fournisseur pour y remédier, ainsi que des recommandations à l'intention des abonnés ou des particuliers concernés et les points de contact auprès desquels des informations supplémentaires peuvent être obtenues.

En cas de violation de nature à affecter les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier (par exemple, lorsqu'elle est susceptible d'entraîner le vol ou l'usurpation d'identité, une atteinte à l'intégrité physique,

une humiliation grave ou une réputation entachée en rapport avec la fourniture de services de communications accessibles au public), ces abonnés ou particuliers doivent également en être avertis sans retard afin de pouvoir prendre les précautions qui s'imposent. La notification faite à l'abonné ou au particulier décrit au minimum la nature de la violation de données à caractère personnel et les points de contact auprès desquels des informations supplémentaires peuvent être obtenues, et recommande des mesures à prendre pour atténuer les conséquences négatives possibles de la violation de données à caractère personnel. La notification d'une violation des données à caractère personnel à l'abonné ou au particulier concerné n'est pas nécessaire si le fournisseur a prouvé, à la satisfaction de la Commission nationale, qu'il a mis en œuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données concernées par ladite violation. De telles mesures de protection technologiques rendent les données incompréhensibles (par encryptions p.ex.) à toute personne qui n'est pas autorisée à y avoir accès.

La Commission nationale a par ailleurs reçu le pouvoir de donner des sanctions financières. Lors d'un premier manquement aux obligations de notification, le fournisseur est averti par la Commission nationale. En cas de manquement répété, elle peut prononcer une amende d'ordre qui ne peut excéder 50.000 euros.

La loi du 28 juillet 2011 prévoit également que les fournisseurs tiennent à jour un inventaire des violations de données à caractère personnel, notamment de leur contexte, de leurs effets et des mesures prises pour y remédier. Les données consignées doivent être suffisantes pour permettre à la Commission nationale pour la protection des données de les vérifier.

3.3.2 Protection des consommateurs

La loi du 28 juillet 2011 porte également modification de l'article L.311-5 du Code de la consommation et dispose que la Commission nationale est dorénavant l'autorité compétente à caractère sectoriel pour toutes les questions relatives à la protection de la vie privée dans le secteur des communications électroniques visées sous le point 17 de l'annexe du Règlement (CE) 2006/2004 dont l'objectif est d'assurer le respect des lois protégeant les intérêts des consommateurs.

Le Ministère de l'Economie et du Commerce extérieur, Direction du Marché intérieur et de la Consommation, exerce dans ce cadre outre le rôle d'autorité compétente à caractère général, la fonction de bureau de liaison unique prévu par l'article L.311-3

Discours d'accueil de Gérard Lommel


Alexander DIX, Richard ALLAN et Gérard LOMMEL


François BILTGEN, Alexander DIX et Gérard LOMMEL

du Code de la consommation. Dans ce cadre, le Ministère est en charge de la mise en œuvre au Luxembourg du système CPC-S (Consumer Protection Cooperation System), qui est un système informatique instauré par la Commission européenne afin d'assurer et de faciliter la coopération entre les Etats membres de l'UE en matière de protection des consommateurs. Cet outil informatique prévoit à la fois de traiter les demandes de coopération en provenance d'organismes des autres Etats membres de l'UE, ainsi que de rédiger, d'adresser et de traiter des demandes en direction des autorités des autres pays membres.

3.4 Conférence « Y a-t-il encore une vie privée sur Internet ? »

Le 27 janvier 2011, à la veille de la Journée européenne de la protection des données et dans le cadre du 30e anniversaire de la Convention du Conseil de l'Europe sur la protection des données, la Commission nationale a organisé une conférence suivie d'une table ronde sur le thème: *«Y a-t-il encore une vie privée sur Internet? »*.

Devant un public de plus de 160 personnes à l'auditoire du Cercle Cité, le Dr Alexander Dix (Commissaire à la protection des données et à l'accès à l'information du Land Berlin), expert en matière de protection des données dans le secteur des communications électroniques, a été le premier à prendre

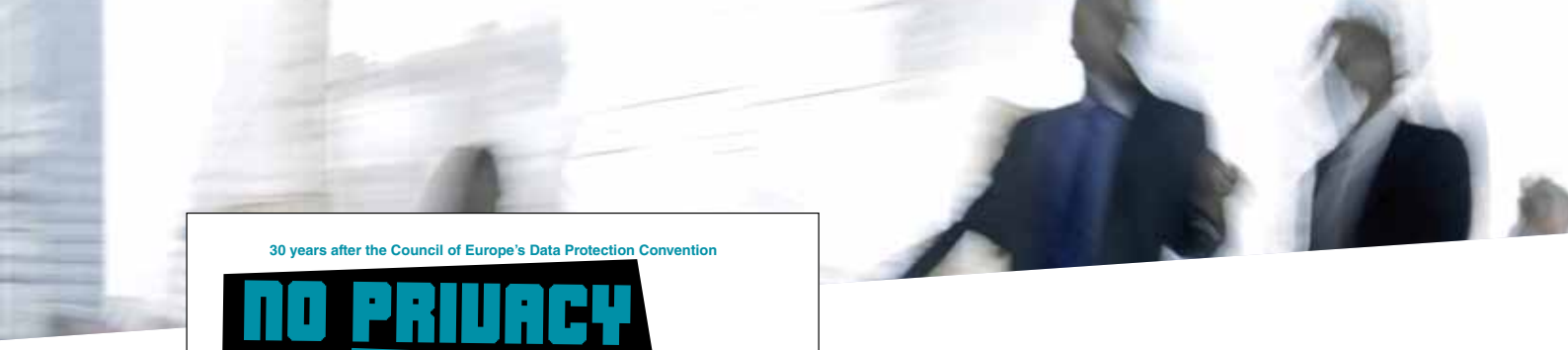
3 Les temps forts de 2011

De gauche à droite: Lucien THIEL (†), Marco GOETZ, Alexander DIX, Gérard LOMMEL, Richard ALLAN et René SCHLECHTER

la parole. Le conférencier a commencé sa présentation en confirmant que la législation européenne protège aussi la vie privée sur Internet.

Depuis plus de 30 ans, la « Convention 108 » du Conseil de l'Europe constitue la base de la législation européenne et reste dans ce domaine l'instrument juridique international de référence. Est-ce que ces dispositions sont encore d'actualité aujourd'hui ? Est-il possible de contrôler ses données sur Internet ? Les services en ligne et notamment les réseaux sociaux ont-ils ouvert une ère de transparence totale et de la fin de la vie privée ? Tels étaient les questions principales posées par le Dr Dix.

Selon lui, beaucoup de réseaux sociaux et autres services sur Internet proposent des paramètres par défaut qui ne protègent pas la vie privée des utilisateurs. Pour cette raison, il a attiré l'attention du public sur l'importance de la sensibilisation et de la responsabilisation des utilisateurs quant aux données publiées. Il a également milité pour un meilleur contrôle de leurs données personnelles par les utilisateurs, la possibilité d'utiliser des pseudonymes et une meilleure sécurisation du système.



Richard Allan, le *Director of Policy Europe* de Facebook, a présenté le fonctionnement des paramètres de confidentialité du réseau social et a rappelé que Facebook permet de configurer son profil de façon à publier ou non un certain nombre d'informations. Une fonction de prévisualisation de la manière dont apparaît un profil, des guides de confidentialité et de sécurité complètent la politique de la société en la matière.
Il a également insisté sur le fait que le réseau social est une plate-forme majoritairement utilisée par des adultes et créée pour que tout le monde sache à qui il s'adresse sur Internet et avec qui il partage des messages, des photos et d'autres documents.
Ensuite une table ronde a eu lieu à laquelle ont encore participé feu Monsieur le Député Lucien Thiel (Député, Président de la Commission des Médias), Monsieur René Schlechter (Chargé de direction du 12345 KannerJugendTelefon, BeeSecure) ainsi que Jan Guth du Chaos Computer Club Luxembourg. Les sources de revenus de ces services en ligne, le traçage sur Internet, la publicité comportementale en ligne, l'impact des smartphones, la protection des jeunes et la sécurité des données étaient parmi les sujets traités au cours de cette table ronde.

« No Privacy Online Anymore ? »

Tu laisses des traces sur Internet

Avec une simple recherche sur Google, on peut trouver facilement des informations sur sa prochaine destination de vacances. Des services en ligne permettent de comparer les vols disponibles et de réserver la meilleure offre en quelques secondes. Les achats en ligne peuvent être payés en un seul clic avec des services comme Paypal. Des sites de commerce électronique tel qu'Amazon détectent « automatiquement » les produits qui pourraient nous intéresser. Les opérations financières peuvent être réglées facilement à domicile. Adresse IP, nom ou numéro de la carte de crédit : nous laissons des traces multiples sur Internet. L'enregistrement des « cookies » sur notre terminal et les « empreintes digitales » de notre navigateur permettent de retracer sans équivoque notre navigation en ligne.

La publicité sur mesure

Si un utilisateur recherche un produit spécifique sur la toile, il n'est pas improbable que des annonces portant sur le même type de produit apparaissent ultérieurement lorsqu'il ouvre d'autres sites. Non, ce n'est pas un hasard.

3 Les temps forts de 2011

Les recherches sur Google, clics et autres renseignements personnels sont analysés pour sélectionner des publicités « sur mesure », adaptées à ses préférences en ligne. Même s'il ne publie pas lui-même des contenus en ligne, ses habitudes et comportements (sites visités, vidéos regardées, liens cliqués, …) sont stockés systématiquement et examinés. Toutes ces traces permettent de créer un profil avec les préférences, les activités et le style de vie de l'utilisateur - souvent à son insu.

Je sais où tu te trouves

L'époque où un GSM servait aux seuls appels téléphoniques est révolue depuis longtemps - les appareils modernes sont de petite taille, ont une grande polyvalence et permettent aisément de surfer sur Internet. Un smartphone avec récepteur GPS et une application appropriée suffisent pour montrer à tout le monde, en temps réel, où on se trouve. Ces *Apps* sont très populaires et disponibles pour de multiples usages – souvent même gratuitement – mais, en contrepartie, elles peuvent transmettre, à votre insu, des données à caractère personnel.

Le cloud computing : un nuage de données dans la toile

Des sociétés comme *Google, Apple et Microsoft* offrent (souvent gratuitement) de l'espace en ligne aux internautes. Les données peuvent être téléchargées sur les serveurs de ces fournisseurs et ne se trouvent plus sur l'ordinateur à domicile, des disques durs ou des réseaux locaux. Elles se trouvent pour ainsi dire « dans les nuages ».

Il peut s'agir de nos rendez-vous personnels, de nos adresses de contact (famille, amis, contacts professionnels, etc.), de photos de famille, vidéos privées, textes ou même de bases de données entières.

Ma vie sur Internet

Un simple clic suffit pour publier sur *Facebook* des photos de la dernière sortie ou pour communiquer à ses amis et au monde entier ce qu'on pense grâce à *Twitter*. Le nombre d'informations, de photos ou de vidéos mises en ligne augmente sans cesse. Beaucoup d'internautes documentent toute leur vie privée et oublient souvent qu'ils ne sont pas anonymes et que ces données peuvent être utilisées de différentes manières.

Des nouveaux développements tels que la fonction de reconnaissance faciale, récemment introduite sur *Facebook*, rend le « marquage » (ou « tagging ») des personnes représentées sur les photos de plus en plus facile.

3.5 Protection des données dans le domaine de la santé

Tout au long de l'année, la Commission nationale a continué la concertation avec le Ministère de la Santé lors de réunions de travail sur le dossier de soins partagé, le médecin référent et l'architecture de sécurité du système informatique y relatif.

Ces travaux ont été effectués dans le cadre du programme « eSanté » désignant l'utilisation d'outils et de solutions basés sur les nouvelles technologies de l'information et de la communication, dans le but de mieux exploiter les données médicales et de santé par un meilleur partage et échange d'informations entre acteurs du secteur de la santé et du social.

La création en décembre 2011 de l'Agence nationale des informations partagées dans le domaine de la santé a constitué une étape importante de ce programme. Cette agence est chargée de mettre en place et d'exploiter la plate-forme d'échange et de partage de données, dont notamment le dossier de soins partagé électronique (ci-après le DSP) du patient.

La loi du 17 décembre 2010 portant réforme du système de soins de santé prévoit la mise en place d'un DSP. Ce dernier permettra d'accéder très rapidement à ces informations sur l'état de santé antérieur du patient, contribuant ainsi à la qualité, à la continuité et à une meilleure coordination et sécurité des soins de santé. Il s'agit d'un dossier électronique de partage d'informations sur le patient, accessible aux prestataires de soins de santé qui sont en relation thérapeutique avec le patient titulaire du dossier, et qui ont l'autorisation de consulter les données relatives à sa santé. À retenir que le patient lui-même y a aussi accès et qu'il bénéficiera de son propre espace d'expression, qui doit lui permettre de partager et de gérer dans son DSP les informations qu'il souhaite porter à la connaissance des prestataires de santé.

Le DSP regroupera à l'avenir des informations relatives à la santé du patient en provenance de diverses sources: médecin référent, médecin généraliste, médecins spécialistes, hôpitaux, laboratoires d'analyses médicales, etc. Le DSP comprendra des informations contribuant directement ou indirectement à optimiser la prise en charge et à coordonner les soins. Seules les données jugées pertinentes et utiles à un partage entre professionnels se retrouveront dans le DSP.

Le Médecin Référent (ci-après le MR) correspond à un profil particulier de médecin. En choisissant d'avoir un médecin

3 Les temps forts de 2011

référent, le patient lui donne accès à l'ensemble des données de son DSP.

L'utilisation du DSP est régie par des règles strictes qui s'appliquent à l'ensemble des utilisateurs et visent à en assurer la confidentialité, l'intégrité et la traçabilité. Ces règles sont les suivantes :

- identification des utilisateurs;
- authentification des utilisateurs;
- autorisation des utilisateurs ;
- gestion de la confidentialité ;
- gestion de l'intégrité et de l'imputabilité des données ;
- traçabilité des accès.

Le 12 octobre 2011, la société Deloitte a organisé - en collaboration avec l'Entente des Hôpitaux Luxembourgeois (EHL) - une journée d'échange sur les principales évolutions de la réforme du système des soins de santé. Le Président de la Commission nationale s'est exprimé sur le sujet: « *Qui a accès à nos données médicales ? Les données des patients seront-elles suffisamment protégées ? Quels droits et quelles restrictions et garanties un cadre légal doit-il prévoir ?* ».

Dans le cadre de cette journée, une table ronde a eu lieu avec

des médecins, des représentants de l'EHL et de la CNPD. Le Président de la Commission nationale est surtout intervenu pour répondre aux questions suivantes:

- comment peut-on s'assurer que le partage des données médicales et d'autres informations concernant le patient soit effectué dans le respect de la sécurité, la continuité et la coordination des soins?
- sous quelle forme faut-il envisager la présentation des données ainsi que leur échange (volet e-santé); quelles sont les précautions à prendre afin de garantir un équilibre adéquat entre circulation/ échange de l'information et respect de la confidentialité des données personnelles?

Les données relatives à la santé sont des données sensibles. Leur communication est interdite en principe, sauf dans des cas précis et notamment si le responsable du traitement a obtenu le consentement explicite et informé de la personne concernée. Des principes juridiques internationaux forts comme le secret médical, les droits prévus par l'article 8 de la Convention européenne des Droits de l'Homme, la Charte des droits fondamentaux de l'Union européenne et la directive européenne sur la protection des données protègent les données des patients. Pourtant, le partage et l'échange de ces données suscitent des inquiétudes.

Pour construire un système bénéficiant de la confiance des patients, les conditions suivantes doivent être respectées :

- Le critère de légitimation (le traitement de données doit être nécessaire, ou alors il faut le consentement explicite et informé du patient) ;
- Les données doivent être exactes, pertinentes et non excessives (« Datensparsamkeit ») ;
- Les usages doivent être limités aux seuls traitements compatibles avec la finalité initiale ;
- Limitation des accès et des destinataires (aux personnes connues par le patient, prévisible et envisagé par lui) ;
- Limitation de la durée de conservation ;
- Sécurité et traçabilité des données et des opérations ;
- Le secret médical portant sur les données du dossier.

Étant donné que la centralisation et la mutualisation des données crée de nouveaux risques de violations de confidentialité et de la sécurité, des restrictions et des garanties doivent être prévues.

Une des garanties est le respect de l'autodétermination du patient qui pour le moins devrait toujours pouvoir interdire la communication et l'introduction dans le dossier de soins partagé de certaines données. Aucune personne ne peut avoir accès aux informations du patient à son insu ou contre son gré, sauf en cas d'urgence. Il doit avoir la possibilité de vérifier a posteriori les accès par Internet.

Par ailleurs, seuls les professionnels de santé qui interviennent en ce moment dans le suivi thérapeutique du patient sont, en tout état de cause, autorisés à accéder au DSP. Les procédures à mettre en place à l'hôpital, dans les cabinets médicaux et chez d'autres prestataires de soins doivent être transparentes pour le patient, étant donné que ceci suppose sa participation.

Enfin, le système de contrôle d'accès et d'authentification des professionnels doit être robuste.

4 Perspectives

Au début de l'année 2012, la Commission européenne a présenté ses propositions pour réformer le cadre légal réglementant la protection des données dans l'Union européenne.

Les principes de base de la directive européenne de 1995, garantissant le bon fonctionnement du marché intérieur et le respect du droit fondamental des personnes à la protection des données, restent valables. Or, ils ont été introduits quand Internet était encore à ses débuts et sont aujourd'hui dépassés par l'évolution des technologies comme les réseaux sociaux, le cloud computing, les cartes à puce ou les services de géolocalisation. À l'heure où notre monde est toujours plus interconnecté, la protection des données ne concerne plus seulement quelques grandes banques de données. Ainsi, un des défis majeurs de la Commission européenne sera de réconcilier l'évolution technologique avec les libertés fondamentales des citoyens.

De plus, certaines différences dans la façon dont chaque État membre applique la législation ont conduit à des inégalités dans le niveau de protection des données à caractère personnel, selon le lieu où une personne vit ou achète des biens et des services. Afin de rendre la protection plus claire et uniforme, la Commission européenne a choisi de mettre en place un règlement européen et non plus une directive. Cela signifie que le texte sera directement applicable dans toute l'Union européenne et ne laissera aucune place à l'interprétation.

Le projet de règlement européen vise trois objectifs.

Il s'agit d'abord de permettre aux citoyens de renforcer leurs droits déjà existants dans les textes précédents, et surtout de leur permettre de mieux les exercer. Les propositions de la Commission européenne sont conçues pour garantir la protection des informations personnelles des citoyens - quel que soit le lieu où elles sont envoyées ou conservées – même en dehors de l'Union européenne, comme cela peut souvent être le cas sur Internet. Cela vaut donc également pour des sociétés comme Google ou Facebook, basées aux Etats-Unis. Parmi les nouveautés, on trouve le droit à l'oubli numérique ou la protection renforcée des mineurs, ainsi que la possibilité d'interdire le profilage des données. Les citoyens pourront notamment obtenir la suppression de données les concernant si aucun motif légitime ne justifie leur conservation, que ce soit sur un moteur de recherche ou un réseau social. La transparence pour

Attitudes à l'égard de la protection des données

- À peine plus d'un quart des utilisateurs de réseaux sociaux (26%) et une part encore moindre des acheteurs en ligne (18%) ont le sentiment de contrôler pleinement l'utilisation de leurs données à caractère personnel.
- 74% des Européens considèrent que la communication d'informations personnelles prend une part de plus en plus grande dans la vie moderne.
- 43% des internautes déclarent qu'il leur a parfois été demandé plus d'informations personnelles que nécessaire.
- Un tiers seulement des Européens savent qu'il existe une autorité publique nationale responsable de la protection des données (33%).
- 90% des Européens veulent que les mêmes droits à la protection des données soient respectés dans l'ensemble de l'Union.

Eurobaromètre spécial 359
Attitudes on Data Protection and Electronic Identity in the European Union (Attitudes à l'égard de la protection des données et de l'identité électronique au sein de l'Union européenne), juin 2011

mieux accéder à ses propres données et le principe de finalité sont aussi mieux encadrés.

Le deuxième objectif est de renforcer la responsabilité et l'obligation de rendre compte des acteurs qui gèrent la collecte de données. Ainsi, les entreprises et organisations devront signaler toute violation grave de données dans les meilleurs délais, et dans la mesure du possible dans les 24 heures. Le non-respect de ces règles peut entraîner des amendes jusqu'à 1 million d'euros ou 2% du chiffre d'affaires annuel d'une entreprise. Elles devront également faire des évaluations de risques sur les données qu'elles utilisent (un travail effectué auparavant par les autorités de contrôle), nommer en leur sein des responsables à la protection des données et intégrer les principes de la vie privée dès la conception (« privacy by design ») et par défaut (« privacy by default »). Les paramètres de confidentialité devraient être configurés de manière restrictive dès l'inscription à un service en ligne. De plus, les contraintes administratives inutiles, comme les obligations de notification qui incombent aux entreprises, seront supprimées.

Avec le nouveau règlement, les citoyens et les entreprises n'auront plus qu'une seule autorité nationale comme interlocuteur (« guichet unique »). Les citoyens pourront ainsi s'adresser à leur autorité nationale, même quand leurs données à caractère personnel sont traitées en dehors de leur pays d'origine. Les entreprises n'auront à traiter qu'avec l'autorité de contrôle du pays de l'Union où se trouve leur siège principal. Le troisième objectif consiste à renforcer les compétences des autorités nationales responsables de la protection des données, afin qu'elles puissent mieux faire appliquer les règles de l'Union européenne dans leur pays. Au Luxembourg, cette initiative européenne aura une influence importante sur le fonctionnement de la Commission nationale et sur les citoyens. La Commission nationale pourra ainsi infliger des amendes, mais elle devra aussi être en mesure de collaborer efficacement avec les entreprises qui traitent des données à caractère personnel. Étant donné que les autorités de chaque pays seront chargées de centraliser les plaintes de leurs ressortissants, même si elles visent une entreprise qui ne se trouve pas sur leur territoire, le règlement demandera une collaboration plus étroite entre les différentes autorités nationales. Celles-ci seront chapeautées par une autorité européenne, le « European Data Protection Board ».

4 Perspectives

Les attentes des citoyens à l'égard de la Commission nationale pour faire appliquer la loi vont être beaucoup plus importantes.

Le projet de règlement doit encore passer plusieurs étapes législatives avant d'être validé et il pourrait s'appliquer au plus tôt dans deux ans. Les propositions de la Commission européenne seront transmises au Parlement européen et aux États membres de l'UE (qui se réunissent au sein du Conseil de ministres) pour y être examinées et débattues.

La modernisation du cadre légal européen sera également un des sujets principaux de la prochaine « Spring Conference ». Les 3 et 4 mai 2012 se tiendra à Luxembourg la conférence annuelle qui réunit traditionnellement au printemps les représentants des autorités de protection des données de l'Union européenne et d'une douzaine de pays non-membres ainsi que du Conseil de l'Europe, de l'OCDE et de la Commission européenne. L'organisation de cette conférence sera sans doute un des défis majeurs pour la Commission nationale en 2012.

L'année 2012 sera aussi marquée par le changement et le renouveau pour l'équipe de la Commission nationale, qui pourra emménager à la fin de l'année dans ses locaux définitifs à Esch-Belval et verra son équipe renforcée avec l'arrivée d'un spécialiste en informatique.

5 Ressources, structures et fonctionnement de la Commission nationale

5.1 Rapport de gestion relatif aux comptes de l'exercice 2011

Dépenses de fonctionnement

Le total des frais de fonctionnement supportés par l'établissement public au cours de l'exercice 2011 s'élève à 1.559.668,68€. Cela représente une augmentation par rapport à l'exercice précédent de 4.08% et reste en dessous des prévisions budgétaires.

Les charges relatives au personnel permanent n'ont pas atteint les prévisions, étant donné que la Commission nationale a dû recourir à des prestations d'experts, à défaut de disposer des ressources spécialisées nécessaires en interne, notamment dans des domaines comportant des aspects technologiques et informatiques complexes. Cependant, il aurait sans doute été préférable pour la continuité du service, d'acquérir et de conserver depuis 2002 les compétences afférentes au sein de l'établissement public. Les prévisions budgétaires prévoyaient un renforcement en personnel, mais qui n'a reçu l'aval du CER (un poste d'ingénieur-informaticien) qu'en novembre 2011.

Parmi les dépenses d'honoraires et frais d'experts et de prestataires externes pour un montant de 176.308,62€ figurent également les honoraires d'avocats et factures de la fiduciaire qui tient la comptabilité et établit le bilan de l'établissement public.
Les loyers et charges locatives relatifs aux locaux provisoires de la CNPD (pris en location dans l'attente de son implantation dans le 1er bâtiment administratif en construction par l'Etat à Belval-Ouest) s'élevant à 105.552,23€ sont restés conformes aux estimations budgétaires.

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

Les frais de déplacement et de séjour à l'étranger se chiffrent à 22.579,92€. Ils sont relatifs à la participation des membres effectifs et les collaborateurs 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 de 48.222,82€ sont restées quelque peu en dessous de nos

prévisions, 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 2011 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. La veille de cette journée européenne de la protection des données, la Commission nationale avait organisé une conférence suivie d'une table ronde sur le thème *« Y a-t-il encore une vie privée sur Internet ? »*.

A défaut de disposer des ressources spécialisées nécessaires en interne pour la gestion et la maintenance des systèmes et réseaux informatiques, ces frais d'un montant de 28.709,13€ ont dépassé nos prévisions budgétaires.

Les amortissements comptabilisés en 2011 atteignent un montant total de 9.494,06€. Ils concernaient pour l'essentiel le mobilier et les équipements informatiques, ainsi que les 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 à l'optimisation des procédures administratives.

Recettes

Le montant des redevances, perçues en application des articles 37 paragraphe (4) et 13 paragraphe (4) de la loi s'élevant à 62.075,00€, est resté quelque peu en dessous de nos prévisions. En outre, des produits financiers (intérêts créditeurs) ont été enregistrés à hauteur de 3514,49€.

Résultat d'exploitation

Compte tenu de la dotation annuelle de 1.494.700€ dont la Commission nationale a bénéficié en 2011 de la part de l'Etat en application de l'article 37 paragraphe (4) de la loi, le résultat d'exploitation de l'établissement public s'établit à 620,81€ au 31 décembre 2011. Il sera reporté sur l'exercice suivant.

5 Ressources, structures et fonctionnement de la Commission nationale

5.2 Personnel et services

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
Dr. Franziska BOEHM,
juriste

Tenue du registre public et prise en charge administrative des notifications et demandes d'autorisations
Thomas FRERES,
chef de bureau adjoint
Marc MOSTERT,
chef de bureau adjoint

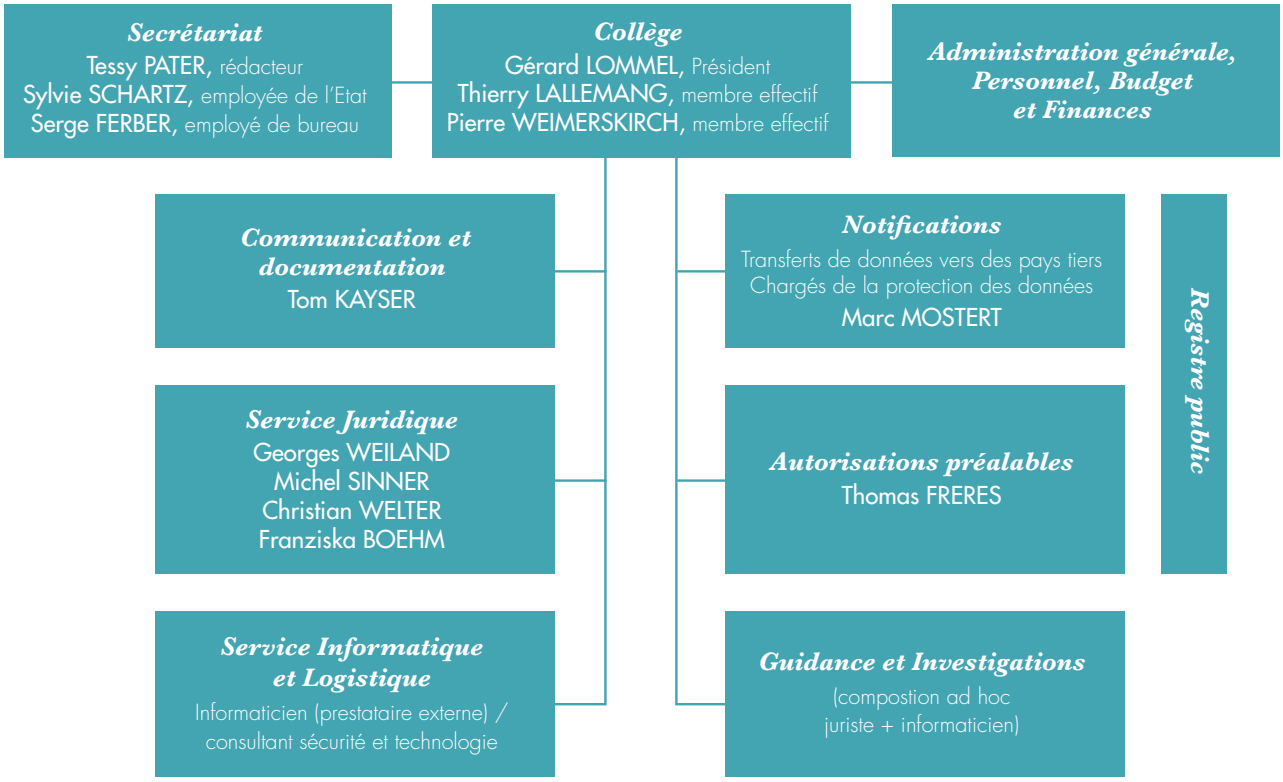
Service informatique et de la logistique
Informaticien (prestataire externe)
Consultant technologies et sécurité (prestataire externe)

Secrétariat, administration générale et finances
Tessy PATER,
rédacteur
Sylvie SCHARTZ,
employée de l'Etat
Serge FERBER,
employé administratif

Service communication et documentation
Tom KAYSER,
attaché de direction

De gauche à droite : Marc MOSTERT, Tessy PATER, Tom KAYSER, Thomas FRERES, Christian WELTER, Michel SINNER, Gwenaëlle DETROUX, Georges WEILAND et Serge FERBER

5.3 Organigramme de la Commission nationale



6 La Commission nationale en chiffres

Formalités préalables

	2003	2004	2005	2006	2007	2008	2009	2010	2011	
a) Notifications										TOTAL
Notifications ordinaires	2.646	850	500	250	760	385	345	295	355	6.386
Notifications simplifiées	750	900	720	890	537	-	-	-	-	3.797
Engagements de conformité	-	-	-	-	-	942	227	15	46	1.230
(Total a)	3.396	1.750	1.220	1.140	1.297	1.327	572	310	401	11.413
b) Autorisations préalables										TOTAL
Demandes d'autorisation	765	406	317	295	392	606	542	607	604	4.534
Engagements de conformité	718	14	17	19	151	220	70	92	49	1.350
(Total b)	1.483	420	334	314	543	826	612	699	653	5.884
(Total général a + b)	4.879	2.170	1.554	1.454	1.840	2.153	1.184	1.009	1.054	17.297
Déclarants (responsables ayant accompli des formalités)	2.220	2.500	2.850	3.300	3.754	4.357	4.772	5.110	5.399	

Demandes de renseignements

	2004	2005	2006	2007	2008	2009	2010	2011
a) Demandes de renseignements par courrier								
- administrations publiques	18	7	8	6	5	11	0	2
- entreprises	49	10	8	5	12	8	14	9
- professions libérales	3	4	9	2	2	2	2	1
- citoyens	12	9	7	12	8	6	3	4
- associations	7	5	2	4	3	1	2	2
(Total a)	89	35	34	29	30	28	21	18
b) Demandes de renseignements par courriel								
(Total b)	67	82	116	119	108	110	189	177
c) Demandes de renseignements par fax								
(Total c)							3	2
d) Demandes de renseignements par téléphone								
(Total d)	1.780	1.550	1.930	1.870	1.586	1.407	1.405	1.634
(Total général a + b + c + d)	1.936	1.667	2.080	2.018	1.724	1.711	1.618	1.831

Plaintes et investigations

	2003	2004	2005	2006	2007	2008	2009	2010	2011
Plaintes, demandes de vérification de licéité et investigations	15	38	40	30	34	63	133	145	115

Séances de délibération

	2004	2005	2006	2007	2008	2009	2010	2011
	39	36	39	40	40	37	38	35

Participations aux groupes de travail sur le plan européen

	2004	2005	2006	2007	2008	2009	2010	2011
	28	33	23	22	22	32	40	37

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

	2004	2005	2006	2007	2008	2009	2010	2011
Secteur public	47	62	32	56	52	54	56	69
Secteur privé	30	38	12	40	44	52	54	71
(Total)	**77**	**100**	**44**	**96**	**96**	**106**	**110**	**140**

Séances d'information, conférences, exposés

	2004	2005	2006	2007	2008	2009	2010	2011
	4	10	11	14	11	23	21	15

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

	2004	2005	2006	2007	2008	2009	2010	2011
Articles et interviews parus dans								
- les quotidiens	14	16	67	127	59	104	202	105
- les hebdomadaires	5	6	4	9	11	10	30	22
- les mensuels	0	7	5	4	2	1	5	4
- les médias audiovisuels	1	3	3	3	16	13	21	7
- Internet							49	36
(Total)	**20**	**32**	**79**	**143**	**88**	**128**	**307**	**174**

7 Annexes

Avis relatif au projet de loi n°5949 relatif aux registres communaux des personnes physiques

Délibération n°11/2011
du 14 février 2011

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 »*.

Bien que n'ayant pas été formellement saisie, la Commission nationale prend un avis d'initiative dans lequel elle expose ses commentaires au sujet du projet de loi n°5949 relatif aux registres communaux des personnes physiques (ci-après : le projet de loi).

Elle salue la mise en place d'un régime uniforme des registres communaux, adapté aux besoins de la société actuelle. La mise en place et la consultation des registres communaux sont des traitements de données à caractère personnel au sens de la loi modifiée du 2 août relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après : la loi du 2 août 2002).

Dans le cadre du projet de loi précité, le bourgmestre, responsable de la tenue des registres communaux, est investi d'une obligation d'information vis-à-vis de ses administrés. A ce titre, ces derniers doivent savoir s'ils sont inscrits sur le registre principal ou sur le registre d'attente et ils doivent être en mesure d'apprécier les droits que confère l'inscription sur l'un ou l'autre registre. La Commission nationale suggère de préciser ces points dans une disposition du projet de loi.

- article 20 du projet de loi

La Commission nationale estime que l'article 20 paragraphe (1) lettre (n) est une disposition vague et imprécise quand il est simplement mentionné que le registre contiendra *« d'autres données nécessaires à l'organisation des services de la commune »*. La Commission nationale propose dès lors de la modifier.

Elle s'interroge aussi sur la nécessité des communes de disposer des données relatives à la profession et à la commune du lieu de travail (article 20 paragraphe (1) lettre (m) du projet de loi). Les auteurs du projet de

loi expliquent dans l'exposé des motifs que ces données sont nécessaires à l'établissement des fiches d'impôt. Or, l'établissement des fiches d'impôt ne fait pas partie des finalités retenues par le dit projet de loi : en effet, les finalités poursuivies sont, au vu de son article 2, l'exécution de la loi électorale et de la loi actuellement en discussion sur l'identification des personnes physiques[1] ainsi que l'organisation des services proposés par les communes.

Il est vrai que ces informations pouvaient s'avérer utiles dans le cadre du recensement fiscal de ses administrés, mission qui lui incombe en vertu du paragraphe 165 de la loi générale des impôts : grâce aux informations collectées et transmises par les communes, les services fiscaux établissaient la fiche d'impôt. Toutefois, la loi du 19 décembre 2008 ayant pour objet la coopération inter-administrative 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[2], précise dans ses articles 10 et 11 que le Centre Commun de la sécurité sociale sera désormais chargé de remettre à l'Administration des contributions directes les informations nécessaires pour l'établissement des fiches de retenue d'impôts, et donc des informations relatives à l'employeur et à l'adresse de cet employeur pour chaque contribuable. Cette mission sera effective à partir de l'année fiscale 2012. L'établissement des fiches de retenue d'impôt n'incombera dès lors plus aux communes, de sorte qu'il ne leur sera plus nécessaire de collecter et de traiter les informations énumérées à l'article 20 paragraphe (1) lettre m) du projet de loi.

Par conséquent, la Commission nationale suggère de supprimer ce point du projet de loi sous examen.

- articles 22 à 25 du projet de loi

La Commission nationale note avec satisfaction que le projet de loi détaille de manière exhaustive le droit d'accès et de rectification du citoyen aux données qui le concernent.

Les articles 22 et 23 du projet de loi présentent en effet les différentes formes de communication, à savoir par voie de courrier ou par voie électronique et exclut toute demande simplement orale. L'article 24 du projet de loi est, pour sa part, consacré aux demandes de rectification des données. L'article 25 du projet de loi est consacré à l'accès à l'historique des consultations. Ce droit d'accès donne un droit de regard concret de la personne sur ses données. Sur ce point la Commission nationale se rallie, dans un souci de clarté, à la proposition de texte émise par le Conseil d'Etat dans son avis du 26 octobre 2010.

- article 26 du projet de loi

Par ailleurs, et tout comme la loi du 2 août 2002, le projet de loi veille à prévoir la possibilité pour les ayants-droit et les représentants légaux ou conventionnels d'avoir communication des données d'une personne. Néanmoins, le projet de loi ne précise pas si ces personnes peuvent également accéder à l'historique des consultations par des tiers. Compte tenu de l'intérêt que présente l'accès à l'historique de consultation, il serait souhaitable que le projet de loi se prononce sur ce point.

- article 27 du projet de loi

Le projet de loi se prononce également sur la communication des données issues des registres communaux à des tiers.

Cet aspect n'est pas, à ce jour, réglé explicitement par un texte légal.

A ce propos, la Commission nationale voudrait relever qu'elle est régulièrement saisie par des communes qui souhaitent savoir quelles suites donner à des demandes de communications

[1] Il s'agit du projet de loi n°5960.
[2] Memorial A n°206 du 24 décembre 2008.

Annexes

d'adresse formulées par des tiers. Elle est également saisie par des particuliers qui souhaitent s'opposer à la communication de leurs données, notamment dans le cadre de mesures d'éloignement de leur conjoint. Jusqu'alors, la Commission nationale se référait aux règles générales régissant la matière de la protection des données pour répondre à ces questions et faisait sienne la position à ce sujet de la Commission consultative instituée par la loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques dans son avis du 9 novembre 1984[3].

Cette Commission consultative avait, en son temps, déjà accepté le principe selon lequel toute personne était en droit d'obtenir des renseignements ponctuelles auprès des communes sur un administré. La Commission nationale a pour sa part toujours suivi cette position, à condition que le demandeur puisse justifier d'un intérêt légitime et qu'il détaille ainsi dans sa demande les raisons pour lesquelles il a besoin d'obtenir ces informations.

Le projet de loi se propose de régler cette question différemment. L'article 27 paragraphe (2) du projet de loi prévoit en effet que « *sur injonction du tribunal de paix territorialement compétent, le bourgmestre est tenu de fournir à tout requérant les renseignements qu'il possède permettant de déterminer la résidence habituelle d'une personne inscrite sur le registre communal* ».

Si le contrôle du juge présente l'avantage de donner un maximum de garanties et d'impartialité, il n'en reste pas moins qu'il nécessite l'accomplissement d'une procédure qui semble excessive d'exiger de la part de certains professionnels. La Commission nationale considère dès lors, qu'il aurait été souhaitable que le projet de loi prévoirait des exceptions en fonction de la qualité ou de la fonction des demandeurs. A titre d'exemple, la loi belge du 8 août 1983 organisant un registre national des personnes physiques liste dans son article 5 les professions pouvant obtenir les informations et dans quelles finalités.

En effet, certaines professions ont besoin dans le cadre de leurs fonctions et de leurs obligations professionnelles, de disposer régulièrement de données d'identification précises et de l'adresse officielle de personnes. Ainsi, la Commission nationale estime par exemple que les officiers ministériels et les auxiliaires de justice ont besoin de disposer de données mises à jour et correctes afin d'établir ou de signifier des actes officiels, respectivement des actes judiciaires.

[3] Avis relatif à la demande d'interprétation émanant du Ministère de l'Intérieur concernant la mise à la disposition de tiers des données personnelles des administrés détenues par les communes.

Elle constate, par ailleurs, que le projet de loi ne contient pas de disposition relative au droit d'opposition à la communication de données à des tiers. Au vu de la rédaction du projet de loi, il n'est pas possible de s'opposer à ce que son adresse soit communiquée à un tiers. Ainsi, une personne protégée par une mesure d'éloignement pourrait, par exemple, voir son adresse communiquée à l'auteur de ses violences. Par conséquent, la Commission nationale propose que le projet de loi introduise expressément un tel droit d'opposition des personnes concernant la communication de leurs données à des tiers. En effet, le droit d'opposition prévu à l'article 30 (1) de la loi modifiée du 2 août 2002 ne peut pas être exercé lorsqu'une disposition légale prévoit expressément un traitement. En outre, que ce soit moyennant l'autorisation du juge ou sur base d'une exception légale introduite en faveur de certaines professions il nous semble que la communication des renseignements aux tiers justifiant d'un intérêt légitime serait plus utilement à prévoir au niveau du service ayant en charge le registre national des personnes physiques au lieu des communes.

- article 29 du projet de loi

Ensuite, la Commission nationale salue la disposition du projet de loi qui pose le principe de l'interdiction de la remise d'informations sur une liste d'administrés. Si elle conçoit parfaitement la possibilité de prévoir des dérogations à cette interdiction, elle se demande toutefois quelles sont les raisons pour lesquelles cette dérogation bénéficie, comme le décrit l'article 30 du projet de loi, *« aux personnes morales de droit luxembourgeois remplissant des missions d'intérêt général et aux autorités étrangères, moyennant l'accord préalable du ministre ayant les affaires étrangères dans ses attributions »*. La Commission nationale s'interroge aussi sur l'intérêt de cette disposition. L'exposé des motifs ne donne pas de précision sur les raisons de la communication d'informations sur des listes d'administrés à des personnes morales ou à des autorités étrangères.

Ainsi décidé à Luxembourg en date du 14 février 2011.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

Avis relatif au projet de règlement grand-ducal modifiant 1. le règlement grand-ducal modifié du 5 septembre 2008 portant exécution de certaines dispositions relatives aux formalités administratives prévues par la loi du 29 août 2008 sur la libre circulation des personnes et l'immigration ; 2. le règlement grand-ducal du 26 septembre 2008 portant création des traitements de données à caractère personnel nécessaires à l'exécution de la loi du 29 août 2008 sur la libre circulation des personnes et l'immigration et déterminant les données à caractère personnel auxquelles le ministre ayant l'immigration dans ses attributions peut accéder aux fins d'effectuer les contrôles prévus par la loi

Délibération n°124/2011
du 12 avril 2011

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

7 Annexes

« 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 28 mars 2011, Monsieur le Ministre du Travail, de l'Emploi et de l'Immigration a invité la Commission nationale à se prononcer au sujet du projet de règlement grand-ducal modifiant 1. le règlement grand-ducal modifié du 5 septembre 2008 portant exécution de certaines dispositions relatives aux formalités administratives prévues par la loi du 29 août 2008 sur la libre circulation des personnes et l'immigration ; 2. le règlement grand-ducal du 26 septembre 2008 portant création des traitements de données à caractère personnel nécessaires à l'exécution de la loi du 29 août 2008 sur la libre circulation des personnes et l'immigration et déterminant les données à caractère personnel auxquelles le ministre ayant l'immigration dans ses attributions peut accéder aux fins d'effectuer les contrôles prévus par la loi.

Le projet opère certaines modifications aux règlements grand-ducaux mentionnés ci-avant. Il prévoit notamment d'introduire un nouvel alinéa 2 à l'article 1er paragraphe (2) du prédit règlement grand-ducal du 26 septembre 2008 qui précise que les données biométriques collectées pour la confection du titre de séjour sont conservées dans un fichier temporaire et que celles-ci sont effacées une fois que le titre de séjour a été délivré au bénéficiaire, ou au plus tard six mois après la production du titre.

Le libellé de la disposition en question correspond au souci de la Commission nationale que des données biométriques ne figurent pas de manière pérenne dans une base de données. Ainsi, dans la mesure où le texte en projet précise que les données biométriques ne sont stockées que temporairement dans un fichier, la Commission nationale n'a pas d'autres observations particulières à formuler.

Ainsi décidé à Luxembourg en date du 12 avril 2011.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

Avis relatif à l'article 32 du projet de loi n°6158 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales

Délibération n°125/2011
du 15 avril 2011

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 courriel du 18 mars 2011, Madame le Ministre des Classes moyennes a invité la Commission nationale pour la protection des données à se prononcer au sujet du projet de loi réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales, en particulier au sujet des dispositions de son article 32. Aux termes de cet article, le Ministre ayant dans ses attributions les autorisations d'établissement tient un registre relatif aux autorisations délivrées, leurs modifications, annulations, révocations etc., spécifiant notamment les activités que l'entreprise du titulaire est en droit d'exercer.

La Commission nationale n'entend pas prendre position à l'égard des réserves exprimées dans son avis par le Conseil d'Etat au sujet de la publication des informations de ce registre et aux conditions pour lesquelles le Ministre peut limiter cette publicité. La question de savoir si rendre public les données mentionnées de ce registre constitue un double emploi avec celles accessibles au public à travers le Registre de Commerce et des Sociétés ne relève pas des libertés et droits fondamentaux des individus, notamment de la protection des données à caractère personnel mais plutôt du choix au niveau de l'accent mis sur une politique de transparence dans le domaine commercial et artisanal et de choix au niveau de l'organisation des pouvoirs publics compétents en la matière.

Il apparaît que les motifs de limitation de la publicité des informations personnelles sont repris dans l'article 15 de la loi modifiée du 2 août 2002 sur la protection des données et issus directement de la directive 95/46/CE qu'elle transpose. Les auteurs du projet de loi se sont donc manifestement inspirés pour justifier des exceptions au principe de transparence du catalogue des cas de figure dans lesquels la Commission nationale peut limiter pour des raisons prépondérantes la publicité faite aux traitements des données qui lui sont déclarés.

Accès du Ministère des Classes moyennes aux données de certains fichiers publics

Le paragraphe (2) dudit article 32 du projet de loi prévoit la possibilité pour le Ministre de s'entourer de toutes les informations utiles requises en vue d'apprécier si une entreprise satisfait aux exigences de la loi et de ses règlements d'exécution, notamment des informations contenues dans les fichiers publics énumérés sub a) à h). Pour obtenir ces renseignements le texte sous revue prévoit que le Ministre ayant les autorisations d'établissement dans ses attributions « peut accéder y compris par un système informatique direct aux traitements de données à caractère personnel » énumérés.

Le dernier alinéa dudit paragraphe (2) précise que les procédés automatisés se font moyennant interconnexion ou consultation de données à travers un accès direct à ces fichiers de données à caractère personnel et sous la garantie que l'accès soit sécurisé, limité et contrôlé. Les conditions, critères et modalités de l'échange sont déterminés par règlement grand-ducal.

7 Annexes

Il y a lieu de remarquer que le libellé reprend mot pour mot celui de l'article 4 de la loi du 19 décembre 2008 ayant pour objet 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 (Memorial A 206 du 24 septembre 2008).

S'il est vrai que la Commission nationale avait avisé favorablement le projet de loi ayant introduit cette disposition, il convient d'observer qu'il vise (du moins pour ce qui est de ses chapitres I et II) un échange de données bilatéral entre administrations dont l'activité se situe dans le même domaine à savoir celui des impôts et de la taxation placé sous l'autorité du Ministre des Finances.

En l'espèce les traitements de données accédés sont opérés par différentes administrations dont les activités se situent dans des domaines variables et correspondent à un intérêt public distinct de celui du Ministre ayant les autorisations d'établissement dans ses attributions. En revanche, l'objectif poursuivi par le présent projet de loi ne nécessite ni échange bidirectionnel avec les fichiers publics énumérés ni interconnexion des données à caractère personnel.

La Commission nationale se rallie dès lors à l'avis du Conseil d'Etat qui s'oppose à l'interconnexion et préconise de restreindre la faculté ouverte au Ministère des Classes moyennes à l'établissement d'une communication sur demande ou d'une consultation à travers un accès direct par des procédés automatisés.

La Commission nationale se félicite dès lors de la suppression envisagée par le gouvernement du terme « interconnexion » dans le libellé du dernier alinéa du 2e paragraphe. Pour assurer que toutes les hypothèses techniques soient couvertes, elle suggère néanmoins d'insérer les termes de « transmission sur demande ou » devant ceux de « consultation de données à travers un accès direct ». Cette formulation laissera une plus grande flexibilité dans la mise en œuvre technique et est en ligne avec celle employée aux articles 9, 10, 11 et 16 de ladite loi sur la coopération interadministrative entre administrations fiscales.

Des termes semblables se retrouvent d'ailleurs également dans la loi du 5 juin 2009 relative à l'accès des autorités judiciaires, de la Police, 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 (Memorial A 135 du 16 juin 2009) et dans celle portant sur la libre circulation des

personnes et de l'immigration du 29 août 2008 (Memorial A 138 du 10 septembre 2008) qui ne prévoient pas que la transmission ou consultation de données par des procédés automatisés à travers un accès informatique direct revêtent les caractéristiques de l'interconnexion de données à caractère personnel.

Ce dernier texte précise en outre au dernier alinéa de l'article 138 que « 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 ». Une telle disposition assurant la traçabilité des accès aux données des fichiers publics constituerait à nos yeux une bonne garantie contre d'éventuels abus de sorte qu'il serait recommandable de l'insérer également dans le présent projet de loi.

Pour ce qui est des conditions, critères et modalités d'application, il est renvoyé aux dispositions d'un règlement grand-ducal à prendre.

Le règlement grand-ducal du 26 septembre 2008 pris en exécution de la loi du 29 août 2008 sur la libre circulation des personnes et l'immigration et déterminant les données à caractère personnel auxquelles le Ministre ayant l'immigration dans ses attributions peut accéder aux fins d'effectuer les contrôles prévus par la loi (Memorial A 145 du 29 septembre 2008) constitue un précédent illustrant une manière appropriée de déterminer de façon claire et limitative les accès justifiés au regard des critères de nécessité et proportionnalité par la finalité légitime inscrite dans la loi visée et l'objet de contrôles ponctuels en vue de prévenir d'éventuels abus.

Pour le surplus la Commission nationale se félicite que l'accord donné préalablement par l'administré concerné soit désormais inscrit formellement comme condition de l'accès (visé sub g) au fichier du casier judiciaire. Même dans ces circonstances et bien que limité au bulletin n°2, un tel accès automatisé au casier judiciaire constitue cas de figure où la priorité donnée au souci de simplification administrative ne va pas sans laisser subsister des interrogations quant à la préservation de la protection de la vie privée.

<u>Accès de certains organismes et administrations publics au registre des autorisations d'établissement</u>

Le paragraphe 3 du projet initial énumère un certain nombre d'organismes et d'administrations publics pour lesquels il prévoit l'accès à certaines données du registre des autorisations d'établissement en vue de faciliter l'exercice de leurs attributions.

Dans son avis le Conseil d'Etat propose la suppression pure et simple de ce paragraphe 3 au motif notamment que pour un certain nombre d'acteurs l'accès au fichier des autorisations d'établissement résulte d'ores et déjà d'autres textes et que l'interconnexion à des données d'autres administrations soulève des interrogations de principe.

La Commission nationale est sensible à ces arguments et se félicite dès lors de l'intention du gouvernement de proposer la suppression pure et simple dudit paragraphe.

Ainsi décidé à Luxembourg en date du 15 avril 2011.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

7 Annexes

Avis concernant l'avant-projet de loi portant sur l'exploitation d'une base de données à caractère personnel relative aux élèves et à l'avant-projet de règlement grand-ducal pris en exécution de la loi du … portant sur l'exploitation d'une base de données à caractère personnel relative aux élèves

Délibération n°126/2011
du 15 avril 2011

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 (ci-après « la Commission nationale ») a notamment pour mission d'*« être demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi »*.

En date du 3 août 2009, Madame le Ministre de l'Éducation nationale et de la Formation professionnelle avait consulté la Commission nationale dans le cadre d'un avant-projet de règlement grand-ducal déterminant les conditions, les critères et les modalités de l'échange de données à caractère personnel entre l'administration de l'éducation nationale et les établissements scolaires, les autorités communales et des tiers. La Commission nationale s'était exprimée à ce sujet dans son avis du 26 juillet 2010.

Par son courrier du 4 avril 2011, Madame le Ministre de l'Éducation nationale et de la Formation professionnelle a saisi la Commission nationale d'un avant-projet de loi portant sur l'exploitation d'une base de données à caractère personnel relative aux élèves ainsi que d'un avant-projet de règlement grand-ducal pris en exécution de la loi du … portant sur l'exploitation d'une base de données à caractère personnel relative aux élèves.

La Commission nationale voudrait relever d'emblée que les textes sous examen reprennent dans une large mesure les observations formulées dans son avis du 26 juillet 2010 (délibération n°238/2010) et elle s'en félicite. La Commission nationale note également avec satisfaction que Madame le Ministre s'est résolue à présenter son projet sous la forme d'une loi accompagnée d'un règlement grand-ducal.

Dans la continuité de l'analyse effectuée dans son précédent avis, la Commission nationale

voudrait néanmoins réitérer ses réserves à l'égard de la communication de données non dépersonnalisées à l'Université du Luxembourg *« aux fins de réaliser des collectes de données pour le suivi longitudinal des élèves, des évaluations externes et des travaux de recherche commandités »* (article 6 alinéa 1er lettre n) de l'avant-projet de loi). Elle émet plus particulièrement des réserves quant au libellé qu'elle estime trop général et pas assez restrictif en vue d'éviter tout risque d'abus. Pour le surplus, elle renvoie aux observations faites au point 7.1. *« le traitement ultérieur de données à des fins de recherches statistiques ou scientifiques par des tiers »* dans son avis du 26 juillet 2010.

Ensuite, la Commission nationale suggère de modifier de la manière suivante l'alinéa 2 de l'article 9 de l'avant-projet de loi afin que les exigences de standards de sécurisation élevés soient également appliquées aux activités de communication visées à l'article 6 :

« La technologie utilisée pour la collecte, le traitement et la communication de données à caractère personnel est sécurisée et protégée par un système d'identification et d'authentification individuelle des utilisateurs ».

Enfin, la Commission nationale voudrait formuler quelques remarques au sujet de la nouvelle disposition relative aux partenariats pour la recherche prévue à l'article 7 de l'avant-projet de loi.

D'un point de vue formel, la Commission nationale propose de modifier l'agencement des dispositions de l'avant-projet de loi, en faisant précéder l'article 8 de l'article 7 ou, le cas échéant, de fusionner ces deux articles en faisant de l'article 7 un second paragraphe de l'article 8.

Afin d'éviter tout risque d'atteinte à la vie privée des personnes, les principes de la protection des données requièrent l'usage de procédés d'anonymisation en cas de traitements ultérieurs de données à des fins de recherches scientifiques ou d'analyses statistiques.

Toutefois, il arrive que pour les besoins de tel ou tel projet d'étude ou de recherche, la dépersonnalisation des données n'aboutit pas toujours à une anonymisation irréversible, de sorte qu'il peut subsister un risque de réidentification des données. Dans ce cas, le traitement n'échappe pas aux prescrits de la loi du 2 août 2002. Dès lors, dans l'hypothèse de partenariats entre le ministère et des partenaires étrangers, établis dans des pays non membres de l'Union européenne, le transfert de données ne pourra avoir lieu que dans le respect des conditions édictées aux articles 18 et 19 de la loi du 2 août 2002.

En ce qui concerne l'avant-projet de règlement grand-ducal sous examen, celui-ci n'appelle pas de commentaires de notre part.

Ainsi décidé à Luxembourg en date du 15 avril 2011.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

7 Annexes

Avis concernant le projet de règlement grand-ducal fixant les conditions d'application et modalités d'exécution relatives au contrat d'accueil et d'intégration

Délibération n°145/2011
du 6 mai 2011

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 « la loi modifiée du 2 août 2002 »), la Commission nationale pour la protection des données (ci-après « la Commission nationale ») a notamment pour mission d'*« être demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi »*.

C'est dans cette optique, et faisant suite à la demande lui adressée par Madame Christiane MARTIN, Directrice de l'Office Luxembourgeois de l'Accueil et de l'Intégration (ci-après « OLAI ») en date du 9 décembre 2010 que la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet du projet de règlement grand-ducal pré-mentionné.

La Commission nationale entend limiter son avis aux dispositions traitant des aspects de la protection des données, à savoir les dispositions du chapitre sept du projet de règlement grand-ducal sous examen fixant les conditions d'application et modalités d'exécution relatives au contrat d'accueil et d'intégration et modifiant divers réglements grand-ducaux.

Le projet de texte sous analyse poursuit deux objectifs, dont le premier consiste à doter l'OLAI d'un outil permettant d'identifier les étrangers remplissant certaines conditions légales pour se voir proposer un contrat d'accueil et d'intégration. Pour ce faire, le projet de règlement grand-ducal prévoit notamment que l'OLAI extrait certaines données à caractère personnel contenues dans la base de données relative à l'entrée et au séjour des étrangers sur le territoire[4].
Le deuxième objectif consiste à alimenter de données à caractère personnel un fichier tenu auprès de l'OLAI, qui doit permettre d'une part de faire une sélection des candidats potentiels et d'autre part d'effectuer le suivi effectif des mesures proposées aux candidats signataires.

Légitimité

Suivant les dispositions de l'article 5 de la loi modifiée du 2 août 2002, un traitement de données ne peut être effectué que s'il

[4] Base de données définie à l'article 1er, paragraphe (2) du règlement grand-ducal du 26 septembre 2008 *« portant création de données à caractère personnel nécessaires à l'exécution de la loi du 29 août 2008 sur la libre circulation des personnes et l'immigration et déterminant les données à caractère personnel auxquelles le ministre ayant l'immigration dans ses attributions peut accéder aux fins d'effectuer les contrôles par la loi »*.

correspond à l'une des conditions de légitimité limitativement énumérées dans son paragraphe (1).

Il ressort des dispositions de la loi du 16 décembre 2008 *« concernant l'accueil et l'intégration des étrangers au Grand-Duché de Luxembourg »* ainsi que du projet de règlement sous analyse que la finalité principale poursuivie par le contrat d'accueil et d'intégration est de favoriser une meilleure intégration des étrangers dans la société contemporaine luxembourgeoise. Une intégration rapide est un facteur qui contribue à la fois à un renforcement de la cohésion sociale et à une augmentation du bien-être des étrangers au sein de la société. L'intégration des étrangers, telle que définie à l'article 2 de la loi précitée, peut donc être considérée comme relevant de l'intérêt public.
Les traitements de données à caractère personnel effectués dans le cadre du présent projet peuvent dès lors être considérés comme légitimes, car nécessaires à l'exécution d'une mission d'intérêt public dont est investi le responsable du traitement.

Au vu des traitements de données envisagés par le projet de règlement grand-ducal sous examen et par application des principes de nécessité et de proportionnalité inscrits dans l'article 4 de la loi modifiée du 2 août 2002, la Commission nationale estime qu'il y a lieu d'analyser, d'une part, s'il existe des limitations de l'accès des agents de l'OLAI à la base de données relative à l'entrée et au séjour des étrangers sur le territoire et, d'autre part, si les catégories de données traitées par l'OLAI sont limitées au strict minimum nécessaire.

Accès à la base de données de l'immigration

Le règlement grand-ducal prémentionné du 26 septembre 2008 limite les personnes qui ont accès à la base de données relative à l'entrée et au séjour des étrangers sur le territoire. Plus précisément, l'accès aux données en question est exclusivement réservé aux agents du service des étrangers du Ministère des Affaires Etrangères, dans le cadre de leurs mission relatives à la libre circulation et l'immigration.

Si l'intérêt public poursuivi par l'OLAI (administration créée sous l'autorité du Ministère de la Famille et de l'Intégration) est intimement lié à l'intérêt public poursuivi par le service des étrangers auprès du Ministère des Affaires Etrangères, toujours est-il que les compétences administratives sont réparties sur deux ministères différents.

Dès lors, la Commission nationale se pose la question s'il ne faudrait pas modifier le règlement du 26 septembre 2008, afin d'intégrer le directeur de l'OLAI – et les agents autorisés par ce dernier - dans la liste des agents autorisés à avoir accès au fichier et à effectuer certains traitements.

Le fichier contenant les données personnelles des candidats signataires

Les traitements de données à caractère personnel envisagés par l'OLAI trouvent leur base légale dans la loi du 16 décembre 2008 précitée et correspondent à l'intérêt public consistant à intégrer au mieux les étrangers dans la société.

L'OLAI, en tant que responsable du traitement, tient un fichier contenant certaines catégories de données à caractère personnel relatives aux candidats signataires, nécessaires à la mise en œuvre et la gestion du contrat d'accueil et d'intégration.

Suivant les dispositions de l'article 4 paragraphe (1) lettre (a) de la loi modifiée du 2 août 2002, l'utilisation des données traitées doit se limiter aux finalités pour lesquelles elles ont été collectées. Les données doivent également être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées.
La finalité du traitement envisagé est la gestion des données et le

suivi administratif des dossiers des étrangers. Le traitement des données est nécessaire afin de garantir le suivi de la mission légale dont est investi le responsable du traitement.

L'article 27 du projet énumère les différentes catégories de données des candidats signataires d'un contrat d'accueil et d'intégration qui sont enregistrées dans un fichier de l'OLAI.

La Commission nationale estime qu'il faudrait limiter avec précision les données à caractère personnel qui seront enregistrées dans les catégories suivantes : « *situation professionnelle* » et « *situation financière* ». En effet, ces catégories sont tellement larges de manière à pouvoir faire état de catégories « fourre-tout ». Par exemple, en ce qui concerne la catégorie « *situation financière* », est-ce que le candidat signataire doit-il justifier de ses moyens (p.ex. fiches de paie), faire état de ses prêts, etc. ou uniquement justifier d'un revenu de subsistance propre ? La même observation vaut en ce qui concerne les données sur la « *situation professionnelle* ».

Dès lors, la Commission nationale suggère de préciser au début de l'article 27 la finalité du fichier et de prévoir une énumération claire et concise des données à caractère personnel enregistrées dans les catégories précitées. Dans la mesure où ces précisions seraient intégrées dans le projet sous analyse, les dispositions de l'article 28, paragraphe (3) et (4) pourraient être supprimées alors qu'elles ne font que reprendre le libellé de l'article 4 paragraphe (1) lettres (a) et (b) de la loi modifiée du 2 août 2002.

Durée de conservation des données

Dans le même ordre d'idées, le paragraphe (5) de l'article 28 ne fait que reprendre textuellement les dispositions relatives à la durée de conservation de la loi modifiée du 2 août 2002, mais ne fixe pas de durée précise de conservation des données.

Suivant l'article 4 paragraphe (1) lettre (d) de la loi modifiée du 2 août 2002 les données personnelles ne doivent pas être conservées pendant une durée qui excède celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées.

Il ressort des dispositions de l'article 9, dernier paragraphe, de la loi du 16 décembre 2008 concernant l'accueil et l'intégration des étrangers au Grand-Duché de Luxembourg, ainsi que de l'article 4 du projet de règlement grand-ducal sous analyse, que la durée maximale du contrat d'accueil et d'intégration est de deux ans. La finalité du traitement étant

la gestion et le suivi du dossier administratif des étrangers, les données ne devront pas être conservées plus longtemps que nécessaires à la réalisation de cette finalité.

Pour les candidats qui acceptent de signer le contrat d'accueil et d'intégration, en tenant compte de la durée maximale du contrat d'accueil et d'intégration de deux ans, un délai de conservation maximal de 3 ans (à partir du moment de l'inscription) est suffisant. Au-delà de cette période, les données devront être anonymisées.

La Commission nationale estime par ailleurs nécessaire de distinguer les données enregistrées relatives aux candidats souscrivant au contrat de celles des candidats refusant la proposition de signer un tel contrat.

La Commission nationale est d'avis que les données relatives aux candidats refusant le contrat (c'est-à-dire le nom, les prénoms, la nationalité et l'adresse) devront être supprimées du fichier après un an. Ce délai tiendrait compte de la possibilité pour l'OLAI de proposer éventuellement une nouvelle fois un contrat d'accueil et d'intégration à ces candidats.

La Commission nationale propose dès lors de modifier le paragraphe (5) de l'article 28 comme suit :

« *Art. 28.* …

(5)~~Elles~~ Les données des candidats signataires du contrat d'accueil et d'intégration ne doivent pas être conservées pendant plus de trois ans. ~~une durée qui n'excède pas la période nécessaire aux finalités pour lesquelles elles ont été collectées ou traitées.~~ Au-delà de cette période ~~requise~~, les données doivent être anonymisées. ~~ne peuvent faire l'objet d'une conservation qu'en vue de répondre spécifiquement à un traitement à des fins historiques, statistiques ou de recherches en vue de dispositions légales.~~ Les données des candidats sélectionnés mais non signataires peuvent être conservées pendant un délai d'un an. Passé ce délai, les données à caractère personnel devront être supprimées du fichier tenu auprès de l'OLAI.»

Mesures de sécurité

Selon les dispositions de la loi modifiée du 2 août 2002, il incombe au responsable du traitement de mettre en œuvre des mesures techniques et d'organisation appropriées afin d'assurer la sécurité des traitements qu'il effectue.

Il découle des articles 22 et 23 de la loi modifiée du 2 août 2002 que le responsable du traitement doit notamment prévoir des mesures techniques assurant un accès sécurisé, limité et contrôlé au traitement des données. Le système mis en place doit donc prévoir des mesures permettant l'utilisation d'un login sécurisé, la journalisation et la traçabilité des consultations.

En ce sens, il pourrait être ajouté un article 30 nouveau au projet sous analyse, comme suit :

« *Art. 30.* « *Le système informatique comprenant le fichier des candidats signataires du contrat doit être aménagé de sorte que les informations relatives à l'agent ayant procédé à l'accès ou au traitement, la date, l'heure ainsi que le motif précis de la consultation ou du traitement, puissent être retracés* ».

Ainsi décidé à Luxembourg en date du 6 mai 2011.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

7 Annexes

Avis concernant l'avant-projet de règlement grand-ducal déterminant la procédure de dépôt de la liasse comptable auprès du gestionnaire du registre de commerce et des sociétés, les conditions de contrôles arithmétiques et logiques concernant les comptes annuels et portant modification du règlement grand-ducal modifié du 23 février 2003 portant exécution de la loi du 19 décembre 2002 concernant le registre de commerce et des sociétés ainsi que la comptabilité et les comptes annuels des entreprises

Délibération n°158/2011
du 3 juin 2011

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 « la loi modifiée du 2 août 2002 »), la Commission nationale pour la protection des données (ci-après « la Commission nationale ») a notamment pour mission d'*« être demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi »*.

C'est dans cette optique, et faisant suite à la demande lui adressée par Monsieur François Biltgen, Ministre de la Justice en date du 31 mai 2011 que la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet de l'avant-projet de règlement grand-ducal pré-mentionné.

La Commission nationale n'a pas d'observations à émettre à l'égard de l'avant-projet de règlement grand-ducal déterminant la procédure de dépôt de la liasse comptable auprès du gestionnaire du registre de commerce et des sociétés et portant modification du règlement grand-ducal du 23 février 2003 pris en exécution de la loi du 19 décembre 2002 concernant le registre de commerce et les comptes annuels des entreprises.

Ledit projet définit la procédure de dépôt par voie électronique des documents comptables au RCS et s'inscrit dans le cadre des efforts déployés en matière de simplification administrative.

Elle s'appliquera dans la majorité des cas à des personnes morales dont les documents financiers ont vocation à faire l'objet de la publicité légale prévue. Ceux-ci ne contiendront guère de données relatives à des personnes physiques, si ce n'est l'identité du représentant des organes d'administration et de surveillance et celle du

représentant du réviseur des comptes.

L'utilisation des données comprises dans la liasse comptable visée par l'avant-projet de règlement grand-ducal à des fins autres que la publication n'est pas réglée dans le texte sous examen mais au niveau du règlement grand-ducal de 2003 ou de la loi même de 2002 sur le RC et les comptes annuels.

Les accès aux données concédées dans certaines conditions au Statec et à d'autres administrations étatiques (Contributions directes, Enregistrement et Domaines) feront l'objet d'un règlement grand-ducal ultérieur.

Du point de vue de la protection des données à caractère personnel, il ne reste donc que la question des garanties de la confidentialité (du moins dans le cas où les documents financiers ne font pas l'objet d'une publicité légale en particulier s'agissant de commerçants en noms particuliers) et de sécurisation de la plateforme de dépôt et de la transmission des données.

La consultation des modalités de mise en œuvre (exposé des motifs et pages web e-CDF du CTIE et du RCS) donne suffisamment d'assurances nécessaires de mise en place des mesures appropriées (authentification via LuxTrust).

Une disposition afférente n'est juridiquement pas nécessaire dans le libellé de l'avant-projet puisque les dispositions des articles 22 et 23 de la loi modifiée du 2 août 2002 relatives à la protection des données personnelles sont pleinement applicables.

Le Conseil d'Etat s'est d'ailleurs à plusieurs reprises montré défavorable à voir insérer dans des textes spécifiques des renvois aux dispositions générales de la loi sur la protection des données, estimant que de telles références croisées étaient susceptibles de créer de l'insécurité juridique dans la détermination de la norme applicable (cela d'autant plus si les formulations divergent).

Il ne nous paraît donc pas indiqué de faire référence à la législation de la protection des données dans le projet.

Ainsi décidé à Luxembourg en date du 3 juin 2011.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

Avis relatif au projet de loi n°6237 relatif à la mise en application du Règlement (CE) n°4/2009 du 18 décembre 2008 relatif à la compétence, la loi applicable, la reconnaissance et l'exécution des décisions et la coopération en matière d'obligations alimentaires et modifiant : a) le Nouveau Code de procédure civile et b) la loi modifiée du 10 août 1991 sur la profession d'avocat

Délibération n°159/2011
du 10 juin 2011

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 8 décembre 2010, Monsieur le Ministre de la Justice a invité la Commission nationale à se prononcer au sujet du projet de loi (devenu le projet de loi n°6237, déposé le

7 Annexes

5 janvier 2011) relatif à la mise en application du Règlement (CE) n°4/2009 du 18 décembre 2008 relatif à la compétence, la loi applicable, la reconnaissance et l'exécution des décisions et la coopération en matière d'obligations alimentaires et modifiant : a) le Nouveau Code de procédure civile et b) la loi modifiée du 10 août 1991 sur la profession d'avocat (ci-après : « le projet de loi »).

L'objectif du règlement communautaire est de faciliter au maximum le recouvrement des créances alimentaires lorsque le créancier et le débiteur d'aliments ne résident pas au sein du même État membre. Suivant l'exposé des motifs, la loi projetée permettra de simplifier, d'accélérer et de réduire les coûts du recouvrement des créances résultant d'obligations alimentaires.

Le règlement communautaire prévoit encore des dispositions qui permettent de déterminer la juridiction compétente, la loi applicable et met le créancier d'une obligation alimentaire en mesure de faire reconnaître et exécuter les titres obtenus. A cette fin, il présente un large éventail de mesures et organise une coopération entre les États membres par l'intermédiaire d'autorités centrales.

En effet, chaque Etat membre désigne une autorité centrale qui assiste les parties dans l'établissement et le recouvrement d'une créance alimentaire. Les autorités centrales exercent des fonctions générales et spécifiques. Au titre de leurs fonctions générales, elles coopèrent entre elles et promeuvent la coopération entre les autorités compétentes dans l'application de ce règlement et la résolution des problèmes qui en découlent. Au titre de leurs fonctions spécifiques, les autorités centrales fournissent une assistance aux parties en ce qui concerne les demandes prévues par le règlement, notamment en transmettant et en recevant ces demandes, et en introduisant des procédures visant l'établissement ou la modification de l'obligation alimentaire ou l'exécution d'une décision en la matière.

Chaque État membre mettra donc en place une autorité centrale, dotée de pouvoirs étendus, qui interviendra notamment en vue de l'obtention, la modification et l'exécution d'une décision. Au Luxembourg, le projet de loi prévoit que ce rôle sera attribué au procureur général d'Etat, vu son attribution déjà acquise en tant qu'autorité centrale dans le cadre de la Convention de New-York du 20 juin 1956 sur le recouvrement des aliments à l'étranger.

Le champ d'application du règlement communautaire est vaste : les matières traitées

concernent la compétence, la loi applicable, la reconnaissance, l'exécution et la coopération. La Commission nationale pour la protection des données s'intéresse donc de près à l'aspect le plus novateur du règlement (transposé par le projet de loi) qui consiste dans l'instauration d'un système de coopération administrative (articles 49s. du règlement (CE) n°4/2009) par lequel chaque autorité centrale aura la possibilité de communiquer et de se faire communiquer des informations, par exemple, visant à localiser le débiteur, à évaluer son patrimoine, à identifier son employeur ou son compte bancaire. Il va de soi que ce règlement confie aux autorités centrales, et en l'espèce au procureur général du Luxembourg, des pouvoirs d'investigation particulièrement étendus, d'autant plus que le règlement (CE) n°4/2009 n'est pas limité au recouvrement de créances alimentaires relatives d'époux ou d'ex-époux, mais s'étend également, par exemple, aux créances alimentaires relatives à des enfants, à des parents ou à des grands-parents.

Le procureur général aura ainsi accès à des données à caractère personnel, détenues par différentes administrations et autorités nationales, qui ont été initialement collectées pour des finalités autres que le recouvrement de créances alimentaires pour ensuite être transmises à l'autorité centrale d'un État membre qui les a demandées (et pour ensuite encore être continuées aux autorités judiciaires ou autres autorités compétentes de l'Etat requérant).

Dans un premier temps, étant donné qu'il résulte du projet de loi que le règlement communautaire s'inscrivera dans la ligne des procédures judiciaires applicables au Luxembourg et plus particulièrement parmi les dispositions du Nouveau Code de procédure civile, la Commission nationale estime que les traitements envisagés par ledit règlement rentreront dans le champ d'application de l'article 8 de la loi modifiée du 2 août 2002 qui vise les traitements de données opérés par les autorités judiciaires.

L'article 8 dispose notamment que *« Le traitement des données dans le cadre (…) de procédures judiciaires est opéré dans le respect des dispositions (…) du Code de procédure civile (…) ou d'autres lois ».*

Dans le texte du projet de loi initial (Dossier parlementaire 4735/00, p.100) concernant la protection des données à caractère personnel, le législateur avait souhaité que *« les traitements de données mis en œuvre conformément aux règles de procédures judiciaires ne doivent pas être notifiés. Cela s'impose afin de ne pas perturber le bon déroulement de la justice et alors que le principe du contradictoire, celui du procès équitable remplissent la plupart des fonctions attribuées à la protection des données ».* La Commission des médias et des communications, quant à elle, a retenu (dossier parlementaire 4735/08, p.9) que *« cette disposition vise à permettre aux autorités judiciaires, sur la base d'une disposition légale expresse, d'effectuer des traitements de données en relation avec des enquêtes ou procédures judiciaires en cours. Plutôt que de réglementer ce type de traitement dans la présente loi, il paraît préférable d'effectuer un renvoi au droit commun en matière de procédure (pénale, civile ou administrative) ».* Le Conseil d'Etat a ensuite rappelé, dans le cadre des travaux parlementaires du projet de loi portant modification de la loi du 2 août 2002 (Dossier parlementaire 5554/04, p.10), que les dispositions de l'article 8 signifient *« que le régime de traitement des données dites judiciaires, y compris et notamment les droits des personnes concernées, doit être déterminé dans les différentes lois organisant les procédures devant les juridictions » et que « la conséquence logique de cette analyse est qu'il n'y a plus lieu de faire référence au traitement des données judiciaires*

dans la suite de la loi générale sur la protection des données personnelles, ni en prévoyant « positivement » l'application de certaines dispositions ni en consacrant des dérogations ou exemptions à certaines obligations légales ».

Or, si les traitements de données opérés par les autorités judiciaires échappent à la mission confiée par le législateur à la Commission nationale, il ressort des articles du règlement (CE) n°4/2009, et plus particulièrement des articles 61 à 63, que le législateur communautaire a spécifiquement voulu réserver une certaine importance aux législations nationales de protection des données pour l'application de ces articles. Ainsi, le projet de loi sous examen qui vise à organiser la procédure judiciaire en question, par référence à l'article 8 paragraphe (1) de la loi modifiée du 2 août 2002, devrait donc respecter la ratio legis de la directive 95/46 et de la prédite loi du 2 août 2002.

Dans la pratique, la procédure se résume comme suit : dès l'entrée en vigueur du règlement et de la loi projetée, un créancier pourra déposer une demande auprès de la juridiction compétente et à la demande de cette dernière, l'autorité centrale enverra une demande à l'autorité centrale de l'État membre requis, laquelle réunira les informations demandées et répondra à l'autorité centrale demanderesse, qui transmettra alors les informations à la juridiction qui les avait demandées.

Cet échange de données pourra donc être effectué, mais dans le respect intégral des exigences découlant de la directive 95/46/CE et, à fortiori, de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement de données à caractère personnel.

1) Quant à l'accès des autorités aux informations : article 3 point 2° paragraphe (1) du projet de loi (article 61 du règlement (CE) n°4/2009)

Le projet de loi prévoit, pour la mise en application de l'article 61, que le procureur général d'Etat soit doté d'un accès direct, par le biais d'un système informatique, aux traitements de données à caractère personnel suivants [article 3 paragraphe (2) alinéa (1) du projet de loi] :

a) le registre général des personnes physiques et morales crée par la loi du 30 mai 1979 organisant l'identification numérique des personnes physiques et morales ;
b) les fichiers gérés par le Centre commun de la Sécurité sociale sur base de l'article 413 du Code de la sécurité sociale à l'exclusion de toutes données relatives à la santé ;

c) le fichier des véhicules routiers et de leurs propriétaires et détenteurs, exploité pour le compte du ministère ayant les Transports dans ses attributions ;
d) les fichiers de la documentation patrimoniale détenus par l'Administration du Cadastre et de la Topographie, exploités pour le compte du ministère des Finances.

Les auteurs du projet de loi entendent en fait s'inspirer de la procédure prévue à l'article 48-24 du Code d'Instruction criminelle créée par 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 de droit public et modifiée par la loi du 5 juin 2009 relative 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.

Ainsi, le texte du projet de loi prévoit un accès informatique direct à l'égard de ces organismes et, à titre subsidiaire ou en cas d'impossibilité technique, une obligation pour ces organismes de fournir ces informations sur demande de l'autorité centrale [article 3 point 2° paragraphe (2)].

Le texte du projet de loi prévoit également une communication sur demande de données issues des fichiers détenus par les organismes débiteurs d'un revenu de remplacement, à savoir la Caisse nationale d'assurance pension, l'Administration du personnel de l'Etat, la Caisse de prévoyance des fonctionnaires et employés communaux, la Société nationale des Chemins de fer luxembourgeois, le Fonds national de solidarité, la Caisse nationale de santé ainsi que l'Association d'assurance accident [article 3 point 2° paragraphe (3)].

La Commission nationale propose d'y insérer le même bout de phrase « *à l'exclusion de toutes données relatives à la santé* » que dans l'article 3 point 2° paragraphe (1) deuxième point du projet de loi. Ceci éviterait que les informations fournies par ces organismes révèlent l'appartenance syndicale ou l'état de santé des personnes concernées. Ces données à caractère personnel sont sensibles et ne sont pas nécessaires pour faciliter le recouvrement de créances alimentaires.

La Commission nationale se félicite que l'exercice de l'accès informatique aux données soit assorti de garanties appropriées permettant d'éviter un usage abusif [article 3 point 2° paragraphes (5) et (6)]. En effet, le projet de loi prévoit que :

- seuls des magistrats et les membres du personnel de l'administration judiciaire disposent du droit d'accès aux informations en cause ;
- les données à caractère personnel auxquelles les magistrats et membres du personnel de l'administration judiciaire ont accès seront fixées de façon détaillée et limitative par un règlement grand-ducal ;
- l'accès informatique doit être configuré de sorte qu'il sera possible de retracer le nom du magistrat ou de l'agent du personnel de l'administration judiciaire qui a procédé à la consultation, les informations qui ont été consultées, le moment exact où la consultation a été effectuée et le motif de celle-ci.

Le commentaire des articles précise par ailleurs que « *le respect des conditions d'accès sera contrôlé et surveillé par la Commission nationale de la protection des données* ». Or, la Commission nationale voudrait relever qu'elle n'est pas compétente pour effectuer un tel contrôle en raison de l'article 8 paragraphe (1) de la loi modifiée du 2 août 2002.

L'article 3 point 2° paragraphe (7) du projet de loi reprend les principes de nécessité et de proportionnalité alors qu'il précise que « *ne peuvent en outre être consultées que les données à*

caractère personnel qui présentent un lien direct avec les faits ayant motivé la consultation ».

Sur ce point, la Commission nationale constate que le deuxième paragraphe de l'article 61 du règlement (CE) n°4/2009 est très précis et limite les catégories de données qui peuvent être traitées, à savoir :

a) l'adresse du débiteur ou du créancier ;
b) les revenus du débiteur ;
c) l'identification de l'employeur du débiteur et/ou du/des compte(s) bancaire(s) dont le débiteur est titulaire ;
d) le patrimoine du débiteur.

Le projet de loi sous examen n'indique pas en détail les données qui seront consultées ou accédées. Il renvoit à ce sujet à un règlement grand-ducal à adopter qui les déterminera.

A ce titre, l'article 3 point 2° paragraphe (4) ne renvoit cependant qu'au paragraphe (1). Or, la Commission nationale est d'avis que cette disposition devrait également renvoyer au paragraphe (3) afin de déterminer quelles données des fichiers y visées pourront faire l'objet d'une communication sur demande à l'autorité centrale.

Le règlement grand-ducal à prendre devra par ailleurs se limiter à énumérer des données qui rentrent dans le cadre strict prévu à l'article 61 point 2 du règlement (CE) n°4/2009.

Ce dernier dispose en outre que *« Pour obtenir ou modifier une décision, seules les informations visées au point a) peuvent être demandées par l'autorité centrale requise. Pour faire reconnaître, déclarer exécutoire ou exécuter une décision, toutes les informations visées au premier alinéa peuvent être demandées par l'autorité centrale requise. Toutefois, les informations visées au point d) ne peuvent être demandées que si les informations visées aux points b) et c) sont insuffisantes pour permettre l'exécution de la décision ».*

Cette « hiérarchie » établie par le texte européen signifie que le fichier des véhicules routiers et de leurs propriétaires et détenteurs, exploité pour le compte du ministère ayant les Transports dans ses attributions, et les fichiers de la documentation patrimoniale détenus par l'Administration du Cadastre et de la Topographie, exploités pour le compte du ministère des Finances, ne peuvent être accédées que lorsque les informations des autres fichiers s'avèrent insuffisantes pour permettre l'exécution d'une décision.

La Commission nationale est d'avis que cette exigence devrait aussi être transposée en droit national, le cas échéant, par le règlement grand-ducal visé à l'article 3 point 2° paragraphe (4) du projet de loi.

2) Quant à l'information de la personne visée par la collecte des données [article 62 du règlement CE]

L'article 63 du règlement prévoit l'obligation d'aviser la personne visée par la collecte de données. Cette obligation de fournir des informations à la personne concernée est l'expression d'un des principes de base de la protection des données, consacré aux articles 10 et 11 de la directive 95/46/CE et transposée en droit national par les articles 26 et 27 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement de données à caractère personnel.

L'information des personnes concernées revêt en l'espèce une importance d'autant plus grande que la règlement (CE) n°4/2009 établit un mécanisme au moyen duquel des données à caractère personnel sont collectées et utilisées pour différentes finalités, pour être ensuite transférées et traitées en passant par des administrations nationales, différentes autorités centrales nationales et des juridictions nationales.

Le législateur communautaire insiste donc sur la nécessité de fournir à la personne concernée un avis complet et détaillé, donné en temps opportun (article 26 paragraphe (2) de la loi modifiée du 2 août 2002), pour l'informer des différents transferts et traitements auxquels ses données à caractère personnel sont soumises.

Toutefois, lorsque l'avis risque de porter préjudice au recouvrement d'une créance alimentaire, le deuxième paragraphe de l'article 63 prévoit la possibilité pour l'autorité centrale de différer cette information pour une durée qui ne saurait excéder 90 jours. Cette disposition laisse donc une certaine marge de manœuvre aux législateurs nationaux qui ont la faculté de prévoir un délai plus court.

Vu l'importance de ces dispositions, la Commission nationale suggère d'implémenter cette obligation d'information dans le corps même du projet de texte sous examen, en précisant également le délai qui permet de différer l'information de la personne visée par la collecte des informations.

Ainsi décidé à Luxembourg en date du 10 juin 2011.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

Avis complémentaire concernant le projet de règlement grand-ducal fixant les conditions d'application et modalités d'exécution relatives au contrat d'accueil et d'intégration

Délibération n°160/2011 du 10 juin 2011

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 « la loi modifiée du 2 août 2002 »), la Commission nationale pour la protection des données (ci-après « la Commission nationale ») a notamment pour mission d'« *être demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi* ».

Suite à la demande d'avis complémentaire lui adressée par l'Office Luxembourgeois de l'Accueil et de l'Intégration (ci-après « OLAI ») en date du 25 mai 2011, la Commission nationale entend présenter ci-après ses observations complémentaires au sujet du projet de règlement grand-ducal pré-mentionné, lequel avait déjà fait l'objet d'un avis de la part de

Annexes

la Commission nationale en date du 6 mai 2011 (délibération n°145/2011).

Le présent avis se limite dès lors à la question relative à la durée de conservation maximale des données soulevée par l'OLAI. Dans son premier avis, la Commission nationale avait notamment suggéré à l'OLAI de limiter la durée de conservation des données des candidats acceptant de signer un contrat à 3 ans et d'anonymiser ces données au-delà de cette période.

L'OLAI estime cependant que la durée de conservation maximale de 3 ans ne serait pas suffisante. A l'appui de son argumentation, l'OLAI invoque notamment que l'article 13 alinéa 2 de la loi du 16 décembre 2008 concernant l'accueil et l'intégration des étrangers au Grand-Duché de Luxembourg prévoit que « *lors de l'examen de la demande en obtention du statut de résident de longue durée, le ministre ayant l'Immigration dans ses attributions peut tenir compte de l'accomplissement du contrat d'accueil et d'intégration pour l'appréciation du degré d'intégration de l'intéressé. Les personnes ayant signé un contrat d'accueil pourront donc s'en prévaloir pour justifier leur intégration. Or, le statut de longue durée est attribué à tout ressortissant d'un pays tiers qui réside au Luxembourg de manière régulière et ininterrompue depuis au moins 5 ans* ».

La Commission nationale voudrait maintenir sa recommandation de limiter la durée de conservation des données à caractère personnel à 3 ans, ce délai commençant à courir à partir du début d'exécution du contrat, c'est-à-dire à partir de la première prestation.

Toutefois, et afin de tenir compte des dispositions de l'article 13 alinéa 2 de la loi du 16 décembre 2008 concernant l'accueil et l'intégration des étrangers au Grand-Duché de Luxembourg, elle suggère de prévoir un fichier séparé contenant un minimum de données dont la seule finalité consisterait à certifier la participation des candidats au contrat d'accueil et d'intégration.

Ce fichier minimaliste pourrait être alimenté à partir du premier fichier exhaustif relatif au contrat d'accueil et d'intégration, c'est-à-dire duquel certaines données pourraient être reprises après l'écoulement du délai de conservation de 3 ans.

Le contenu dudit fichier séparé devrait être limité aux données d'identification minimales des candidats telles que le(s) nom(s), le(s) prénom(s), le matricule, l'adresse ainsi qu'à l'information que le candidat a accompli à bonne fin ou non le contrat

d'accueil et d'intégration.
Ces données pourraient être conservées pendant une durée maximale de 10 ans.

Ainsi, ledit fichier, ne contenant qu'un nombre très limité de données, permettrait de tenir compte de l'accomplissement du contrat d'accueil et d'intégration afin d'apprécier le degré d'intégration d'un candidat, sans pour autant devoir conserver l'intégralité des données à caractère personnel relatives au contrat d'accueil et d'intégration au-delà du délai de 3 ans.

L'ajout d'un article supplémentaire au projet de règlement grand-ducal pourrait venir transposer la proposition formulée ci-avant en précisant la finalité dudit fichier séparé, la collecte et l'utilisation des données, l'indication des données à caractère personnel, les destinataires des données ainsi que la durée de conservation.

Ainsi décidé à Luxembourg en date du 10 juin 2011.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

Avis concernant le projet de règlement grand-ducal portant exécution de l'article 3 de la loi du 3 août 2011 relative à la mise en application du Règlement (CE) n°4/2009 du 18 décembre 2008 relatif à la compétence, la loi applicable, la reconnaissance et l'exécution des décisions et la coopération en matière d'obligations alimentaires, modifiant le nouveau Code de procédure civile

Délibération n°161/2011
du 17 juin 2011

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 « la loi modifiée du 2 août 2002 »), la Commission nationale pour la protection des données (ci-après « la Commission nationale ») a notamment pour mission d'*« être demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi ».*

C'est dans cette optique, et faisant suite à la demande lui adressée par Monsieur le Ministre de la Justice en date du 15 juin 2011 que la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet du projet de règlement grand-ducal prémentionné.

Le projet de règlement grand-ducal porte exécution de l'article 3 de la loi du (…) relative à la mise en application du Règlement (CE) n°4/2009 du 18 décembre 2008 relatif à la compétence, la loi applicable, la reconnaissance et l'exécution des décisions et la coopération en matière d'obligations alimentaires, modifiant le nouveau Code de procédure civile, en projet actuellement (projet de loi no 6237).

Ledit article 3 précise les modalités d'application, pour le territoire du Grand-Duché du Luxembourg, de l'article 61 du Règlement (CE) n°4/2009 en prévoyant d'une part, un accès direct du procureur général d'Etat à certains fichiers d'organismes publics par le biais d'un système informatique et, d'autre part, l'obligation pour certains autres organismes publics de fournir des informations sur demande de l'autorité centrale.

Le texte du projet de règlement grand-ducal sous examen ne comporte pas de dispositions garantissant, tel qu'il est prévu à l'article 61 point 2 du règlement (CE) n°4/2009, que les données concernant *« le patrimoine*

7 Annexes

du débiteur » ne peuvent être demandées que dans l'hypothèse où les informations concernant « *les revenus du débiteur* » ou « *l'identification de l'employeur du débiteur et/ou du/des compte(s) bancaire(s) dont le débiteur est titulaire* » se révèlent insuffisantes pour permettre l'exécution d'une décision. La Commission nationale réitère sa proposition émise dans son avis du 10 juin 2011 (délibération n°159/2011 – avis relatif au projet de loi n°6237 relatif à la mise en application du règlement (CE) n°4/2009 du 28 décembre 2008) de transposer cette « hiérarchie », établie par le texte européen, aussi en droit national.

Les articles 1 à 4 du projet de règlement grand-ducal sous examen déterminent de façon détaillée et limitative les données à caractère personnel des fichiers en question qui pourront être accédées par l'autorité centrale. L'article 5 par contre reste plus vague alors qu'il n'énumère pas de données précises, mais parle d' « *informations relatives à la propriété immobilière* ». A l'instar des articles 1 à 4 du projet de règlement grand-ducal, il serait préférable de voir déterminer aussi à l'article 5 le détail des données du fichier de l'Administration du Cadastre et de la Topographie pouvant être accédées par l'autorité centrale.

Parmi les données énumérées à l'article 2 du projet de règlement grand-ducal figurent au point 6 les « *dates et lieux de naissance des employeurs personnes physiques* ». La Commission nationale s'interroge sur la nécessité de collecter ces données, alors que le point 7, à savoir (« *l'identification numérique des employeurs personnes physiques et morales* »), permet déjà une identification sans équivoque de l'employeur du débiteur, en vertu du règlement grand-ducal du 7 juin 1979 fixant les modalités d'application de la loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales.

Pour ce qui est du point 2 de l'article 4, la Commission nationale se demande également quelle est la nécessité de vouloir collecter « *les informations relatives au pays d'exportation du véhicule ainsi que les noms, prénoms, adresses, dates et lieux de naissance des résidents étrangers destinataires du véhicule exporté* », dans la mesure où ces données semblent se rapporter au véhicule exporté qui ne fait a priori plus partie du patrimoine du débiteur.

Pour le surplus, la Commission nationale estime que le projet de règlement grand-ducal sous examen répond aux préoccupations déjà exprimées dans son avis du 10 juin 2011 précité, alors et surtout que le texte du projet de loi n°6237

prévoit des garanties appropriées au niveau de l'exercice de l'accès informatique aux données précisées dans le projet de règlement grand-ducal.

Ainsi décidé à Luxembourg en date du 17 juin 2011.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

Avis relatif au projet de loi n°6021 sur le surendettement et modifiant certaines dispositions légales

Délibération n°168/2011 du 17 juin 2011

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 modifiée du 2 août 2002 »), la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale ») a notamment pour mission d'*« être demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi »*.

Par courrier du 30 novembre 2010, Monsieur le Ministre de la Famille et de l'Intégration a invité la Commission nationale à se prononcer au sujet du projet de loi n°6021 sur le surendettement portant 1) modification de la loi modifiée du 8 décembre 2000 sur le surendettement ; 2) modification de l'article 2016 du Code civil ; 3) modification de l'article 4 du Nouveau Code de procédure civile et 4) modification de l'article 536 du Code de commerce.

Suivant l'exposé des motifs, l'objectif du projet de loi consiste d'une part, à procéder à la modification des procédures prévues dans le cadre de la loi du 8 décembre 2000 relative au surendettement et, d'autre part, à introduire un régime de faillite civile en droit luxembourgeois.

Les dispositions mises en place par la loi du 8 décembre 2000 sur le surendettement, ne prévoyant pas de mécanisme de publicité, permettaient uniquement de toucher les créanciers connus du débiteur. Afin de préserver l'égalité de tous les créanciers, le besoin s'est fait ressentir de mettre en place un système de publicité susceptible d'informer l'ensemble des créanciers, coobligés et cautions du débiteur surendetté. À cette fin, le projet de loi instaure un « répertoire » dans le souci de les informer des différentes phases du déroulement de la procédure de règlement collectif des dettes.

La Commission nationale se limitera à examiner, dans le présent avis, la mise en place du répertoire prévu à l'article 23 de la version coordonnée du projet de loi.

La Commission nationale voudrait soulever d'emblée qu'elle reconnait l'intérêt d'assurer une telle publicité en vue notamment

de préserver l'égalité entre les créanciers et d'avertir les coobligés et cautions du débiteur surendetté sur l'exécution de leurs engagements. Quant à l'effet potentiellement intrusif du répertoire dans la vie privée du débiteur, celui-ci pourra être atténué en mettant en place des garanties appropriées. Dans l'exercice de sa mission de conseiller le gouvernement sur divers projets, la Commission nationale peut être amenée à exprimer des recommandations quant aux options les plus compatibles avec les principes de la protection des données.

Ci-après, nous commenterons, à la lumière des notions clés et des principes du droit à la protection des données à caractère personnel, les options prises dans le projet de loi et nous ferons ressortir les précisions nécessaires qui devront faire l'objet du futur règlement grand-ducal d'application.

1) La finalité du traitement

Suite à la mise en place de la loi du 8 décembre 2000 relative au surendettement, certaines lacunes sont apparues, notamment dues au manque de publicité de la mise en place d'une procédure en matière de surendettement à l'égard de l'ensemble des créanciers du débiteur. Seuls les créanciers connus de ce dernier étaient impliqués.

Les commentaires des articles mettent en exergue la nécessite de mettre en place un système de publicité susceptible de toucher l'ensemble des créanciers, coobligés et cautions existants du débiteur surendetté afin de préserver l'égalité de tous les créanciers. D'autant plus que *« le présent projet de loi propose de compléter la phase judiciaire de la procédure de règlement collectif des dettes par une procédure de rétablissement personnel pouvant aboutir à une liquidation du patrimoine du débiteur et à la répartition de son patrimoine parmi les créanciers ».*[5]

Les rédacteurs du projet de loi sous examen souhaitent ainsi y parer par la mise en place d'un fichier positif, le répertoire, dont la finalité est la publicité visant à rendre accessible aux créanciers, coobligés et cautions les étapes essentielles du déroulement de la procédure de règlement collectif des dettes, en tenant ainsi compte à la fois du besoin d'information des créanciers, coobligés et cautions et des besoins de protection du débiteur surendetté.

2) Les personnes concernées par le traitement

La Commission nationale note que les personnes concernées par le traitement sont *« toute personne physique, domiciliée au Grand-Duché de Luxembourg, éprouvant des difficultés financières durables pour faire face à l'ensemble de*

[5] Projet de loi n°6021 sur le surendettement, commentaires des articles, page 44.

ses dettes non professionnelles exigibles et à échoir »[6] pour qui une procédure de règlement collectif des dettes est ouverte. Le débiteur ne peut avoir la qualité de commerçant au sens de l'article 1er du Code de commerce à moins qu'il n'ait cessé son activité commerciale depuis au moins six mois ou, en cas de faillite, si la clôture des opérations a été prononcée.

3) La question de la responsabilité du traitement

Le droit de la protection des données repose sur des droits et obligations, énumérés dans la directive 95/46/CE du Parlement européen et du Conseil (transposée en droit national par la loi modifiée du 2 août 2002), dont le respect doit être assuré par le ou les responsable(s) du traitement.

La question de la responsabilité du traitement est évoquée à l'article 23 paragraphe (1) alinéa 2 de la version coordonnée du texte en projet qui prévoit d'instituer le Procureur général d'Etat au titre de responsable du traitement au sens de l'article 2 lettre (n) de la loi modifiée du 2 août 2002.

La Commission nationale n'entend pas prendre position à l'égard du choix de la personne qui assurera cette responsabilité.

Bien que la responsabilité du traitement soit confiée au Procureur général d'Etat, la tenue du répertoire est, quant à elle, confiée à deux autres personnes, à savoir au secrétaire de la Commission de médiation pour ce qui est des avis à établir dans le cadre de la phase du règlement conventionnel devant la Commission de médiation et au greffier par lui délégué pour ce qui est des phases judiciaires de la procédure de règlement collectif des dettes. Il faut en conclure qu'ils devraient être considérés comme « sous-traitants » au sens de l'article 2 lettre (o) de la loi modifiée du 2 août 2002.

4) Le contenu du répertoire : les données traitées

Le répertoire est appelé à centraliser les avis et informations établis en matière de procédure de règlement collectif des dettes. Son contenu ne fait pas l'objet d'une disposition unique, mais figure à divers endroits dans le texte en projet. En regroupant ces différentes dispositions, nous comprenons que le répertoire pourrait notamment se composer de :

- l'avis de règlement collectif des dettes ayant pour objet de documenter l'admission du demandeur à la procédure de règlement conventionnel (article 5 paragraphe (1)) ;

- en cas de plan de règlement conventionnel, la date de décision actant l'accord intervenu, le terme du plan et la date de révocation dudit plan (article 7 paragraphe (1) alinéa 5) ;

- la recommandation de la Commission de médiation de suspendre l'exigibilité des créances dans des circonstances précises (article 7 paragraphe (4) alinéa 2) ;

- en cas de situation du débiteur compromise à un tel point qu'un plan de règlement conventionnel ou un moratoire s'avèrent illusoires ou en cas de non-acceptation du plan de règlement conventionnel par les parties, mention du procès-verbal de carence sera faite dans un avis publié au répertoire (article 7 paragraphe (5) et article 8 paragraphe (1)) ;

- en cas de rétablissement personnel, la publication d'un avis portant sur le jugement d'ouverture de la procédure de rétablissement personnel (article 16 paragraphe (4) alinéa 3).

Le projet de loi n'est toutefois pas plus explicite quant aux catégories de données à caractère personnel susceptibles d'y figurer.

Au stade actuel, il est dès lors difficile d'apprécier, à la lumière de l'article 4 paragraphe (1)

[6] Article 2 alinéa 1er de la version coordonnée du projet de loi.

lettre (b) de la loi modifiée du 2 août 2002, le caractère adéquat, pertinent et non excessif des données que contiendra le répertoire.

Le projet de loi ne contenant pas une énumération précise des données, celles-ci devront nécessairement être déterminées, au plus tard, dans un règlement grand-ducal.

Certes, il aurait été préférable, à l'instar d'autres textes législatifs, de préciser au moins les grandes catégories de données dans le texte de loi en projet et les données détaillées dans un règlement grand-ducal.

5) Le fonctionnement du répertoire : les opérations de traitement

L'article 23 paragraphe (2) alinéa 1 du texte en projet prévoit que « *la publicité des extraits de décision des avis conservés au répertoire est assurée par une inscription dans un fichier, mécanique ou informatique, au nom de la personne protégée* ».

La Commission nationale s'interroge quant à la signification du terme « *mécanique* » alors qu'il n'apparait pas clairement s'il est fait référence à une autre forme de traitement non électronique ou à un traitement manuel.

Le projet de loi, en son article 23 paragraphe (5), prévoit que les modalités de fonctionnement même du répertoire et de publication des avis et des informations, seront déterminées par voie de règlement grand-ducal.

Au stade actuel, ces modalités n'étant pas encore connues, la Commission nationale ne peut pas se prononcer.

6) Les destinataires des données contenues dans le répertoire

Le répertoire étant créé dans un souci d'assurer une meilleure publicité, toute personne physique justifiant de son identité a le droit de le consulter gratuitement en vue d'obtenir connaissance des avis et informations concernant une personne déterminée et dont la publication est prescrite par le présent projet de loi (article 23 paragraphe (2) alinéa 2).

Dans sa version initiale, le projet de loi prévoyait que seules certaines personnes limitativement désignées auraient le droit de consulter le répertoire dont, entre autres, celles justifiant d'un intérêt légitime. Suite notamment à l'avis du Conseil d'Etat[7] qui ne comprenait pas la frilosité des auteurs à faciliter davantage l'accès au répertoire, le texte fût amendé.

La Commission nationale se rallie à l'avis du Conseil d'Etat

[7] Avis du Conseil d'Etat du 22 juin 2010 relatif au projet de loi n°6021, page 24.

selon lequel une telle restriction serait vouée à l'échec. Bien qu'en théorie il serait satisfaisant de conditionner l'accès aux données par la justification d'un tel intérêt légitime en vue d'éviter toute consultation du répertoire motivée par la curiosité malsaine ou la commercialisation des données consultées, en pratique cela s'avérerait illusoire. À titre d'illustration, citons l'exemple d'un contrat de vente : s'il est parfaitement légitime pour le vendeur de s'interroger quant à la solvabilité de son acheteur éventuel, il serait impossible de vérifier qu'il est effectivement en phase précontractuelle lorsqu'il voudrait consulter le répertoire.

7) Les droits des personnes concernées

Le projet de loi, en son article 23 paragraphe (2) alinéa 3, rappelle l'article 28 de la loi modifiée du 2 août 2002, à savoir le droit pour toute personne d'accéder aux données qui la concerne. En cas de traitement de données non conforme à ladite loi, notamment en raison du caractère incomplet ou inexact des données, le texte en projet reconnait également à la personne concernée un droit de rectification.

À noter toutefois que les données contenues dans le répertoire et issues de la phase judiciaire de la procédure de règlement collectif des dettes (règlement judiciaire et procédure de rétablissement personnel) constituent une catégorie particulière de données, à savoir des données judiciaires, visée à l'article 8 de la loi modifiée du 2 août 2002.

Pour ces données, la mise en œuvre du droit d'accès et de rectification n'est pas assurée car, obéissant au régime spécifique de l'article 8 de la loi modifiée du 2 août 2002, elles échappent à la compétence de la Commission nationale.

8) Les mesures de sécurité

Le droit de la protection des données s'appuie sur l'idée fondamentale que le responsable du traitement doit s'assurer que les données à caractère personnel qu'il traite le sont loyalement et licitement et ne sont pas traitées ultérieurement 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 tiers.
Il a également l'obligation de mettre en œuvre toutes les mesures techniques et l'organisation appropriées afin d'assurer la sécurité du traitement. Les dispositions du règlement grand-ducal à adopter devront en tenir compte au niveau des modalités de fonctionnement du répertoire.

La Commission nationale note avec satisfaction qu'une disposition impose par ailleurs une obligation de confidentialité à tous ceux qui, à quelque titre que ce soit, participent à la collecte, à l'enregistrement, à la gestion ou à la communication des données enregistrées dans le répertoire (article 23 paragraphe (3)).

9) La durée de conservation des données

L'article 4 paragraphe (1) lettre (d) de la loi modifiée du 2 août 2002 requiert que les données personnelles soient *« 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 »*. Par référence à cette disposition, la Commission nationale relève que la conservation des données pendant une durée limitée est une garantie supplémentaire des libertés et droits des personnes concernées. Dans l'optique de la future révision de la directive 95/46/CE du Parlement européen et du Conseil, la loi reconnaît à l'individu un « droit à l'oubli » en limitant dans le temps la conservation des données nominatives.

La Commission nationale note avec satisfaction qu'une disposition relative à la durée

de conservation des données contenues dans le répertoire a été ajoutée dans la version coordonnée du texte en projet.

L'article 23 paragraphe (4) du texte sous examen envisage la durée des inscriptions au répertoire comme suit :

« a. les plans de règlement conventionnel, les plans de redressement judiciaire et les plans de redressement judiciaire établis à des fins probatoires sont inscrits au répertoire pour la durée de leur exécution sans pouvoir excéder sept ans à compter de la date de leur établissement ;

b. les recommandations de la Commission ayant fait l'objet d'une acceptation et ayant trait au moratoire prévu à l'article 7 paragraphe (4) de la loi sont conservées pendant une durée ne pouvant excéder sept ans à compter de l'acceptation de la recommandation par la Commission ».

La finalité du traitement étant l'information des créanciers, des cautions et des coobligés du débiteur surendetté sur l'état d'avancement de la procédure de règlement collectif des dettes, les données ne devront pas être conservées plus longtemps que nécessaires à la réalisation de cette finalité. La Commission nationale constate que la durée de sept ans fait référence à l'article 7 paragraphe (3) et à l'article 12 alinéa 5 qui limitent, sauf exceptions, la durée du plan de règlement conventionnel et du redressement judiciaire.
En vue également de ne pas conserver les données plus longtemps que nécessaire, la Commission nationale salue l'initiative des auteurs du projet de loi de prévoir la possibilité de solliciter la radiation anticipée du répertoire pour le débiteur surendetté capable de justifier le règlement intégral de ses dettes auprès de tous les créanciers figurant au plan de règlement conventionnel ou au jugement arrêtant le plan de redressement judiciaire (article 23 paragraphe (4) alinéa 3).

Quant aux débiteurs surendettés ayant bénéficié de la procédure de rétablissement personnel, ceux-ci font l'objet d'une inscription au répertoire pour une période de cinq ans à compter de la date du jugement de clôture de la procédure de rétablissement personnel ayant acquis autorité de chose jugée. Une fois cette période écoulée, la radiation du débiteur surendetté du répertoire est acquise de plein droit et est réalisée d'office (article 21 paragraphe (1)).

Aux yeux de la Commission nationale, ces durées de conservations sont justifiées au regard des finalités poursuivies.

Ainsi décidé à Luxembourg
en date du 17 juin 2011.

La Commission nationale pour
la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

Avis concernant l'avant-projet de règlement grand-ducal modifiant le règlement grand-ducal du 17 février 1987 sur l'identification des menues embarcations

Délibération n°181/2011
du 1er juillet 2011

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 « la loi modifiée du 2 août 2002 »), la Commission nationale pour la protection des données (ci-après « la Commission nationale ») a notamment pour mission d'*« être demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi »*.

Par courrier du 18 avril 2011, Monsieur le Ministre du Développement durable et des Infrastructures a consulté la Commission nationale au sujet d'une première version de l'avant-projet de règlement grand-ducal modifiant le règlement grand-ducal du 17 février 1987 sur l'identification des menues embarcations.

C'est suite aux observations formulées par la Commission nationale lors d'une réunion avec les représentants du Ministère du Développement durable et des Infrastructures - Département des transports, Service de la navigation, qu'une version remaniée du texte a été transmise pour avis à la Commission nationale en date du 7 juin 2011. Cette nouvelle version de texte tenant compte de ses observations antérieures, la Commission nationale se limitera dans le présent avis aux commentaires suivants :

En ce qui concerne la durée de conservation des données, l'avant-projet de règlement grand-ducal prévoit, dans son article 4, alinéa 4, que « *Les données restent inscrites dans le registre tant qu'un changement n'est pas notifié au responsable du traitement par le titulaire de la marque d'identification. Après la cessation de la validité de la marque d'identification, conformément à l'article 10, les données sont encore archivées pendant 5 ans. Le titulaire de la marque d'identification peut demander à tout moment et gratuitement un extrait concernant son inscription dans le registre, voire sa radiation du registre* ».

L'objet de cette disposition est d'instaurer une durée de conservation limitée des données contenues dans le registre des menues embarcations.

7 Annexes

La Commission nationale comprend que les données seront conservées dans le registre aussi longtemps que la marque officielle d'identification est valide et que le certificat d'identification a été prorogé. Ce n'est qu'en cas de cessation de la validité d'une marque d'identification que le responsable du traitement entend supprimer ces données du fichier pour ensuite les archiver pendant une période de cinq ans.

L'article 4 paragraphe (1) lettre (d) de la loi modifiée du 2 août 2002 pose le principe que les données personnelles ne doivent pas être conservées pendant une durée qui excède celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées.

La Commission nationale estime que les modalités relatives à la conservation des données dans le registre peuvent être considérés comme proportionnées par rapport aux principes énoncés par la loi modifiée du 2 août 2002.

En ce qui concerne la deuxième phrase de l'article 4, alinéa 4, relative à la cessation de la validité d'une marque d'identification, elle comprend que les auteurs ont voulu faire référence à « *l'article 7* » au lieu de « *l'article 10* ».

En ce sens, l'article 4, alinéa 4 du texte en projet pourrait prendre la teneur suivante :

« *Les données restent inscrites dans le registre pendant la durée de validité ~~tant qu'un changement n'est pas notifié au responsable du traitement par le titulaire~~ de la marque d'identification.*

~~Après la cessation de validité~~ Lorsque la validité ~~de la marque d'identification~~ celle-ci cesse, conformément à l'article ~~10~~7, les données sont ~~encore~~ archivées pendant ~~5~~cinq ans.

Le titulaire de la marque d'identification peut demander à tout moment et gratuitement un extrait concernant son inscription dans le registre, voire sa radiation du registre ».

L'article 4, alinéa 5 de l'avant-projet de règlement grand-ducal prévoit que « *le traitement des données est utilisé dans le cadre de la gestion des numéros attribués en vue de leur identification* ». Cette disposition entend préciser la finalité du registre des menues embarcations.

La Commission nationale propose le libellé suivant :
« *~~Le traitement des données est utilisé dans le cadre de la gestion des numéros attribués en vue de leur identification.~~ Le registre d'identification des menues embarcations a comme finalité la gestion des marques officielles attribuées aux menues embarcations en vue de leur identification, ainsi que leur suivi*

administratif ».

L'article 4, alinéa 7 prévoit que *« Le Parquet général, la Police Grand-Ducale et le STATEC sont autorisés à prendre connaissance des données de la banque de données pour autant que ces données les concernent directement dans l'exécution de leurs fonctions ».*

La Commission nationale souhaiterait apporter à cette disposition les précisions suivantes :

« Le Parquet général, la Police Grand-Ducale et le STATEC sont autorisés, sur demande, à prendre connaissance des données contenues dans le registre des menues embarcations ~~de la banque de données~~ pour autant que ces données les concernent directement dans l'exécution de leurs fonctions ».

Ainsi décidé à Luxembourg en date du 1er juillet 2011.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

Avis au sujet d'une demande d'échanges de données relatives aux enfants de fonctionnaires du Parlement européen soumise par cette institution communautaire au Ministère de l'Enseignement Supérieur et de la Recherche

Délibération n°270/2011 du 3 août 2011

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 « la loi modifiée du 2 août 2002 »), la Commission nationale pour la protection des données (ci-après « la Commission nationale ») a notamment pour mission d'*« être demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi ».*

Par courrier du 27 juillet 2011, Monsieur le Ministre de l'Enseignement supérieur et de la Recherche a consulté la Commission nationale au sujet d'une demande d'échanges de données relatives aux enfants de fonctionnaires du Parlement européen soumise par cette institution communautaire au Ministère de l'Enseignement Supérieur et de la Recherche.

La direction générale du Personnel du Parlement européen à Luxembourg par l'organe du Chef d'unité « Droits individuels et rémunérations » a en effet saisi par courrier du 1er juin le Ministre de l'Enseignement Supérieur et de la Recherche – CEDIES d'une demande d'échange de données au sujet des aides financières accordées le cas échéant aux enfants de fonctionnaires européens ayant demandé l'attribution d'une allocation scolaire communautaire.

Le critère de légitimation invoqué par le service du Parlement européen est celui visé à l'article 8 sub (a) du règlement 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 les institutions et organes communautaires et à la libre circulation de ces données.

Cette disposition vise le transfert par une institution européenne de données à caractère personnel à des destinataires autres que les institutions et organes communautaires et relevant de la directive 95/46/CE, lorsque le destinataire démontre que les données sont nécessaires à l'exécution d'une mission effectuée dans l'intérêt public ou

relevant de l'exercice de l'autorité publique.

Or, en l'espèce le destinataire – Ministère de l'Enseignement Supérieur et de la Recherche de l'Etat luxembourgeois : service CEDIES – n'entend pas invoquer la nécessité à l'exécution d'une mission d'intérêt public ou relevant de l'autorité publique, dont est investi le responsable du traitement ou le tiers auxquels les données sont communiquées. Les informations relatives aux enfants des demandeurs d'une allocation scolaire européenne ne sont ni nécessaires ni pertinentes au regard de l'exécution de ses missions et attributions.

Il ne pourrait d'ailleurs procéder à un tel échange d'informations entre ses fichiers et les listings que les services du Parlement européen se proposent de lui fournir pour vérification à défaut d'un texte de loi prévoyant un tel échange et rapprochement de données.

Le principe de légalité et de prévisibilité instauré par l'article 8 paragraphe 2 de la Convention européenne des Droits de l'Homme et des Libertés fondamentales présuppose en effet que toute ingérence dans la vie privée des citoyens soit non seulement nécessaire dans une société démocratique pour un des intérêts publics majeurs y visés ou pour la protection des droits d'autrui (principe de proportionnalité), mais aussi qu'elle soit prévue par la loi.

L'article 5 paragraphe 1er lettre (a) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel et l'article 8 lettre (a) du règlement communautaire 45/2001 submentionné (qui en constitue le pendant pour ce qui concerne les traitements effectués par les institutions et organes communautaires) sont en effet à lire sous réserve et sans préjudice des articles 4, 5, 6 et 10 du prédit règlement communautaire.

Or, c'est précisément l'article 4 qui reprend explicitement les conditions de loyauté et de licéité du traitement.

Dans l'hypothèse examinée le Ministère de l'Enseignement Supérieur et de la Recherche excèderait clairement les finalités pour lesquelles il a obtenu les données relatives aux allocataires d'aides financières de l'Etat luxembourgeois qu'il traite, s'il acceptait de les échanger et de les rapprocher avec celles fournies par les services d'une institution européenne ou d'un autre tiers.

La finalité de ce traitement ultérieur qu'il soit nécessaire ou non pour les besoins de l'exécution de la mission d'intérêt public relevant de la compétence du destinataire (Parlement

européen), n'est pas pour le moins couverte par les prévisions du législateur luxembourgeois et amènerait donc les services gouvernementaux à encourir le reproche de violation des principes de l'article 4 paragraphe 1er (a) de la loi modifiée du 2 août 2002 (traitement pour une finalité incompatible).

Il est évident que l'application de l'article 67 du statut des fonctionnaires européens ne relève pas de la compétence de l'administration luxembourgeoise et dépasse les finalités du traitement de données qu'il effectue. Le Ministère doit aux termes de cet article 4 de la loi s'assurer que les données qu'il traite le sont loyalement et licitement. Il doit donc s'abstenir à notre avis de divulguer à des tiers des données à caractère personnel confidentielles en l'absence de dispositions prévoyant explicitement un échange de données et la finalité afférente (de contrôle du respect des dispositions anti cumul éventuellement applicables).

A défaut d'une base légale spécifique, il appartiendrait aux services du Parlement européen de justifier du consentement donné dans le respect des conditions légales par chacun des étudiants concernés ou plus facilement de demander à leurs parents de joindre à leur demande d'allocation scolaire communautaire un certificat à établir par le CEDIES que l'étudiant en question ne bénéficie pas d'une aide financière de l'Etat.

Ainsi décidé à Luxembourg en date du 3 août 2011.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

Avis relatif à l'avant-projet de loi relatif aux droits et obligations du patient et aux droits et obligations correspondants du professionnel de la santé, relatif à la médiation dans le domaine de la santé et portant modification de la loi du 28 août 1998 sur les établissements hospitaliers

Délibération n°357/2011
du 28 octobre 2011

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 ».*

Faisant suite à la demande lui adressée par Monsieur le Ministre de la Santé en date du 7 juillet 2011, la Commission nationale expose ci-après ses réflexions et commentaires au sujet de l'avant-projet de loi relatif aux droits et obligations du patient et aux droits et obligations correspondants du professionnel

de la santé, relatif à la médiation dans le domaine de la santé et portant modification de la loi du 28 août 1998 sur les établissements hospitaliers (ci-après : l'avant-projet de loi).

Introduction

A ce jour, la matière des droits des patients est régie par des lois[8] disparates ainsi que dans des textes internationaux[9]. La Commission nationale ne peut que se satisfaire de l'initiative qui conduit à l'élaboration de l'avant-projet de loi soumis à son appréciation, qui consacre une législation spécifique aux rapports entre un patient – et son entourage – et les prestataires des soins de santé. Les patients auront ainsi une meilleure visibilité de leurs droits et obligations, ce qui leur permettra de s'en prévaloir plus facilement en cas de nécessité. L'avant-projet de loi innove aussi en instituant de nouveaux droits fondamentaux au patient et en modifiant, parfois en profondeur, certaines règles et pratiques existantes.

A titre liminaire, la Commission nationale relève que l'avant-projet de loi confère au patient un rôle plus actif dans ses relations avec les prestataires de soins de santé. Le patient se voit reconnaître une responsabilité personnelle dans les décisions relatives à sa santé. Cette participation est d'autant plus effective que l'avant-projet de loi prévoit un véritable droit à l'information du patient tout au long de sa relation avec le professionnel de la santé.

De plus, la Commission nationale adhère à l'affirmation posée dans l'exposé des motifs annexé à l'avant-projet de loi[10] selon laquelle le respect des droits du patient est une obligation fondamentale du prestataire de soins de santé.

Il ressort de l'exposé des motifs que l'avant-projet de loi s'inspire des législations relatives aux droits des patients qui existent en France et en Belgique et se réfère à la Déclaration de l'OMS, à la Convention d'Oviedo et à la Charte des droits fondamentaux de l'Union européenne publiée le 18 décembre 2000. Par ailleurs, il y a lieu de prendre en compte 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 personne et à la libre circulation de ces données[11] qui traite notamment du droit à l'information des personnes ou encore du droit d'accès aux informations qui les concernent.

La Commission nationale marque son approbation avec cette réforme législative ; au cours du passage en revue des articles, elle présente quelques observations et suggère des adaptations.

---

[8] Notamment la loi du 2 août 2002 et la loi modifiée du 28 août 1998 sur les établissements hospitaliers (ci-après : la loi sur les établissements hospitaliers).

[9] Dont la Déclaration sur la promotion des droits des patients en Europe de l'OMS de 1997 (ci-après : la Déclaration de l'OMS), la Convention du Conseil de l'Europe pour la protection des droits de l'homme et de la dignité de l'être humain à l'égard des applications de la biologie et de la médecine signée à Oviedo le 4 avril 1997 (appelée « Convention d'Oviedo ») et la Charte des droits fondamentaux de l'Union européenne publiée le 18 décembre 2000.

[10] cf. page 5 de l'exposé des motifs.

[11] ci-après : la directive 95/46/CE.

Chapitre 1 :
Champ d'application et définitions (articles 1 à 2)

La Commission nationale estime que le champ d'application de l'avant-projet de loi sous examen couvre le dossier de soins partagé. En effet, compte tenu de la généralité des termes utilisés dans l'avant-projet de loi, les droits et obligations édictés dans le texte sous examen doivent s'appliquer de façon similaire dans le cadre du dossier de soins partagé, tel que prévu à l'article 60quater de loi du 17 décembre 2010 portant réforme du système de soins de santé et modifiant : 1. le Code de la sécurité sociale ; 2. la loi modifiée du 28 août 1998 sur les établissements hospitaliers. Les droits et obligations existant dans le cadre de la relation en binôme avec un professionnel de la santé doivent également s'appliquer dans un dossier où plusieurs professionnels de la santé interviennent.

En ce qui concerne les définitions de l'article 2 du texte sous examen, la Commission s'interroge sur l'opportunité de donner une définition restrictive des soins de santé. En effet, l'exception édictée à l'article 2, lettre (b), de l'avant-projet de loi prive les patients concernés de l'ensemble des droits fondamentaux prévus aux articles qui suivent.

Chapitre 2 :
Droits et obligations du patient dans sa relation avec le prestataire de soins de santé (articles 3 à 19)

La loi du 2 août 2002 contient des dispositions qui intéressent directement les patients et leur famille : le droit à l'information (article 26), le droit d'accès aux informations (article 28), le droit de rectification et de suppression (article 28), le droit à la sécurité (articles 22 et 23) ainsi que le droit d'opposition (article 30).

La Commission nationale estime que le texte sous examen ne devrait pas s'écarter des principes posés par la directive 95/46/CE et la loi du 2 août 2002 qui transpose cette directive. En effet, si l'avant-projet de loi peut préciser et compléter les modalités relatives aux droits et obligations prévus dans ces textes, il ne peut pas les contredire. Le considérant (68) de la directive 95/46/CE dispose ainsi que « *les principes énoncés dans la présente directive et régissant la protection des droits et des libertés des personnes, notamment du droit à la vie privée, à l'égard du traitement des données à caractère personnel pourront être complétés ou précisés, notamment pour certains secteurs, par des règles spécifiques conformes à ces principes* ».

Article 6 :
Droit à l'accompagnement par un proche

L'article 6 de l'avant-projet de loi introduit le rôle de l'accompagnateur du patient, à l'instar des législations d'autres Etats membres, de la loi du 16 mars 2009 relative aux soins palliatifs, à la directive anticipée et à l'accompagnement en fin de vie et de la loi du 16 mars 2009 relative à l'euthanasie et l'assistance au suicide.

L'intérêt de cette officialisation de l'accompagnateur du patient permet d'éviter que l'accompagnateur se voit opposer le secret médical à l'égard des données du patient. La Commission nationale est satisfaite que l'article 18 du texte sous examen prévoit qu'en contrepartie de la levée du secret médical à son égard, l'accompagnateur doit assurer la confidentialité des informations qu'il reçoit.

Article 7 :
Droit à l'information sur l'état de santé

L'information est un préalable à l'autodétermination du patient. L'avant-projet de loi instaure un renforcement des obligations des professionnels de santé dans ce domaine. L'article 7 de l'avant-projet de loi prévoit que dans le cadre des relations entretenues entre un patient et un prestataire

de soins de santé, le patient peut également se prévaloir du droit d'être tenu dans l'ignorance (le droit de ne pas savoir) sauf si cela risque de causer un préjudice grave à un tiers.

La Commission nationale estime, d'une part, que le préjudice grave auquel il est fait référence doit être en rapport avec la santé du tiers. La Commission de la protection de la vie privée[12] s'est prononcé en ce sens : « *le préjudice grave qui serait manifestement causé (…) à des tiers doit avoir un lien avec la santé du patient (…), parce que le praticien professionnel peut uniquement se prononcer en connaissance de cause à ce sujet. (…) Le texte proposé est plus large et peut aussi viser un préjudice purement patrimonial. La Commission est d'avis qu'on ne peut pas charger le praticien de l'évaluation des intérêts autres que ceux qui concernent la santé, ces derniers étant il est vrai compris au sens large (bien-être physique, psychique et social* »[13].

La Commission nationale se demande, d'autre part, si, comme en Belgique, le praticien ne devrait pas consulter un confrère et la personne de confiance éventuellement désignée avant de prendre sa décision[14].

Article 9 :
Exception thérapeutique

Selon l'article 9 du texte sous avis, l'exception thérapeutique dispense le praticien de donner les informations sur l'état de santé si sa communication risque de causer un préjudice grave à la santé du patient. Si l'avant-projet de loi prévoit que la non-divulgation ne s'étend pas aux autres praticiens, il ne précise pas si elle peut être invoquée à l'encontre du tiers de confiance, respectivement à l'accompagnateur.

En outre, la Commission nationale se demande s'il ne serait pas préférable que le prestataire de soins de santé prenne l'avis d'un confrère avant de faire appliquer l'exception thérapeutique. Le principe « des quatre yeux » permet en effet d'éviter les abus et les appréciations erronées. Ce mécanisme de vérification est une garantie qui apporte des garanties au bien-fondé de la décision relative à l'exception thérapeutique. Les règles de déontologie médicale au Luxembourg prévoient également le recours à l'avis d'un confrère ; il serait inapproprié qu'il existe une incohérence entre le texte sous examen et les pratiques déontologiques qui sont actuellement en vigueur.

Ensuite, si le texte précise que l'exception thérapeutique sera inscrite dans le dossier, il n'en précise pas l'impact sur l'exercice du droit d'accès du patient, en dehors des hypothèses spécifiques des articles 16

[12] Ci-après : la Commission belge.
[13] Avis n°30/2001 du 22 août 2001 portant sur l'avant-projet de loi relatif aux droits du patient, page 6.
[14] Article 7 paragraphe 4 de la loi modifiée du 22 août 2002 relative aux droits du patient.

paragraphe (5) et 9 paragraphe (2) du texte sous examen.

Article 10 :
Modalités d'expression du consentement

Le consentement est l'expression du droit à l'autodétermination du patient. L'article 10 de l'avant-projet de loi précise les modes de délivrance du consentement du patient à l'égard des décisions concernant sa santé qui font l'objet de l'article 8 dudit avant-projet de loi. La Commission nationale note que le consentement donné par écrit est érigé en règle par l'alinéa 1er de article 10 paragraphe (1) du texte sous examen. Le consentement tacite prévu à l'alinéa 2 constitue l'exception. Or, la CNPD se soucie que l'exception du consentement tacite risque de devenir en pratique la règle. Elle est donc à se demander s'il ne faudrait pas prévoir des garde-fous pour pallier à ce risque. En tout état de cause, tout consentement qu'il soit écrit ou tacite présuppose une information préalable et exhaustive.

L'autodétermination du patient joue aussi un rôle important lorsque la décision commune du patient et de son médecin ne porte pas sur le choix thérapeutique lui-même, mais sur le fait d'associer d'autres professionnels de la santé au diagnostic et à l'administration des soins et traitements. Lorsqu'il est décidé d'associer d'autres prestataires de soins, ceux-ci doivent nécessairement aussi recevoir accès au dossier du patient.

Or, nous estimons que des prestataires de soins autres que le médecin initialement consulté par le patient ne doivent pas pouvoir accéder au dossier du patient à l'insu de celui-ci, voire contre son gré. En effet, hormis l'hypothèse de l'urgence médicale, et dans le respect du secret médical, un professionnel de la santé ne peut accéder à un dossier patient que si au moment de l'accès, il existe une relation thérapeutique à laquelle le patient a marqué son accord. Une transparence totale à l'égard du patient doit être assurée à tous les stades quant aux instances médicales et prestataires de soins de santé ayant accès au dossier. Ceci suppose que des garanties appropriées doivent être mises en place pour que le patient ait la maîtrise sur son dossier, garanties qui doivent exister aussi bien pour les dossiers se trouvant dans un cabinet ou un établissement hospitalier que pour les dossiers de soins partagé. Le choix de certains pays d'utiliser la remise de la carte électronique du patient pour valider les accès à son dossier nous apparaît comme la meilleure façon de garantir au patient une participation active et une transparence totale à cet égard. A ce sujet, nous renvoyons en outre à notre avis relatif au projet de loi n°6196 portant réforme du système de soins de santé et plus particulièrement au point 3. *« Le rôle du patient dans la tenue du dossier – Lors de la consultation du dossier » (délibération du n°345/2010 du 24.11.2010).*

Articles 12 à 14 :
Représentation du patient

Le rôle d'une personne de confiance est, aux termes de l'article 12 (1) alinéa 2 de l'avant-projet de loi, de se substituer au patient qui ne serait plus en mesure d'exercer ses droits. La Commission nationale fait sienne la réflexion de la Commission belge lorsqu'elle affirme que *« la personne de confiance, en acceptant de jouer son rôle, accepte tacitement de n'utiliser les informations qui lui seront communiquées que dans le seul intérêt du patient. (…) La Commission peut marquer son accord sur le fait que la communication d'informations à une personne de confiance ne soit pas soumise à des conditions supplémentaires »*[15]. Il faut également saluer l'avant-projet de loi en ce qu'il précise que le professionnel de la santé doit toujours rechercher la volonté du patient avant de se retourner vers la personne de confiance car la volonté du patient doit toujours prévaloir.

[15] Avis précité 30/2001, page 6.

7 Annexes

La Commission nationale exprime également sa satisfaction à ce que les incapables majeurs et mineurs puissent dans la mesure du possible exercer eux-mêmes les droits et obligations prévus par l'avant-projet de loi. Elle approuve également le système cohérent en cascade des personnes pouvant représenter les incapables majeurs et mineurs[16] car « *un praticien professionnel peut désigner rapidement et de façon pragmatique un représentant unique pour le patient, ce qui permet de prévenir les conflits* »[17].

Il ressort des commentaires des articles relatifs au texte sous examen que si l'avant-projet de loi envisage l'éventualité d'une pluralité de personnes de confiance, il ne se prononce pas sur une possible divergence de position entre ces personnes de confiance, respectivement sur une possible représentation en cascade, à l'instar de ce qui est prévu pour les incapables.

Article 15 :
Tenue des dossiers du patient

Aux termes de l'article 15 de l'avant-projet de loi, l'établissement et la mise à jour du dossier médical incombent aux médecins et aux médecins-dentistes. Ces derniers sont donc les responsables du traitement au sens de l'article 2 lettre (n) de la loi du 2 août 2002. La CNPD déduit de la lecture combinée de l'article 36 de la loi modifiée du 28 août 1998 sur les établissements hospitaliers tel qu'il est proposé à l'article 24 du projet de loi sous examen, et de l'article 15 du texte sous examen, que sont responsables conjoints du dossier médical les médecins qui alimentent le volet médical et les établissements hospitaliers sous la responsabilité de son directeur médical. L'identification du responsable du traitement est cruciale en matière de protection des données, étant donné qu'il lui incombe des devoirs et des obligations en vertu de la loi du 2 août 2002.

La Commission nationale regrette que le texte sous examen ne prévoie pas le contenu du dossier médical, respectivement du volet médical du dossier du patient, l'article 15 paragraphe (2) de l'avant-projet renvoyant simplement à un règlement grand-ducal à prendre. La loi modifiée du 28 juillet 1998 sur les établissements hospitaliers renvoyait déjà à un règlement grand-ducal pour préciser le contenu du dossier médical et, à ce jour, ce règlement n'a pas été pris. Les auteurs du texte sous examen auraient pu saisir l'occasion de préciser le contenu du dossier médical dans le corps même de l'avant-projet.
Mais s'il estime que le recours à un règlement grand-ducal est plus adapté pour préciser le contenu du dossier, alors la CNPD aurait souhaité l'analyser

[16] Articles 13 et 14 de l'avant-projet de loi.
[17] Avis précité 30/2001 page 13.

ensemble avec l'avant-projet de loi.

Article 16 :
Droit d'accès aux dossiers du patient et aux données relatives à sa santé

Le texte prévoit que le patient peut exercer son droit d'accès au dossier médical soit directement soit par l'intermédiaire d'un proche ou d'un médecin. Il prévoit ainsi que le patient décide seul de la manière selon laquelle s'exercera son droit d'accès, le praticien pouvant seulement demander, sans l'imposer, que la consultation ait lieu en présence d'un prestataire pouvant procéder à une consultation d'annonce. En toute hypothèse, le choix final sera pris par le patient. La Commission nationale suit la position de la Commission nationale de l'Informatique et des Libertés[18] qui dans son avis sur le projet de loi de modernisation du système de santé approuve *« la faculté laissée au médecin de recommander, lors de la consultation de certaines informations, la présence d'une tierce personne pour des motifs déontologiques tenant aux risques que leur connaissance sans accompagnement pourrait faire courir à la personne concernée »*[19].

De plus, la Commission nationale relève que l'article 16 paragraphe (5) du texte sous examen s'écarte des dispositions de l'article 28 paragraphe (3) de la loi du 2 août 2002 qui ne prévoient pas qu'un proche puisse consulter le dossier médical d'un patient[20]. Elle s'interroge dès lors sur les risques qui pourraient apparaître, en termes de sécurité juridique, en cas de divergences d'interprétation entre ces deux dispositions.

Elle note encore que l'article 16 paragraphe (3) alinéa 2 de l'avant-projet de loi entre en contradiction avec les dispositions de la loi du 2 août 2002 ayant trait au coût éventuel de la communication des informations. En effet, le texte sous examen prévoit que la *« contribution aux frais de copie éventuellement mis à la charge du patient ne peut excéder le coût réel »* alors que l'article 28 paragraphe (1) de la loi du 2 août 2002 précise que la personne concernée ou ses ayants droit peuvent obtenir sans frais la communication des données faisant l'objet du traitement. Une contrariété entre ces deux textes n'est pas souhaitable.

La CNPD remarque par ailleurs que l'article 16 paragraphe (5) prévoit une modalité particulière du droit à la consultation du dossier médical : si le prestataire a des raisons de craindre que la consultation du dossier peut causer un préjudice grave à la santé du patient, il peut demander la présence d'un prestataire capable de procéder à une consultation d'annonce. Un tel aménagement au droit d'accès s'inscrit parfaitement dans les exceptions prévues à l'article 13 paragraphe (1) lettre (g) de la directive 95/46/CE et de l'article 27 paragraphe 1er de la loi du 2 août 2002 qui prévoit une exception au droit à l'information si la limitation *« constitue une mesure nécessaire pour sauvegarder la protection de la personne concernée ou des droits et libertés d'autrui ».*

Article 19 :
Accès aux dossiers et aux données du patient décédé

Le régime relatif à l'accès aux dossiers et aux données du patient décédé est distinct du régime posé à l'article 28 paragraphe (3) de la loi du 2 août 2002.

En effet, l'avant-projet de loi ne requiert pas que la consultation du dossier doive, en cas de décès du patient, nécessairement requérir l'intermédiaire d'un médecin. La CNPD peut concevoir que l'exigence d'un intermédiaire correspondait aux standards généralement acceptés dans le passé mais que les évolutions sociales les ont dépassé. Il semble nécessaire de trancher entre ces deux dispositions.

---

[18] Ci-après : la CNIL.
[19] Délibération 01-041 du 10 juillet 2001.
[20] L'article 28 paragraphe (3) dispose qu'en *« cas de décès du patient, son conjoint non séparé de corps et ses enfants ainsi que toute personne qui au moment du décès a vécu avec lui dans le ménage ou, s'il s'agit d'un mineur, ses père et mère, peuvent exercer, par l'intermédiaire d'un médecin qu'ils désignent, le droit d'accès (…) ».*

De plus, l'avant-projet de loi prévoit des dispositions qui n'existent dans la loi du 2 août 2002. Ainsi, l'article 19 de l'avant-projet de loi prévoit que le patient majeur, le patient incapable majeur et le patient mineur disposant des capacités de discernement nécessaires peuvent s'opposer à la consultation après leur mort de leur dossier médical. Ce texte précise encore que la personne de confiance peut aussi demander à consulter le dossier médical. Enfin, les demandeurs devront justifier les raisons pour lesquelles ils souhaitent consulter le dossier[21]. La Commission nationale estime que les finalités pour lesquelles le demandeur demande l'accès doivent être déterminées et légitimes. L'énumération des raisons pour lesquelles l'accès est permis n'est pas particulièrement critiquable. Toutefois, ces raisons ne doivent pas être appréciées par la personne qui donne l'accès au dossier : seules les instances et les services compétents pourront se prononcer sur un éventuel détournement de finalités, s'il s'avérerait que le demandeur n'avait pas respecté les finalités énumérées à l'article 19 du projet de loi.

Compte tenu de l'incohérence entre l'article 28 de la loi du 2 août 2002 et l'article 19 du texte sous examen, la Commission nationale suggère l'abrogation du paragraphe (3) dudit article 28 qui était la reprise de l'article 36 alinéa 5 de la loi du 28 août 1998[22], article qui est appelé à être entièrement refondé selon l'article 24 du texte sous examen.

Articles 20 à 23 : Médiation dans le domaine de la santé

L'article 21 du texte sous examen prévoit les services hospitaliers de médiation (article 21) et l'article 22 le Service national de médiation dans le domaine de la santé (article 22). Ces dispositions ne mettent pas en cause les prérogatives de la Commission nationale conférées par la loi du 2 août 2002 en vue de faire respecter les droits des patients, de leurs représentants ou de leurs proches.

Il y a lieu de noter que le projet de loi n°6272[23] introduit la médiation civile et commerciale dans le Nouveau Code de la procédure civile (ci-après : le NCPC). Il ressort de l'économie de l'article 1251-1 paragraphe (2) du NCPC que le projet de loi n°6272 propose d'introduire que le domaine de la médiation peut également couvrir celui de la santé. La Commission nationale se demande dès lors s'il n'existe pas un risque que deux processus de médiation soient ouverts concomitamment pour une même affaire sans qu'il ne soit prévu qu'un service se dessaisisse au profit d'un autre.

---

[21] Exception faite si le patient était mineur.
[22] Travaux parlementaires 4735/13 page 26.
[23] Projet de loi n°6272 portant – introduction de la médiation en matière civile et commerciale dans le Nouveau Code de la procédure civile ; - transposition de la directive 2008/52/CE du Parlement européen et du Conseil du 21 mai 2008 sur certains aspects de la médiation en matière civile et commerciale ; - et modification de la loi modifiée du 10 août 1991 sur la profession d'avocat.

Une autre différence surgit entre le texte sous avis et le projet de loi n°6272 en ce qui concerne les pouvoirs du médiateur. En effet, et comme le relève le Collège Médical dans son avis du 18 mai 2011, le texte sous examen attribue des pouvoirs d'investigation au médiateur. Or, le considérant (13) de la directive 2008/52/CE du 21 mai 2008 sur certains aspects de la médiation en matière civile et commerciale que le projet de loi n°6272 entend transposer, insiste sur le fait que la médiation est *« un processus volontaire en ce sens que les parties elles-mêmes sont responsables du processus et peuvent l'organiser comme elles l'entendent (…) »*. Respectant le sens et la portée de cette disposition, l'article 1251-2 paragraphe (2) du NCPC en préparation prévoit encore que *« le médiateur ne dispose pas de pouvoir d'instruction [mais que] toutefois il peut avec l'accord des parties entendre les tiers qui y consentent »*. La Commission nationale est d'avis que le médiateur dans le domaine de la santé devrait avoir des prérogatives identiques à celles qui sont prévues dans le projet de loi n°6272.

Elle s'interroge également sur l'indépendance et l'impartialité du médiateur intervenant dans les services hospitaliers de médiation. En effet, bien que l'avant-projet entende donner des garanties relatives à l'indépendance et à l'impartialité des médiateurs, la Commission nationale constate que, dans un établissement hospitalier, l'organisme gestionnaire met en place le service de la médiation[24]. Or, l'article 3 de la directive précitée 2008/52/CE définit le médiateur comme *« tout tiers sollicité pour mener une médiation avec efficacité, impartialité et compétence (…), »* et l'article 1251-2 paragraphe (2) du NCPC en préparation stipule que le médiateur est *« tout tiers sollicité pour mener une médiation avec efficacité, impartialité et compétence »*. Il résulte des travaux préparatoires du projet de loi n°6272 que les parties à la médiation doivent pouvoir choisir en toute liberté le médiateur qui sera chargé de leur plainte. Ainsi, la Commission nationale est d'avis que, compte tenu des liens entre les médiateurs et l'organisme gestionnaire de l'établissement hospitalier, les patients et toutes les personnes qui souhaiteront déposer une plainte pourraient avoir le sentiment que les médiateurs intervenant dans le service hospitalier ne disposent pas des qualités d'indépendance et d'impartialité pour traiter leur demande. Par conséquent, la Commission nationale suggère que l'organisme gestionnaire n'intervienne pas dans la désignation des médiateurs, ce choix devant être libre, à l'instar de ce que le projet de loi n°6272 propose.

Enfin, la CNPD constate que jusqu'à cinq intervenants différents peuvent être saisis en cas de réclamation ou de plainte dans le domaine de la santé (en dehors de toute procédure contentieuse), à savoir :

- un médiateur dans le cadre de la procédure prévue dans le NCPC envisagée dans le projet de loi n°6272,

- le médiateur du service hospitalier de médiation,

- le Service national de médiation dans le domaine de la Santé,

- le Directeur de la Santé, selon l'article 24 du projet de loi sous examen, et

- la Commission nationale.

Les différents textes n'ont prévu que l'hypothèse d'un désistement entre les instances du service hospitalier de médiation et le Service national de médiation, pour le reste aucun désistement n'est organisé. Il ne ressort pas non plus des différents textes que les différents intervenants potentiels seront formellement informés des plaintes ouvertes et traitées par les autres intervenants. Par conséquent, il existe une certaine incohérence entre les différents textes ci-avant cités et, à cause de la différence de régime entre les différentes procédures, une insécurité juridique risque d'apparaître.

[24] Article 21 paragraphe (1) de l'avant-projet de loi.

7 Annexes

Ainsi décidé à Luxembourg
en date du 28 octobre 2011.

La Commission nationale pour
la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

Avis concernant le projet de loi n°6325 relatif à la mise en application du règlement (UE) n°211/2011 du Parlement européen et du Conseil du 16 février 2001 relatif à l'initiative citoyenne

Délibération n°378/2011
du 11 novembre 2011

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 « la loi modifiée du 2 août 2002 »), la Commission nationale pour la protection des données (ci-après « la Commission nationale ») a notamment pour mission d'*« être demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi »*.

Par courrier du 1er août 2011, Monsieur le Ministre des Communications et des Médias a invité la Commission nationale à se prononcer au sujet de l'avant-projet de loi relative à la mise en application du Règlement (UE) n°211/2011 du Parlement européen et du Conseil du 16 février 2011 relatif à l'initiative citoyenne, déposé à la Chambre des Députés comme projet de loi

n°6325 en date du 6 septembre 2011.

L'initiative citoyenne constitue une nouvelle forme de participation politique à destination des citoyens européens. Une telle initiative consiste en la possibilité pour un million de citoyens européens, provenant d'un quart des Etats membres, d'inviter la Commission européenne à faire une proposition d'acte juridique sur un sujet qui leur paraît important. Le règlement (UE) n°211/2011 du Parlement européen et du Conseil du 16 février 2011 établit les procédures et conditions pour une telle initiative citoyenne et il sera directement applicable en droit interne à partir du 1er avril 2012. Le projet de loi sous analyse a pour objet de préciser les mesures concrètes d'application au niveau national de ce règlement.

Le projet de loi, dans son article 4, autorise la collecte et l'utilisation du numéro d'identification personnel des signataires d'une initiative citoyenne. Plus précisément, cet article permet aux organisateurs d'une initiative citoyenne de traiter le numéro d'identité, tel que défini par la loi modifiée du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales, et plus communément connu sous les termes de « matricule » ou « d'identifiant unique ».

Alors que la Commission nationale peut comprendre que l'utilisation d'un tel identifiant unique peut présenter certains avantages pratiques, elle tient à relever que cette utilisation présente également de nombreux risques significatifs au niveau des atteintes aux libertés et droits des citoyens.

Afin d'essayer de limiter ces risques, certains textes internationaux sont venus apporter des précisions et limitations à la mise en place et l'utilisation de tels identifiants uniques. Ainsi, 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[25] et 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[26] (transposée en droit interne par la loi du 2 août 2002) exigent que des « garanties appropriées » devront être mises en place dans le cadre de l'utilisation d'un numéro d'identification unique afin d'éviter des abus potentiels.

La nécessité de telles « garanties appropriées » avait déjà été identifiée par le législateur luxembourgeois lors de l'adoption de la loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales. Le principe général contenu dans ce texte est que le numéro d'identification unique doit rester confidentiel à l'égard des tiers. En effet, ledit numéro est réservé à un usage administratif interne et aux relations avec le titulaire du numéro[27]. Par ailleurs, les fichiers qui peuvent contenir le numéro d'identité doivent être autorisés par voie de règlement grand-ducal.

Toujours est-il qu'en pratique il a été fait abstraction, au fur et à mesure, de ces dispositions et l'utilisation du numéro d'identité s'est largement répandue et n'est pas restée cantonnée au domaine des relations entre administrations et administrés (cf. réponse de Monsieur le Ministre des Communications Jean-Louis Schiltz du 12 juin 2006 à la question parlementaire du 4 juin 2006 n°1.056 posée par l'honorable députée Madame Colette Flesch[28]), de sorte que le gouvernement a pris l'initiative de réformer le système actuel, tout en prenant en compte les nécessités des divers acteurs ainsi que la mise en place de garanties juridiques et techniques permettant d'assurer les principes régissant la protection des données à caractère personnel[29].

Le projet de loi n°6330 (qui opère la fusion entre les projets de loi nos 5949 et 5950)

---

[25] Recommandation (86)1 relative à la protection des données à caractère personnel utilisées à des fins de sécurité sociale – Annexe – paragraphe 5 et Recommandation (86)1 – Exposée des motifs - Points 34. et 35.

[26] Article 8, point 7 de la directive 95/46/CE du 24 octobre 1995 « 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 ».

[27] Loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales, article 5.

[28] « Des évolutions récentes montrent également que l'utilisation fréquente du numéro d'identité national dans les procédures et usages administratifs vient de diluer la ligne de démarcation entre les usages licites et non licites dudit numéro tel qu'elle avait été tracée par la loi de 1979. … ».

[29] Pour une analyse complète de la problématique du numéro d'identification unique, la Commission nationale tient à renvoyer à son avis n°48/2009 du 10 mars 2009 portant sur 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.

a, entre autres, pour objet de mettre en œuvre cette réforme relative à l'identifiant unique. S'il est prévu d'élargir l'utilisation du numéro d'identification à des entités privées (commerçants, artisans, personnes morales de droit privé, etc.), il faut noter que l'utilisation par des acteurs privés ne sera permise que sous certaines conditions restrictives. De manière générale, le projet de loi n°6330, dans son article 2, maintient le principe que l'utilisation du matricule ne doit pas être possible pour tout un chacun.

Alors même que l'adoption de l'article 2 paragraphe 5 du projet de loi n°6330 rendrait possible l'utilisation du numéro d'identification dans le cadre d'une initiative citoyenne, la Commission nationale estime que des garanties appropriées, pourtant exigées par les textes européens mentionnés plus haut, feraient défaut.

Aux termes de l'article 5 paragraphe 2 du règlement (UE) n°211/2011 précité, les déclarations de soutien d'une initiative citoyenne peuvent être recueillis par voie électronique ou sur papier. Il ressort de l'annexe III, partie B (modèle de formulaire de déclaration de soutien) que les données à y renseigner comportent les catégories suivantes :

- prénoms complèts,
- noms de famille,
- résidence permanente,
- lieu de naissance,
- nationalité,
- numéro d'identification personnel,
- date et signature.

En pratique, un tel formulaire aura donc vocation à circuler entre les différents signataires de l'initiative citoyenne, afin qu'ils puissent y déclarer leur soutien. Il est fort probable que les signataires recevront communication des données personnelles des autres signataires. Les organisateurs d'une initiative citoyenne auront par ailleurs accès aux données personnelles, y compris le numéro d'identification de l'ensemble des signataires. Les risques potentiels d'abus par les signataires ou les organisateurs lors de la collecte des données ainsi que les risques de détournement de finalité ne peuvent pas être écartés. A l'aide des nouvelles technologies il sera notamment aisé de copier les données dans un fichier.

La Commission nationale est donc à se demander pourquoi le Grand-Duché de Luxembourg a opté pour l'utilisation du matricule[30]. Certains Etats membres qui disposent également d'un numéro d'identification ont fait le choix de ne pas faire figurer ce dernier sur les formulaires de déclaration de soutien (tel que la Belgique, p.ex.). En prenant en compte que le nombre minimum de signataires

[30] Donnée désignée par la doctrine comme « la donnée personnelle ultime » dans La protection des données personnelles, Cyril Pierre-Beausse, Promoculture, page 32.

est de 4.500 pour le Luxembourg (celui de la Belgique étant de 16.500) la CNPD considère qu'il n'est pas nécessaire de collecter le numéro d'identité et que l'ensemble de toutes les autres données personnelles recueillies à l'occasion d'une initiative citoyenne devraient amplement suffire pour procéder aux vérifications de l'identité des signataires. Pour toutes les raisons exposées, la Commission nationale recommande de ne pas avoir recours au numéro d'identification national dans le cadre d'une initiative citoyenne.

Sa position reflète par ailleurs l'opinion adoptée par le Contrôleur européen de la protection des données en la matière. Dans son avis du 21 avril 2010 relatif au règlement 211/2010[31], le CEPD estime notamment que « … *les champs d'information obligatoires sur le formulaire type sont tous nécessaires pour organiser l'initiative citoyenne et garantir l'authenticité des déclarations de soutien, à l'exception du numéro d'identification personnel.* … » et « *En tout état de cause, le CEPD ne perçoit pas la valeur ajoutée de l'identification personnelle aux fins de vérifier l'authenticité des déclarations de soutien. Les autres informations demandées peuvent déjà être considérées comme suffisantes pour réaliser cet objectif. Le CEPD recommande dès lors de supprimer ce champ d'information du formulaire type figurant à l'annexe III* ».

Pour le surplus, la Commission nationale pour la protection des données note avec satisfaction que les auteurs du projet de loi ont transposé, dans l'article 5, les principes retenus à l'article 12 du règlement (UE) n°211/2011, principes généraux qui se dégagent également des dispositions la loi-cadre modifiée du 2 août 2002.

Ainsi, le paragraphe (2) de l'article 5 détermine les responsables du traitement dans le cadre d'une initiative citoyenne. Suivant cette disposition, sont considérés comme responsables du traitement d'une part les organisateurs d'une initiative citoyenne et d'autre part le CTIE. Le paragraphe (3) dudit article, limite la finalité du traitement de données dans le cadre d'une initiative citoyenne et prévoit l'obligation pour les organisateurs de détruire les données endéans un délai clairement défini. Dans le même ordre d'idées, le paragraphe (4) de l'article 5 prévoit des limitations similaires pour le CTIE. Une conservation au-delà de ces délais indiqués peut uniquemement être envisagée dans le cadre d'une procédure judiciaire ou administrative concernant la proposition d'initiative citoyenne (paragraphe (5), article 5).

Ainsi décidé à Luxembourg en date du 11 novembre 2011.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

[31] Avis du Contrôleur européen de la protection des données sur la proposition de règlement du Parlement européen et du Conseil relatif à l'initiative européenne (2010/C 323/01) du 21 avril 2010.

7 Annexes

Participations aux travaux européens

Documents adoptés par le groupe de travail « Article 29 » en 2011

Document	Date d'adoption	Référence
Avis 16/2011 sur les meilleurs pratiques d'IAB Europe et de l'EASA en matière de publicité comportementale en ligne	08.12.2011	WP 188
Avis 15/2011 sur la définition du consentement	13.07.2011	WP 187
Avis 14/2011 sur les questions de protection des données relatives à la prévention du blanchiment de capitaux et du financement du terrorisme	13.06.2011	WP 186
Avis 13/2011 sur les services de géolocalisation des dispositifs mobiles intelligents	16.05.2011	WP 185
Document de travail 01/2011 concernant le cadre juridique relatif aux violations de données à caractère personnel actuellement en vigueur dans l'UE et présentant des recommandations quant aux actions à entreprendre à l'avenir	05.04.2011	WP 184
Avis 12/2011 sur les compteurs intelligents	04.04.2011	WP 183
Avis 11/2011 relatif au niveau de protection des données à caractère personnel assuré en Nouvelle-Zélande	04.04.2011	WP 182
Avis 10/2011 sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière	05.04.2011	WP 181
Avis 9/2011 sur la proposition révisée des entreprises relative au cadre d'évaluation de l'impact sur la protection des données et de la vie privée des applications reposant sur l'identification par radiofréquence (RFID)	11.02.2011	WP 180

Groupe de travail « Article 29 » – « Avis 10/2011 sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière »

Adopté le 5 avril 2011

1. Introduction

Le 2 février 2011, la Commission européenne a présenté sa proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière. Le groupe de travail avait rendu un avis sur la proposition précédente de l'UE en matière de données PNR [la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (PNR) à des fins répressives], qui avait été présentée par la Commission le 6 novembre 2007[32]. Par le passé, le groupe de travail a également formulé, dans plusieurs avis, de nombreuses observations sur les différents accords PNR conclus entre l'UE et des pays tiers, ainsi que sur la démarche de la Commission définie dans sa communication du 21 septembre 2010[33]. En outre, il a rappelé ses préoccupations au sujet des questions que soulèvent les dossiers PNR dans différentes lettres adressées au commissaire Barrot, à la commissaire Malmström, au directeur général Jonathan Faull et à la commission LIBE du Parlement européen.

Le présent avis s'adresse aux parties associées à l'élaboration de la dernière proposition présentée dans ce domaine et aux discussions à son sujet, à savoir la Commission, le groupe de travail GENVAL du Conseil et le Parlement européen.

2. Nécessité et proportionnalité

La proposition de 2011 s'accompagne d'une analyse d'impact qui vise à présenter de manière plus détaillée la raison d'être de la proposition et de ses dispositions. Le groupe de travail considère que la lutte contre le terrorisme et la criminalité organisée est nécessaire et légitime et que les données à caractère personnel, et en particulier certaines données relatives aux passagers, peuvent être utiles pour évaluer les risques ainsi que pour prévenir et combattre le terrorisme et la criminalité organisée. Cependant, s'agissant d'un système PNR européen, il est indispensable que la restriction des libertés et droits fondamentaux soit dûment justifiée et que sa nécessité soit clairement établie afin de trouver le juste équilibre entre les exigences de la protection de la sécurité publique et la limitation des droits en matière de respect de la vie privée.

Le groupe de travail a invariablement mis en doute la nécessité et la proportionnalité des systèmes PNR et maintient cette position à l'égard de la proposition de 2011. S'il reconnaît la valeur des précisions supplémentaires fournies dans l'analyse d'impact, il estime que cette analyse ne contient pas d'évaluation appropriée de l'utilisation des données PNR et ne prouve pas la nécessité de la proposition. Celle-ci devrait indiquer clairement si elle a pour objectif de lutter contre les formes graves de criminalité (transnationale), dont le terrorisme, ou si elle a pour objet de lutter uniquement contre le terrorisme et les infractions liées au terrorisme. Le point 3.2 de l'analyse d'impact intitulé « Respect des droits fondamentaux » se borne à indiquer que la « check-list droits fondamentaux » a été utilisée, mais il ne contient aucune autre information pouvant justifier les conclusions qu'il en tire. En outre, ce point de l'analyse d'impact présente un

[32] WP 145 – avis commun adopté conjointement avec le groupe de travail sur la police et la justice.
[33] Avis WP 103 (Canada), WP 138 (États-Unis), WP 151 (États-Unis - information des passagers) et WP 178 (démarche globale de la Commission).

raisonnement circulaire en ce qui concerne les atteintes aux droits en matière de respect de la vie privée consacré à l'article 8 de la convention européenne des droits de l'homme, et aux articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne. Pour être légale, une atteinte à ces droits doit en effet être « nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui », et être « nécessaire dans une société démocratique », « sous réserve du respect du principe de proportionnalité ». Le fait que l'objectif de la proposition soit la prévention du terrorisme et des formes graves de criminalité ne signifie pas qu'elle satisfait clairement à ces conditions; il faut encore établir sa nécessité et sa proportionnalité. La Commission, dans sa propre présentation générale des systèmes de gestion de l'information[34], s'exprime en ces termes :

« Nécessité
L'ingérence d'une autorité publique dans l'exercice par les personnes de leur droit au respect de leur vie privée peut être nécessaire dans l'intérêt de la sécurité nationale, de la sûreté publique ou de la prévention de la criminalité. La jurisprudence de la Cour européenne des droits de l'homme établit trois conditions auxquelles ces restrictions peuvent être justifiées : si elles sont prévues par la loi, si elles poursuivent un but légitime et si elles sont nécessaires dans une société démocratique. L'ingérence dans le droit au respect de la vie privée est considérée comme nécessaire si elle répond à un besoin social impérieux, si elle est proportionnée au but poursuivi et si les motifs invoqués par les autorités publiques pour la justifier apparaissent pertinents et suffisants. Dans toutes ses futures propositions, la Commission évaluera l'incidence attendue de l'initiative en question sur le droit des personnes au respect de la vie privée et à la protection des données à caractère personnel et précisera en quoi cette incidence est nécessaire et en quoi la solution proposée est proportionnée au but légitime que constituent le maintien de la sécurité intérieure dans l'Union européenne, la prévention de la criminalité ou la gestion des flux migratoires ».

Le groupe de travail ne pense pas que la Commission a rempli les engagements dont il est fait état ci-dessus en ce qui concerne la proposition de l'UE en matière de PNR. Les arguments relatifs à la nécessité et à la proportionnalité recouvrent plusieurs autres aspects qui sont également examinés ci-dessous.

[34] Présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice, COM(2010) 385 final.

2.1. Sécurité accrue

La proposition et l'analyse d'impact indiquent que le système PNR de l'UE garantirait la sécurité et préviendrait les failles résultant de la suppression des contrôles aux frontières intérieures en vertu de la convention de Schengen. Cet objectif serait légitime s'il était dûment justifié; le groupe de travail constate toutefois qu'aucun élément probant satisfaisant n'a encore été présenté pour démontrer que le fait que les données PNR soient traitées dans tous les États membres éviterait les failles en matière de sécurité qui résulteraient du traitement de ces données dans quelques États membres seulement.

Il existe déjà des systèmes et des instruments au niveau de l'UE, prévus par l'« acquis de Schengen », pour contrebalancer la suppression des contrôles aux frontières entre les pays de l'espace Schengen, de sorte que si des failles demeurent sur le plan de la sécurité, la première mesure à prendre serait de vérifier si les systèmes existants fonctionnent correctement.

2.2. Coopération existante et instruments et systèmes déjà en place

Dans sa présentation générale des systèmes de gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice, la Commission n'a pas évalué l'efficacité des différents systèmes existants; elle ne s'est pas davantage posé la question de savoir si, considérés dans leur ensemble, ils offrent les instruments appropriés pour combattre le terrorisme et la criminalité organisée et, dans la négative, où se situeraient les failles. Le groupe de travail estime qu'une telle évaluation est indispensable avant d'imposer de nouvelles mesures de nature analogue, comme un système PNR de l'UE. La proposition PNR entraînera un chevauchement des obligations imposées aux transporteurs et obligera à recueillir des données déjà disponibles par l'intermédiaire d'autres systèmes; elle présente en outre un risque sérieux de détournement d'usage. La directive 2004/82/CE du Conseil concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers (dite « directive API ») oblige par exemple les transporteurs à communiquer à l'avance les informations relatives aux passagers, l'utilisation de ces données ne se limitant pas aux contrôles aux frontières, mais pouvant aussi s'étendre à des fins de maintien de l'ordre. Bien qu'il ait porté cette question plusieurs fois à l'attention de la Commission, le groupe de travail attend toujours une évaluation en bonne et due forme de l'efficacité de la directive API et de sa mise en œuvre au niveau national, et s'interroge sur l'utilité de maintenir cette directive si un système PNR applicable à toute l'UE est introduit.

Le groupe de travail se demande si toutes les formes de coopération policière et judiciaire en place dans l'UE et ayant pour but de prévenir et de poursuivre les infractions, et notamment de lutter contre le terrorisme et les formes graves de criminalité, ne constituent pas des instruments adéquats pour atteindre les objectifs que la proposition de système PNR de l'UE entend remplir. Cette question n'a pas été examinée dans le cadre de l'analyse d'impact.

Le groupe de travail reconnaît que certains des États n'appartenant pas à l'espace Schengen ne peuvent profiter de tous ces instruments et systèmes existants, ce qui n'est pas sans incidence sur l'application du critère de nécessité à ces pays. Toutefois, ces États membres peuvent appliquer la directive API, ce qu'ils font d'ailleurs, et il y a lieu de se demander si une meilleure utilisation des systèmes existants et un renforcement de la coopération entre ces États membres et les autres ne permettraient pas d'obtenir les informations nécessaires aux finalités recherchées. Il convient également de faire observer que le fait que les données PNR soient utilisées comme outil de

renseignement, comme l'indique l'analyse d'impact, entraîne aussi un relèvement du niveau des exigences en ce qui concerne les garanties relatives à la protection des données.

2.3. Proportionnalité

La proposition prévoit la collecte d'un volume très important de renseignements à caractère personnel relatifs à l'ensemble des passagers aériens arrivant dans l'UE ou quittant son territoire, que ceux-ci soient suspects ou non. La collecte et le traitement des données PNR aux fins de la lutte contre le terrorisme et les formes graves de criminalité ne devraient pas permettre de suivre à la trace et de surveiller l'ensemble des voyageurs sans distinction. Selon le groupe de travail, il est disproportionné et, partant, contraire à l'article 8 de la charte des droits fondamentaux de recueillir et de conserver l'ensemble des données relatives à tous les voyageurs sur la totalité des vols. Comme indiqué ci-dessus, l'analyse d'impact ne comprend aucun élément de preuve convaincant à cet égard. Les propositions présentées au niveau de l'UE doivent être spécifiques et ciblées afin de résoudre un problème particulier et, dans ce contexte, toute proposition doit être axée sur les risques que posent le terrorisme et les formes graves de criminalité.

Le groupe de travail nourrit de sérieux doutes quant à la proportionnalité de la mise en concordance systématique de l'ensemble des passagers avec certains critères préétablis et des « bases de données pertinentes » qui ne font l'objet d'aucune autre précision. Aucun élément de la proposition n'indique clairement comment ces critères préétablis et ces bases de données pertinentes seront définis, si les données PNR seront utilisées pour créer ou mettre à jour les critères, ni dans quelle mesure les correspondances feront toutes automatiquement l'objet de recherches complémentaires. Le groupe de travail souhaiterait aussi rappeler que, dans certains États membres, les méthodes de surveillance (policière) de cette nature ne sont constitutionnelles et, partant, ne peuvent être utilisées par la police qu'après accord des autorités judiciaires et dans des circonstances particulières, comme en cas de menace spécifique. Le système PNR proposé ferait de cette méthode exceptionnelle un instrument ordinaire dans le cadre du travail de la police.

Les mesures qui ne peuvent garantir la protection des droits et libertés des voyageurs ne sont proportionnées que si elles sont introduites à titre temporaire pour contrer une menace spécifique, ce qui n'est pas le cas de la proposition dont il est question ici. L'atteinte à la vie privée des

voyageurs doit être proportionnée à l'utilité de la proposition sur le plan de la lutte contre le terrorisme et les formes graves de criminalité. Le groupe de travail attend toujours de voir des statistiques indiquant le rapport entre le nombre de voyageurs innocents dont les données PNR ont été recueillies et le nombre de fois où ces données PNR ont abouti à des résultats sur le plan du maintien de l'ordre.

En résumé, le groupe de travail continue de penser que la nécessité du système n'a pas été établie et que les mesures proposées sont contraires au principe de proportionnalité. En dépit de cette conclusion, il juge constructif de commenter également d'autres aspects de la proposition de directive.

3. Finalités

La proposition de directive prévoit deux finalités générales et quatre activités spécifiques en ce qui concerne le traitement des données PNR. Les données PNR ne peuvent faire l'objet d'un traitement qu'aux fins :

- de la prévention et de la détection d'infractions terroristes et d'infractions graves, ainsi que d'enquêtes ou de poursuites en la matière, en évaluant les passagers avant l'arrivée ou le départ grâce à une confrontation des données avec celles figurant dans des bases de données pertinentes (finalité 1, activité 1) et grâce aux réponses apportées aux demandes des autorités compétentes dans des cas spécifiques (finalité 1, activité 2) ; et
- de la prévention et la détection d'infractions terroristes et d'infractions transnationales graves, ainsi que d'enquêtes ou de poursuites en la matière, en évaluant les passagers avant l'arrivée ou le départ par rapport à des critères déterminés (finalité 2, activité 3) et en analysant les données PNR afin de mettre à jour ces critères ou d'en définir de nouveaux (finalité 2, activité 4).

Il est difficile de savoir avec certitude ce que ces finalités recouvrent dans la pratique. La finalité 1, activité 1, semble impliquer de mettre en concordance les données PNR avec les listes de personnes à surveiller, le SIS ou d'autres bases de données établies au niveau national ou de l'UE. La finalité 1, activité 2, semble faire référence à un partage d'informations au cas par cas, à la suite d'une demande spécifique. La finalité 2, activité 3, semble impliquer de confronter les données PNR aux profils établis pour des infractions spécifiques, et la finalité 2, activité 4, semble renvoyer à l'utilisation des données PNR pour définir ces profils.

La définition stricte des finalités et activités est l'un des principes essentiels en matière de protection des données. Les « bases de données pertinentes » devraient être définies de manière plus précise, éventuellement en les ajoutant à la liste des autorités compétentes que chaque État membre devrait fournir à la Commission. En tout état de cause, les bases de données utilisées devraient être celles établies pour les mêmes finalités, à savoir la prévention et la détection d'infractions terroristes et d'infractions graves, ainsi que les enquêtes ou poursuites en la matière. En outre, les mesures d'application doivent être claires en ce qui concerne les restrictions à l'utilisation de ces bases de données. Le groupe de travail rappelle également l'importance de veiller à ce que les critères d'évaluation utilisés par les États membres pour analyser les données soient spécifiques, nécessaires, justifiés et régulièrement réexaminés.

3.1. Définitions

La proposition définit les « infractions terroristes » comme les infractions en droit national visées aux articles 1er à 4 de la décision-cadre 2002/475/JAI du Conseil. Les « infractions graves » et les « infractions transnationales graves » sont définies comme les infractions en droit national visées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI du Conseil. Le groupe de

travail souligne l'importance de définitions concrètes dans ce domaine ; il faut cependant constater que la définition des infractions graves est plutôt large, ce qui amène le groupe de travail à s'interroger sur la nécessité et la proportionnalité de l'utilisation des données PNR pour certaines de ces infractions.

À ce sujet, le considérant 12 de la proposition indique que les États membres peuvent exclure les infractions mineures au cas où le traitement de données PNR ne serait pas conforme au principe de proportionnalité, mais cette décision est laissée au libre choix de chaque État membre, de sorte que ces infractions pourraient se trouver exclues dans un État membre et pas dans un autre. Il est difficile de savoir avec certitude qui prend la décision sur la proportionnalité et si cette décision doit être portée à la connaissance de la Commission, laquelle pourrait avoir un rôle à jouer en vue de garantir la cohérence et l'application correcte du principe de proportionnalité.

Les préoccupations du groupe de travail au sujet du champ potentiellement très large de la définition des infractions graves s'appliquent aussi aux dispositions de la directive proposée relatives au partage de données avec d'autres autorités tant sur le territoire de l'UE qu'en dehors de celui-ci.

4. Conservation

Les durées de conservation proposées sont clairement réduites par rapport à la proposition précédente et aux divers accords PNR conclus au niveau de l'UE. Toutefois, le groupe de travail considère toujours que la proposition de conserver les données pendant cinq ans est disproportionnée, même si les données sont masquées. Dans le cadre des systèmes PNR, l'un des sujets de préoccupation tient depuis longtemps au fait que toutes les données concernant l'ensemble des voyageurs sont conservées pour une durée identique et que cette durée de conservation est, en soi, disproportionnée. Selon le groupe de travail, il n'a pas été démontré de manière suffisamment convaincante que les données de l'ensemble des voyageurs doivent être conservées ni qu'elles doivent être conservées pendant cinq ans.

4.1. Masquage des données

Alors que la proposition indique que les données seront masquées après 30 jours et, en règle générale, uniquement accessibles à certains membres du personnel des unités de renseignements passagers dont le rôle est de définir des profils et des structures de déplacement, un accès intégral à toutes les données demeurerait possible pendant

toute la durée de conservation. Même si le masquage constitue un effort de limitation des données et de contrôle d'accès, qui sont des principes importants dans le domaine de la protection des données, le groupe de travail continue de s'interroger sur la raison pour laquelle l'ensemble des données de tous les voyageurs sont nécessaires, et il estime que les données des voyageurs non suspects devraient être effacées.

Si le législateur décidait de conserver les données pour une durée limitée, les données devraient être protégées de manière à ce que les éléments permettant l'identification ne soient pas divulgués. Cette protection devrait être en place au plus tard à l'arrivée du vol. L'accès aux données protégées afin d'obtenir des éléments permettant l'identification devrait être subordonné à une décision judiciaire prise au cas par cas dans le cadre d'une enquête pénale spécifique.

Le groupe de travail souhaiterait aussi souligner avec force la nécessité d'utiliser un langage précis qui ne sème pas la confusion ni n'induise en erreur. La proposition fait mention tant du masquage que de l'anonymisation. Or, ces deux termes ne sont pas synonymes, et il est clair que c'est de masquage dont il s'agit, et non d'anonymisation, puisque les données permettant l'identification d'une personne continuent de pouvoir être facilement extraites. La proposition ne devrait pas semer la confusion ou induire en erreur, à dessein ou non, ni promettre l'impossible.

5. Droits individuels en matière de protection des données

La proposition contient des dispositions se rapportant spécifiquement à la protection des données. Le groupe de travail estime nécessaire que toute proposition présentée au niveau de l'UE et ayant une incidence sur les droits et libertés des citoyens contienne des dispositions prévoyant des droits individuels d'accès et de rectification, ainsi que des droits individuels à réparation et à un recours juridictionnel. Or, les droits prévus par la proposition examinée sont ceux conférés par la décision-cadre 2008/977/JAI, et non ceux prévus par la directive 95/46/CE, et sont par conséquent plus limités. Il est difficile de savoir avec certitude si les droits s'appliquent uniquement aux données transférées à une autre autorité, ou comprennent les données conservées par l'autorité nationale. Dans certains États membres qui utilisent actuellement les données PNR, les personnes concernées disposent de droits d'accès et de rectification ainsi que d'un droit à un recours juridictionnel au titre de la législation nationale qui transpose la directive 95/46/CE ; ces droits seront réduits si la proposition de directive en matière de PNR entre en vigueur.

Il existe également un risque de discrimination du fait de l'activité de profilage puisque ce système cible les passagers aériens en tant que groupe. Les passagers ne reçoivent aucune information au sujet des critères au regard desquels ils sont évalués, ce qui a une incidence sur l'exercice des droits des personnes directement concernées par l'activité de profilage.

Le groupe de travail rappelle l'importance d'inclure, dans les propositions au niveau de l'UE qui ont une incidence sur les droits et libertés des citoyens, des garanties et mesures appropriées en matière de protection des données, comme des règles relatives à la confidentialité et au traitement sécurisé, des obligations d'informer les citoyens, l'interdiction de transférer des données à des acteurs privés, et une disposition prévoyant qu'aucune décision ne peut être prise sur la base d'un traitement automatisé uniquement. Le groupe de travail souligne également qu'il ne faut pas négliger de faire mention des autorités nationales de surveillance qui jouent un rôle au niveau national dans la mise en œuvre de la législation adoptée au niveau de l'UE.

En ce qui concerne les données sensibles, la proposition indique que le filtrage et la suppression de ces données devraient être réalisés par l'unité de renseignements passagers. Dans les avis qu'il a rendus sur les différents accords PNR conclus par l'UE avec des pays tiers, le groupe de travail a toujours soutenu l'interdiction de traiter les données sensibles dans ce contexte, et il réaffirme avec force le point de vue qu'il défend de longue date selon lequel le filtrage devrait être effectué par le transporteur avant que les données ne soient transmises à l'autorité destinataire.

Le groupe de travail souligne combien il est essentiel de veiller à ce que les propositions présentées au niveau de l'UE qui portent atteinte aux droits et libertés des citoyens prévoient des obligations de surveillance et de réexamen, comme la journalisation des demandes de données et des opérations de traitement à des fins de vérification de la licéité du traitement, d'autocontrôle et de garantie de l'intégrité des données et de la sécurité du traitement des données par les autorités nationales de contrôle de la protection des données. Il est toutefois indispensable de comprendre comment ces systèmes fonctionneront en pratique et comment la journalisation et la documentation effectives permettront de respecter les principes de limitation des données comme indiqué ci-dessus.

6. Éléments de données

Contrairement aux données API, les données PNR ne sont pas vérifiées et sont, par conséquent, moins fiables. Les éléments de données énumérés en annexe de la proposition examinée sont les mêmes que les dix-neuf éléments figurant dans les accords PNR conclus entre l'UE et les États-Unis et entre l'UE et le Canada. Le groupe de travail maintient sa position selon laquelle aucun élément de preuve satisfaisant ne permet de connaître les champs qui se sont avérés nécessaires, de sorte qu'une telle liste est disproportionnée. Les catégories sont générales, et plusieurs comportent en outre des sous-ensembles de données.

Alors même que le traitement des données à caractère personnel sensibles est interdit, la liste des éléments de données comprend le champ « remarques générales » qui pourrait contenir des informations de toutes sortes, comme les demandes relatives aux repas, les demandes relatives à des services particuliers, etc. Selon le groupe de travail, aucun élément de preuve satisfaisant ne permet d'établir quels éléments des données PNR se sont avérés nécessaires ou ont produit des résultats à des fins de maintien de l'ordre. En outre, il faut constater

que les données PNR ne sont pas recueillies par tous les transporteurs.

7. Autorités compétentes et transferts ultérieurs

Selon la proposition, les États membres doivent communiquer à la Commission la liste de leurs autorités compétentes dans un délai maximal de douze mois à compter de l'entrée en vigueur de la directive, cette liste étant ensuite publiée au Journal officiel. Le groupe de travail soutient les mesures de transparence qui permettent de connaître précisément les autorités habilitées à recevoir et à traiter les données. Cependant, la répartition des rôles (responsable du traitement/sous-traitant) entre les autorités compétentes et les unités de renseignements passagers n'est pas claire. Le groupe de travail fait une nouvelle fois part de ses préoccupations quant à la définition très large des infractions graves notamment par rapport aux transferts ultérieurs, tant sur le territoire de l'UE qu'en dehors de celui-ci.

8. Réexamen et réciprocité

Selon la proposition, la directive fera l'objet d'un réexamen dans un délai de quatre ans à compter de son entrée en vigueur. Un réexamen spécial aura lieu dans un délai de deux ans à compter de l'entrée en vigueur de la directive afin de voir s'il convient d'étendre son champ d'application aux vols intra-UE. Le groupe de travail souligne la nécessité que les procédures de réexamen de la législation de l'UE prévoient des critères clairs par rapport auxquels évaluer la nécessité et l'efficacité d'un système. Il insiste également une nouvelle fois sur l'importance d'associer les autorités nationales chargées de la protection de données à toute procédure de réexamen, en particulier dans la mesure où une telle participation est prévue par d'autres instruments au niveau de l'UE, comme les accords PNR conclus par l'UE avec des pays tiers.

Le groupe de travail souligne l'importance, lors de l'élaboration de propositions au niveau de l'UE, de mesurer les implications des obligations potentielles de réciprocité. Un système européen en matière de PNR pourrait être à l'origine d'obligations analogues imposées, sur la base de la réciprocité, par des pays non démocratiques ou des pays qui ne garantissent pas un niveau adéquat de protection des libertés et droits fondamentaux, notamment du droit au respect de la vie privée et à la protection des données à caractère personnel. Il ne fait aucun doute que les conséquences pour les citoyens pourraient être graves si de tels pays recevaient les données PNR de l'UE.

9. Conclusion

Le groupe de travail est d'avis que la nécessité d'un système PNR propre à l'UE n'a pas encore été établie et que les mesures proposées ne sont pas conformes au principe de proportionnalité, notamment parce que le système envisage la collecte et la conservation de l'ensemble des données de tous les voyageurs sur la totalité des vols. Il nourrit également de sérieux doutes sur la proportionnalité de la mise en concordance systématique des données de l'ensemble des passagers avec des critères préétablis.

Le groupe de travail recommande en premier lieu d'évaluer les méthodes et systèmes de coopération existants ainsi que la manière dont ceux-ci s'articulent, afin d'identifier les failles sur le plan de la sécurité. Si de telles failles sont constatées, l'étape suivante devrait consister à analyser la meilleure manière d'y remédier, ce qui n'implique pas nécessairement de mettre en place un système totalement nouveau. Les mécanismes existants pourraient être mieux exploités et améliorés.

Si cette proposition de directive entrait en vigueur, elle devrait prévoir des garanties et mesures de protection des données appropriées et adéquates. La Commission devrait également

envisager la possibilité d'abroger des instruments existants à la suite de l'entrée en vigueur de la directive, comme la directive API, afin d'éviter tout chevauchement de mesures.

Le groupe de travail continuera à suivre de près l'état d'avancement de la proposition et accueillerait favorablement toute possibilité qui lui serait donnée de présenter et de préciser son point de vue aux différentes parties associées à cette proposition. Il continuera également à rendre des avis en fonction des circonstances et des besoins.

Fait à Bruxelles, le 5 avril 2011

Pour le groupe de travail
Le Président
Jacob Kohnstamm

Groupe de travail « Article 29 » – « Avis 12/2011 sur les compteurs intelligents »

Adopté le 4 avril 2011

Introduction et champ d'application

L'objectif du groupe de travail « article 29 », dans le présent avis, est de clarifier le cadre juridique applicable au fonctionnement de la technologie de comptage intelligent dans le secteur énergétique. Le présent avis n'est pas destiné à présenter un aperçu complet de tous les aspects spécifiques des programmes de comptage intelligent dans les États membres, la disparité de la situation actuelle ne le permettant pas. Les compteurs intelligents offrent de nouvelles fonctionnalités, comme la production d'informations détaillées sur la consommation d'énergie, la possibilité d'effectuer des relevés à distance, l'élaboration de nouveaux tarifs et services sur la base des profils énergétiques et la possibilité d'interrompre la fourniture à distance.

Les réseaux intelligents ouvrent encore davantage de perspectives de développement et de traitement de données à caractère plus personnel. Le groupe de travail n'a pas l'intention, à ce stade, d'inclure la fonction de réseau intelligent dans le champ d'application du

présent avis. Nous n'excluons pas, cependant, d'approfondir notre analyse du réseau intelligent quand la situation se précisera. La directive relative à l'efficacité énergétique dans les utilisations finales et aux services énergétiques (2006/32/CE) fixe des objectifs à adopter par chaque État membre en matière d'économie d'énergie. Afin d'atteindre ces objectifs, et sous réserve d'un nombre limité d'exceptions, l'article 13 de la directive oblige les États membres à mettre à la disposition des consommateurs des compteurs qui mesurent avec précision leur consommation effective et qui fournissent des informations sur le moment où l'énergie a été utilisée. Ces compteurs intelligents s'inscrivent dans le cadre des efforts pour réaliser les objectifs que l'Union européenne s'est fixés en vue de garantir un approvisionnement énergétique durable pour 2020.

La direction générale de l'énergie a mis en place une task force sur les réseaux intelligents. Le groupe d'experts 2, qui fait partie de cette task force, a demandé l'assistance du groupe de travail « article 29 » afin de disposer d'une analyse plus large des mesures mises en œuvre au niveau national. À cet effet, en 2010, un questionnaire a été diffusé auprès des autorités de contrôle de la protection des données. Six questions portaient sur leurs points de vue concernant les évolutions en matière de réseaux intelligents (dont beaucoup sont aussi examinées dans le présent avis). Une autre série de douze questions demandait des informations à propos de l'état actuel du déploiement des systèmes de relevés intelligents dans les États membres. Les États membres qui ont répondu aux six questions considèrent que le niveau de sécurité doit être comparable à celui d'autres systèmes de grande envergure comme les opérations bancaires sur l'internet. Les réponses à la série de douze questions ont montré que la mise en œuvre de programmes de déploiement de compteurs intelligents chez les consommateurs domestiques d'énergie constitue un thème pertinent et urgent dans de nombreux États membres de l'UE. Les systèmes de relevés intelligents revêtent une importance particulière dans la mesure où ils peuvent avoir une incidence sur la vie de presque tous les citoyens, qui sont tous susceptibles de recevoir un approvisionnement en électricité et gaz. Leur portée est extrêmement étendue et ne se limite pas à ceux qui ont pris la décision d'épouser le progrès technologique. L'objectif est d'atteindre une couverture de 80% des consommateurs d'ici 2020[35].

Les compteurs intelligents permettent la production, la transmission et l'analyse de données relatives aux consommateurs, dans une mesure bien supérieure à ce qui est possible avec un compteur « traditionnel ». Par conséquent, ils permettent également à l'exploitant du réseau (aussi appelé « gestionnaire du réseau de distribution » – GRD), aux fournisseurs d'énergie et à d'autres parties de rassembler des informations détaillées relatives à la consommation énergétique et aux modèles d'utilisation, ainsi que de prendre des décisions concernant les consommateurs individuels sur la base de profils d'utilisation. S'il est admis que ces décisions peuvent souvent être favorables aux consommateurs en termes d'économies d'énergie, il apparaît aussi qu'il existe une possibilité d'intrusion dans la vie privée des citoyens par l'intermédiaire d'appareils installés dans les maisons. Ces systèmes marquent en outre un changement dans notre relation fondamentale avec les fournisseurs d'énergie dans la mesure où, traditionnellement, les clients payaient les fournisseurs pour l'électricité et le gaz qu'ils avaient consommés. Avec l'avènement des compteurs intelligents, le processus est plus complexe, en ce que les données soumises donneront aux fournisseurs un aperçu des habitudes personnelles de consommation.

[35] Compteurs intelligents : contrôler votre facture énergétique ? Euractiv.com, accessible [en ligne] à l'adresse : http://www.euractiv.com/fr/energie-efficacite/compteurs-intelligents-controler-votrefacture-energetique-linksdossier-260179 [consulté le 25 mars 2011]. Cet article présente les jalons du « troisième paquet Énergie », adopté en juin 2009.

7 Annexes

Les avantages largement évoqués de l'utilisation intelligente de l'énergie comportent notamment diverses possibilités pour les consommateurs de réduire leurs factures en changeant leurs habitudes, par exemple en utilisant l'énergie à des moments différents pour profiter de tarifs plus bas, ainsi que des possibilités pour l'industrie de prévoir plus précisément la demande, et donc d'éviter des coûts élevés de stockage de l'électricité. La réalisation des objectifs en matière de changement climatique dépend dans une certaine mesure de la fourniture de données à caractère personnel par les consommateurs, mais il faut faire en sorte que toutes les parties qui interviennent dans les programmes visant à introduire des compteurs intelligents et développer les réseaux intelligents veillent à ce que les droits fondamentaux des personnes physiques soient protégés et respectés. Sans une telle protection, le risque existe non seulement que le traitement des données à caractère personnel enfreigne les lois nationales qui transposent la directive 95/46/CE, mais aussi que ces programmes soient rejetés par les consommateurs qui jugent inacceptable la collecte de données personnelles. Ce rejet peut se produire même s'il n'y a pas d'infraction à la loi. En résumé, du point de vue de la protection des données, le groupe de travail « article 29 » tient à souligner que, si ces programmes offrent des avantages potentiels appréciables et d'une portée considérable, ils permettent aussi de traiter de plus en plus de données à caractère personnel – phénomène sans précédent dans ce secteur – et de rendre ces données personnelles aisément accessibles à un cercle d'utilisateurs plus large qu'actuellement.

Le groupe de travail n'ignore pas que les circonstances varient énormément entre les États membres, depuis ceux où le déploiement est en grande partie accompli, selon le mandat assigné par les autorités, jusqu'à ceux où aucun compteur n'a encore été installé. Le niveau de participation des autorités chargées de la protection des données est également très variable. Dans les cas où ces autorités n'ont pas encore été consultées, le groupe de travail tient à rappeler l'importance de cette consultation à toutes les parties qui interviennent dans le déploiement des systèmes de relevés intelligents.

D'autres différences peuvent être constatées entre les États membres dans la nature du marché et dans l'attribution de la responsabilité de l'installation des compteurs. Dans plusieurs États membres, ce sont des entreprises de service public qui en sont chargées. Ailleurs, il existe un marché concurrentiel.

Les exploitants du réseau de distribution jouent un rôle plus ou moins prépondérant selon les pays. Dans certains États membres, le remplacement des compteurs est obligatoire pour tous les consommateurs. Quand le relevé est envoyé au GRD, les fournisseurs d'énergie ont un droit d'accès aux informations dont ils ont besoin pour la gestion de leur clientèle et l'émission de leurs factures. Ils peuvent aussi accéder à des informations plus détaillées (par exemple, pour conseiller les consommateurs en matière d'économie d'énergie), mais uniquement avec l'accord des clients. Le GRD a aussi le droit de collecter des informations détaillées sur la consommation afin de gérer et d'entretenir son réseau physique.

Les méthodes de communication sont, elles aussi, multiples et complexes. Elles comportent des points d'accès et des voies de transmission des données supplémentaires, qui créent des problèmes de sécurité compliqués pour lesquels des solutions globales doivent être trouvées.

Compte tenu de la situation complexe et disparate du secteur, la formulation de recommandations peut se révéler une tâche difficile et il semble qu'à ce stade, ces recommandations doivent se cantonner dans un registre plus général que spécifique. Il paraît donc sensé et réaliste, à ce stade, de définir clairement l'objet de cette analyse, en prenant comme axe principal la relation entre les exigences légales énoncées dans la directive relative à la protection des données et le contexte des systèmes de relevés intelligents. Le cas échéant, l'analyse renverra aux recherches déjà effectuées par le groupe d'experts de la task force sur les réseaux intelligents[36]. Par exemple, les recommandations du présent avis concernant la prise en compte du respect de la vie privée dès la conception et la sécurité coïncident avec celles qui ont été formulées par le groupe. Il est incontestable que le déploiement massif de compteurs intelligents a déjà commencé. Il est donc urgent que nous parvenions, ensemble, à comprendre la façon dont les compteurs intelligents traitent les données personnelles et les problèmes qui en résultent, même si la portée de ce travail n'est pas exhaustive.
Le présent avis vise à traiter les questions suivantes : la définition des données à caractère personnel dans le contexte des systèmes de relevés intelligents, le contrôle des données et l'appréciation de la légitimité de leur traitement. Les recommandations formulées ici s'appuieront sur les connaissances actuelles, mais d'autres travaux seront probablement nécessaires à l'avenir pour examiner de nouvelles questions (par exemple, les appareils intelligents).

Définitions

Diverses définitions des compteurs et des réseaux intelligents ont déjà été proposées. Néanmoins, pour englober l'ensemble des questions et des priorités retenues par le groupe de travail « article 29 », il est utile de définir les compteurs et les réseaux intelligents de la façon suivante.

Les compteurs intelligents sont installés dans les habitations des consommateurs de services publics et permettent des communications dans les deux sens. Ils informent les clients de la quantité d'énergie qu'ils consomment et ces informations peuvent aussi être transmises aux fournisseurs d'énergie et à d'autres parties désignées. La caractéristique essentielle des compteurs intelligents est qu'ils rendent possibles ces communications à distance entre le compteur et des parties autorisées comme les fournisseurs, les exploitants du réseau et d'autres tierces parties ou sociétés de services énergétiques. Les compteurs intelligents peuvent accroître la fréquence des communications entre le consommateur et les autres parties et augmenter de ce fait le volume des données concernant les consommateurs qui sont accessibles à ces autres parties. La collecte et l'utilisation

[36] Afin de faciliter et de soutenir la mise en place d'un réseau intelligent à l'échelle de l'UE, la Commission européenne a décidé de constituer une task force sur les réseaux intelligents. À cet effet, trois groupes d'experts ont été créés pour formuler des recommandations concernant le déploiement de réseaux intelligents. Le document utilisé pour éclairer le présent avis est le suivant : Groupe d'experts 2 de la task force sur les réseaux intelligents, Regulatory Recommendations for Data Safety, Data Handling and Data Protection Report, publié le 16 février 2011, accessible [en ligne] à l'adresse : http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf [consulté le 25 mars 2011].

des données sont beaucoup plus étendues et servent à des usages plus nombreux que ce n'est le cas pour les compteurs traditionnels, qui font l'objet de relevés physiques de façon relativement peu fréquente.

Fondamentalement, dans les termes les plus abstraits, le compteur intelligent effectue un relevé qui reflète l'utilisation de l'énergie dans un bien immeuble. À un certain moment, ce relevé peut être transmis, ainsi que d'autres informations, en dehors du bien. Dans certains modèles, il sera envoyé directement à un serveur central de communications où sont gérées les données des compteurs intelligents. Là, il est accessible aux GRD, aux fournisseurs et aux sociétés de services énergétiques. La mise en place des compteurs intelligents est une condition préalable au déploiement du réseau intelligent. Le réseau intelligent combine des informations provenant des utilisateurs de ce réseau afin de planifier la fourniture d'électricité de façon plus efficace et rationnelle que ne le permettait l'environnement précédent.

Application du droit en matière de protection des données au traitement des données collectées par les compteurs intelligents

Lorsque des données à caractère personnel figurent parmi les informations produites et diffusées par un compteur intelligent, le groupe de travail considère que la directive 95/46/CE s'applique à leur traitement.

Sur la base des informations générales disponibles sur la question et de discussions détaillées au niveau national concernant le fonctionnement des compteurs intelligents, il a été établi que les types de données suivants peuvent être présumés faire l'objet d'un traitement :

- numéro d'identification unique du compteur intelligent et/ou numéro de référence unique du bien immeuble (même en l'absence de ces identifiants, le compteur pourrait aussi être identifié par son diagramme unique de charge énergétique) ;
- métadonnées se rapportant à la configuration du compteur intelligent ;
- description du message transmis, indiquant par exemple s'il s'agit d'un relevé ou d'une alerte en cas de tentative de falsification ;
- date et heure ;
- contenu du message.

Le contenu du message est susceptible d'inclure les types d'informations suivants :

- relevé du compteur – il peut s'agir d'un relevé simple ou d'un groupe de relevés dans le cas d'un tarif plus complexe ;
- alertes – le compteur peut transmettre un message signalant qu'un événement a déclenché son système d'alarme ;

- informations sur le niveau du réseau, comme la tension, les coupures de courant et la qualité de l'alimentation électrique ;
- diagrammes de charge, avec divers niveaux de précision.

Les données peuvent être envoyées en temps réel au responsable de leur traitement ou être conservées dans le compteur intelligent. Quoi qu'il en soit, conformément à la directive relative à la protection des données, il est considéré dans les deux cas que les données ont été collectées par le responsable du traitement.

Cette liste est loin d'être exhaustive, mais le groupe de travail note que le fonctionnement des compteurs intelligents – et, par extension, tout autre développement des réseaux et appareils intelligents – suppose le traitement de données à caractère personnel, tel qu'il est défini par l'article 2 de la directive 95/46/CE et interprété par le groupe de travail dans son avis 4/2007. De plus, l'accroissement du volume des données personnelles traitées, la possibilité de gérer la connexion à distance et la probabilité d'établissement de profils énergétiques à partir des relevés détaillés exigent impérativement que le droit fondamental des personnes physiques au respect de la vie privée soient dûment pris en considération.

Les raisons pour lesquelles il a été conclu que des données à caractère personnel font l'objet d'un traitement sont les suivantes :

1. Les données produites par les compteurs intelligents telles qu'elles sont énumérées ci-dessus sont, dans la plupart des cas, associées à des identifiants uniques, comme un numéro d'identification du compteur. Pour les clients domestiques des fournisseurs d'énergie, cet identifiant est indissociablement lié au titulaire du compte. Autrement dit, l'appareil permet de distinguer ces personnes des autres consommateurs.

2. De plus, les informations collectées dans le contexte d'un service de relevé intelligent se rapportent au profil énergétique du consommateur et servent à prendre des décisions qui concernent directement cette personne. Ces décisions consistent bien évidemment à déterminer le niveau des montants facturés pour la fourniture d'énergie, mais ne se limitent pas à des objectifs de facturation.

3. Cette analyse est d'ailleurs confirmée par les avantages, largement mis en avant, du déploiement des compteurs intelligents, comme la réduction de la consommation totale d'énergie dans les États membres. Un tel objectif ne peut de toute évidence être atteint que si la consommation individuelle d'énergie des particuliers baisse elle aussi et, selon les fournisseurs d'énergie et les réseaux, sa réalisation dépend, dans une large mesure, de la collecte de grandes quantités d'informations sur le comportement de ces consommateurs.

Définition du responsable du traitement des données applicable dans le cas des compteurs intelligents

Il est établi que la directive 95/46/CE impose des obligations au responsable du traitement des données à caractère personnel. Avant d'examiner comment ces obligations s'appliquent dans le contexte du présent avis, il est important que le groupe de travail précise quelles sont les personnes morales qui, dans son optique, relèvent de la définition du responsable du traitement des données.

Le déploiement des compteurs intelligents fait intervenir plusieurs organisations dans le traitement de données à caractère personnel, qui peuvent être notamment, mais non exclusivement, des fournisseurs d'énergie, des exploitants de réseau, des organes de régulation, des administrations

publiques, des prestataires de services et des fournisseurs de communications. Eu égard au nombre et à la complexité des relations dont il faut tenir compte, il est probable que l'application des définitions pertinentes posera certaines difficultés, mais l'analyse formulée dans le présent avis reflète l'approche adoptée par le groupe de travail dans son avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant ». Les responsabilités découlant de la législation qui régit la protection des données doivent donc être clairement assignées de façon à assurer suffisamment, dans la pratique, le respect des règles applicables en la matière.

Fournisseurs d'énergie

Dans certains États membres, la personne morale principalement responsable du traitement des données à caractère personnel est le fournisseur d'énergie. C'est avec lui que les personnes concernées passent le contrat qui l'autorise à traiter leurs données et, dans la mesure où c'est lui qui choisit les données dont il a besoin pour remplir ses fonctions ainsi que la façon de les collecter, de les conserver et de les utiliser, il peut de toute évidence être considéré comme étant la personne morale ayant déterminé la finalité et les modalités du traitement des données à caractère personnel. Ces éléments désignent de façon très claire le fournisseur d'énergie comme le responsable du traitement des données à caractère personnel produites par un compteur. Le groupe de travail est d'avis que, nonobstant le fait que les compteurs intelligents rendent la situation plus complexe, le fournisseur reste un responsable du traitement dans ce contexte.

Exploitants du réseau ou GRD

Dans d'autres modèles, le GRD auquel appartient le réseau est responsable de l'installation et du fonctionnement du système de compteurs intelligents. C'est aussi au GRD que revient le soin de déterminer comment les données sont collectées, conservées et utilisées. Dans ce modèle, le GRD est responsable du traitement des données. Lorsque les fournisseurs d'énergie disposent d'un droit d'accès aux données transmises par les compteurs et les utilisent à leurs propres fins (par exemple, pour établir leurs factures ou conseiller leurs clients), ils sont aussi responsables du traitement des données à caractère personnel dont ils se servent.

Autres parties

Il existe de nombreuses autres parties qui pourraient éventuellement traiter des données à caractère personnel pour tenir leur rôle dans le cadre d'un programme de déploiement de compteurs intelligents. Il se

peut même que certains de ces intervenants n'apparaissent que lorsque les effets de la transition vers le traitement d'un volume plus important de données à caractère personnel se manifesteront pleinement. Il serait donc imprudent de vouloir en dresser une liste définitive à ce stade. Il ne faut pas non plus perdre de vue les variations dans les modèles de fourniture d'énergie et dans leur conception entre les États membres. L'important est de retenir que, sans une compréhension commune de la façon dont s'applique la définition de la notion de responsable du traitement des données, le risque de manquements à la conformité et aux bonnes pratiques augmente. Dans cette optique, le groupe de travail tient à rappeler à toutes les parties l'importance des points suivants :

1. Certains modèles de déploiement comportent une fonction centrale de communications qui gère la transmission de données entre le compteur et le fournisseur. Cette fonction peut être assurée par un sous-traitant, agissant uniquement sur les instructions des fournisseurs qui reçoivent et envoient les données. Toutefois, dans le cas où la fonction de communications intervient dans la décision d'autorisation de consultation par un tiers de données à caractère personnel ou de leur traitement à d'autres fins, cette fonction peut avoir à assumer le rôle de responsable du traitement des données à caractère personnel concernées.

2. Les régulateurs du secteur énergétique sont eux aussi des acteurs importants. Ils peuvent avoir accès à des données à des fins de recherche ou de formulation des politiques. Dans la mesure où il s'agit de données à caractère personnel, l'organe de régulation assumera le rôle de responsable du traitement.

3. Les prestataires tiers (souvent appelés « sociétés de services énergétiques » ou « SSE ») joueront un rôle de plus en plus important dans l'utilisation des données produites par les compteurs intelligents. Lorsque des données à caractère personnel sont divulguées aux SSE pour leur permettre de fournir un service au consommateur ou à une autre partie, comme un fournisseur, les SSE assumeront le rôle de responsable du traitement.

Légalité et légitimité du traitement des données

Dès lors qu'il a été établi qu'une personne morale doit être considérée comme responsable du traitement des données, il est important de définir les obligations légales que lui impose la directive relative à la protection des données. Conformément à l'article 6 de la directive, les données à caractère personnel doivent être traitées loyalement et licitement. Pour être licite, le traitement de données à caractère personnel doit remplir au moins une des six conditions de légitimité énoncées à l'article 7 de la directive.

Le groupe de travail note que dans beaucoup d'États membres, sinon tous, la nature exacte des finalités du traitement des données à caractère personnel conservées ou transmises par un compteur intelligent doit encore être clarifiée ou définie. En conséquence, le groupe de travail est d'avis qu'il convient d'établir ces finalités avant de pouvoir soutenir que le traitement des données repose sur des motifs légitimes.

Le groupe de travail observe aussi que chaque finalité distincte doit être, en elle-même et par elle-même, légitime et qu'une finalité légitime ne peut servir à en légitimer une autre.

En particulier, les données à caractère personnel ne peuvent faire l'objet d'un nouveau traitement en vue d'une autre finalité qui est incompatible avec la finalité pour laquelle elles ont été collectées à l'origine.

7 Annexes

Le point de vue du groupe de travail est qu'il existe cinq motifs possibles sur lesquels peuvent s'appuyer les responsables du traitement des données dans ce contexte.

Consentement

Il est évident que bon nombre des motifs pour lesquels des données à caractère personnel peuvent être utilisées se rapporteront à l'amélioration des services proposés aux personnes concernées, comme des tarifs différenciés selon le moment de l'utilisation ou des conseils en matière d'économies d'énergie. Dès lors que la personne concernée accepte qu'un tel service lui soit fourni, il est probable que le prestataire de services – qu'il s'agisse d'un fournisseur d'énergie ou d'un tiers – pourra obtenir son consentement pour le traitement de données à caractère personnel.

Le groupe de travail tient à rappeler aux responsables du traitement des données qu'il ne peut y avoir de consentement valable sans que la personne concernée ait pris sa décision en toute connaissance de cause. Le consentement ne peut être invoqué comme motif pour le traitement de données à caractère personnel que si la personne concernée a reçu suffisamment d'informations sur le traitement de ses données personnelles pour opérer un véritable choix. En particulier, lorsqu'il existe plusieurs fonctionnalités différentes, le consentement doit être suffisamment détaillé pour refléter ces finalités multiples et ne peut à lui seul servir à légitimer des finalités potentiellement divergentes et sans relation entre elles.

Le groupe de travail recommande que le secteur mette au point des moyens pratiques et efficaces permettant aux personnes concernées d'exprimer leur consentement. Il est important de rappeler que le consentement doit être donné librement et doit donc pouvoir être révoqué. Il faut que les méthodes employées pour recueillir le consentement de la personne concernée lui laissent la possibilité de changer d'avis sans rencontrer trop de difficulté. Une solution possible pourrait être de concevoir le tableau de commande du compteur domestique de façon à inclure un accord par pression sur un « bouton poussoir ». La disponibilité de ce type de fonctionnalité dépendrait du niveau de perfectionnement du compteur et du tableau de commande, afin de garantir la validité du processus de consentement.

Contrat

Le traitement des données peut également être nécessaire à

l'exécution d'un contrat auquel la personne concernée est partie, ou à l'accomplissement de démarches préalables à la conclusion d'un contrat à la demande de la personne concernée. Cette base juridique pourrait servir à légitimer le traitement de données à caractère personnel à des fins de facturation, dans la mesure où le contrat de fourniture d'énergie ne peut être exécuté sans l'établissement d'une facture exacte.

En ce qui concerne la facturation, il est important de rappeler que cette condition repose sur un élément de nécessité. Autrement dit, si les motifs du traitement des données consistent dans l'exécution d'un contrat qui ne prévoit que l'établissement et le paiement de factures trimestrielles, il n'est pas nécessaire que le fournisseur effectue des relevés plus fréquents dans le cadre du contrat. Pour ce faire, il conviendrait que le contrat comporte des dispositions juridiques valables prévoyant des relevés plus fréquents ou que le fournisseur s'appuie sur une autre base juridique pour justifier ces relevés.

Exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique

Dans certains États membres, l'exploitant du réseau d'électricité est chargé de veiller au bon fonctionnement du réseau physique, mais aussi de faire baisser la consommation électrique dans son ensemble. Cette consommation concerne à la fois la consommation globale et la consommation durant les heures de pointe. Il s'agit d'une mission d'intérêt public qui légitime l'installation des compteurs intelligents.

Obligation légale

Dans certains États membres, l'exploitant du réseau a l'obligation de placer des compteurs intelligents et de s'en servir pour collecter des données dans chaque nouvelle installation[37].

Intérêt légitime

Conformément à l'article 7, point f), de la directive, le traitement peut être licite s'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits fondamentaux de la personne concernée.

Le point essentiel à retenir ici est que, pour pouvoir s'appuyer sur cette base juridique, il convient de prendre en considération les intérêts et les droits des personnes concernées. Il peut sembler indéniable qu'un renforcement de l'efficacité de la fourniture et de la consommation d'énergie sert l'intérêt légitime du responsable du traitement et de la société dans son ensemble, et que les données à caractère personnel collectées par les compteurs intelligents permettent d'y parvenir. Pour autant, ce n'est pas parce que cette utilisation particulière des données à caractère personnel semble légitime (et, pour de nombreuses personnes, souhaitable) qu'elle justifie n'importe quel aspect du traitement. Autrement dit, bien que l'impératif de réduction de la consommation d'énergie puisse constituer un objectif raisonnable en matière de politique publique, il ne prévaut pas dans tous les cas sur les droits et les intérêts des personnes concernées.

Il est clair que l'inclusion de mesures pratiques, telles que des technologies renforçant la protection de la vie privée et des évaluations d'impact sur la vie privée, afin de renforcer la sécurité et la confidentialité des données traitées par les compteurs intelligents donnera à un responsable du traitement de meilleures chances de remplir cette condition.

Ce critère revêt une importance particulière dans le cas où le traitement des données aux fins de la réalisation de l'intérêt légitime poursuivi par le responsable du traitement est, en soi, trop intrusif ou lorsqu'il a pour effet de causer un préjudice

[37] Voir le décret français n°2010-1022 du 31 août 2010.

non justifié à la personne concernée. Ce pourrait être le cas, par exemple, de la création de profils détaillés des personnes concernées sans réelle nécessité pour la finalité recherchée, de la communication d'informations à des tiers à l'insu de la personne concernée ou sans son accord, ou de l'utilisation de données à caractère personnel pour prendre des décisions de déconnexion à distance sans que la protection des données et autres droits de la personne concernée aient été dûment pris en considération. Le groupe de travail tient aussi à rappeler au secteur que, dans certains États membres, la personne concernée a la possibilité de refuser l'installation du compteur intelligent et que, dans de tels cas, ses préférences priment tout autre intérêt.

Autres problèmes de conformité soulevés par les systèmes de relevés intelligents

Du fait de la portée très vaste des questions soulevées par les systèmes de relevés intelligents, il n'est pas possible pour le groupe de travail de dresser une liste exhaustive des points à propos desquels des orientations pourraient être formulées. Il s'agit en fait d'un domaine d'activité émergent et le groupe de travail s'attend à voir apparaître d'autres problèmes et des solutions nouvelles en matière de protection des données à mesure que l'installation de compteurs intelligents prendra de l'ampleur. Il y a cependant certaines questions d'intérêt général qui méritent, selon le groupe de travail, d'être sérieusement examinées par tous les intervenants dans ce domaine.

Prise en compte du respect de la vie privée dès la conception

Le groupe de travail renvoie à son avis 168 dans lequel il était indiqué que les services et technologies qui dépendent du traitement de données à caractère personnel devraient être conçus avec un paramétrage par défaut favorable au respect de la vie privée. À cet égard, le déploiement de systèmes de relevés intelligents devrait intégrer dès le départ la prise en compte du respect de la vie privée, non seulement par des mesures de sécurité, mais aussi par une réduction au minimum du volume des données à caractère personnel traitées. Certains États membres ont adopté des plans de mise en œuvre qui prévoient une évaluation d'impact sur la vie privée. Le groupe de travail recommande ce genre d'approche.

Les compteurs intelligents qui sont actuellement testés dans certains États membres prennent plusieurs relevés, selon le type de contrat souscrit par le consommateur.

Par exemple, si le contrat stipule simplement que le client paie

le même prix pour l'électricité consommée tout au long de la journée, le compteur effectuera un seul relevé quotidien. À l'inverse, si le consommateur a conclu un contrat selon lequel des tarifs différents sont appliqués en fonction du moment de la journée, le compteur effectuera dix relevés par jour. Au niveau le plus élémentaire, la prise en compte du respect de la vie privée dès la conception garantirait que la fréquence de transmission des relevés ne soit pas supérieure à ce qui est nécessaire pour le fonctionnement du système ou pour la fourniture d'un service que le consommateur a accepté.

Par exemple, un type de compteur en usage actuellement effectue des relevés de consommation en temps réel toutes les 10 à 60 minutes afin d'établir un diagramme de charge. La fréquence peut être ajustée à distance par l'exploitant du réseau d'électricité. Ce diagramme de charge est conservé dans le compteur, avec un historique de deux mois, et est collecté par l'exploitant selon ses besoins. L'adoption d'une approche de prise en compte du respect de la vie privée dès la conception permettrait d'adapter ce modèle pour que la collecte des données et l'enregistrement du diagramme de charge soient effectués uniquement sur demande.

Les spécifications techniques du réseau devraient aussi garantir que toutes les données collectées restent sur le réseau domestique à moins que leur transmission ailleurs ne soit nécessaire ou que la personne concernée n'ait donné son accord. Le système devrait aussi être conçu pour que, même dans le cas où des données à caractère personnel sont transmises, tous les éléments non nécessaires soient filtrés ou supprimés. L'objectif général devrait être de réduire au strict minimum les volumes des données traitées et transmises.

Le groupe de travail recommande aussi que la conception des systèmes ne permette d'accéder aux données à caractère personnel que dans la mesure nécessaire à la mission assurée par le responsable du traitement. Il convient de vérifier que toutes les parties ayant accès à des données à caractère personnel en sont bien les destinataires appropriés et compétents et ne peuvent consulter que les données nécessaires à l'accomplissement de leur mission. Elles ne doivent pas avoir accès à des données à caractère personnel qui sortent de ce cadre.

Conservation des données à caractère personnel

Avant l'arrivée des compteurs intelligents, les pratiques en vigueur dans le secteur de l'énergie en matière de conservation des données à caractère personnel se limitaient à certaines finalités, par exemple, la facturation. L'environnement des systèmes de relevés intelligents fait apparaître de nouveaux défis. Étant donné que les volumes des données traitées seront sensiblement plus importants, il sera nécessaire d'établir des stratégies et des pratiques de conservation des données en vue de nouvelles finalités et de revoir celles qui ont cours pour les finalités existantes. Il faut donc parvenir à une compréhension plus claire des finalités du traitement pour s'assurer que la durée de conservation des données n'excède pas le temps nécessaire à la réalisation d'un objectif licite et bien spécifié. Les responsables du traitement des données à caractère personnel seront ainsi en mesure de démontrer que ces données ne sont conservées qu'aussi longtemps que nécessaire. Par exemple, le fait que les données collectées par un compteur permettraient de dispenser des conseils en matière d'économie d'énergie constitue une finalité mentionnée très fréquemment. Dans certains cas, ce type de service pourrait inclure des comparaisons d'une année à l'autre et, à cet effet, il a été avancé qu'une période de conservation des données à caractère personnel de treize mois serait appropriée. Toutefois, une période de

conservation aussi longue ne serait acceptable que dans le cas où les personnes concernées ont convenu qu'un tel mécanisme pourrait leur être profitable. Pour la fourniture d'autres types de service, une période de conservation beaucoup plus courte s'imposerait.

En outre, il peut être envisagé que la plupart de ces données restent stockées dans les compteurs des consommateurs ou dans des appareils comparables destinés à servir de passerelles (autres que ceux requis à des fins de facturation). De cette façon, les personnes concernées auraient la possibilité de faire leurs propres choix en matière de conservation des données. Si tel était le cas, il serait souhaitable de mettre en place un système d'invitations ou de rappels pour aider les consommateurs à gérer la conservation de leurs données.

Traitement de données à caractère personnel par des tiers

Il est probable que de nombreuses tierces parties ou sociétés de services énergétiques contribueront au déploiement des systèmes de relevés intelligents. Le groupe de travail estime que leurs interventions devront faire l'objet d'un examen attentif.

L'influence et la participation de tiers seront variables d'un État membre à l'autre, mais il est évident que, sous sa forme la plus intrusive, le déploiement de compteurs intelligents pourrait déboucher sur la diffusion de profils énergétiques au bénéfice des parties qui souhaitent commercialiser des services énergétiques.

Parmi les techniques qui ont été proposées afin de garantir la conformité des systèmes figurent notamment la mise en place d'un serveur central d'information et de communications par lequel passeraient tous les intervenants désireux d'accéder aux données des consommateurs ; un code auquel devraient souscrire toutes les parties ; et une charte qui couvrirait l'ensemble du secteur. Le groupe de travail tient à préciser que plus le traitement est intrusif, plus les mesures de protection doivent être strictes. Le groupe de travail invite instamment les organes de régulation à se prononcer sur l'acceptabilité des traitements plus intrusifs.

Toutes ces dispositions reposeraient sur le consentement du consommateur, à charge pour le secteur de veiller à ce que la personne concernée soit en position d'accepter en connaissance de cause. Le groupe de travail insiste sur le fait qu'il serait inacceptable que des tiers puissent traiter des informations détaillées concernant la consommation énergétique d'une personne à l'insu et sans l'accord de cette dernière.

Sécurité

Dans le cadre de la prise en compte du respect de la vie privée dès la conception, des évaluations des risques pour la sécurité et pour la vie privée recenseront les risques pour la sécurité des données. Compte tenu des vastes perspectives nouvelles qui sont ouvertes par le réseau intelligent et les technologies associées, l'anticipation des besoins en matière de sécurité constitue une tâche difficile.

Dans cette optique, afin de réduire les risques, le présent avis recommande une approche intégrale qui associe toutes les parties et s'appuie sur une expertise très étendue. Les considérations de sécurité ne doivent pas venir se greffer ultérieurement sur l'architecture du réseau, mais y être intégrées dès les premiers stades de la conception.

Le groupe de travail insiste sur le fait que les personnes concernées doivent recevoir des garanties suffisamment solides pour être sûres que leurs données à caractère personnel sont traitées en toute sécurité et que leurs droits fondamentaux en matière de respect de la vie privée sont protégés. Ces garanties devraient s'appliquer à l'ensemble du processus, et notamment aux éléments du réseau dans leurs habitations, à la transmission des données à caractère personnel sur le réseau et à la conservation et au traitement des données par les fournisseurs, les exploitants du réseau et autres responsables du traitement.

Le groupe de travail prévoit que les compteurs intelligents auront une longue durée de vie et il recommande donc que les mesures de sécurité soient mises à jour et perfectionnées au fil du temps et fassent régulièrement l'objet de révisions et de tests. Compte tenu du volume accru des données à caractère personnel traitées, il est évident que le risque augmente aussi en ce qui concerne la confidentialité des données. C'est pourquoi le groupe de travail recommande que des garanties, d'ordre technique et organisationnel, couvrent au moins les domaines suivants :

- la prévention de la divulgation non autorisée de données à caractère personnel ;
- le maintien de l'intégrité des données pour éviter toute modification non autorisée ;
- l'authentification efficace de l'identité des destinataires des données à caractère personnel ;
- les mesures destinées à éviter que des services importants soient interrompus en raison d'atteintes à la sécurité des données à caractère personnel ;
- la possibilité de procéder à des vérifications appropriées des données à caractère personnel conservées ou transmises par un compteur ;
- des contrôles appropriés de l'accès aux données et des périodes de conservation ;
- l'agrégation des données dans tous les cas où leur conservation au niveau individuel n'est pas nécessaire.

Respect des droits de la personne, notamment en ce qui concerne les informations fournies aux personnes concernées

Le déploiement de compteurs intelligents donnera lieu à des opérations complexes et nouvelles de traitement des données à caractère personnel. La plupart des personnes concernées n'auront pas connaissance de la nature de ces opérations et de leurs conséquences possibles en termes de respect de la vie privée. En l'absence d'informations sur le traitement des données à caractère personnel, il est évidemment impossible de prendre des décisions en connaissance de cause à cet égard.

L'obligation d'informer les personnes concernées à propos du traitement de leurs données à caractère personnel est l'un des principes fondamentaux de la directive relative à la protection des données. L'article 10 régit la fourniture de ces informations et impose au responsable du

traitement de communiquer les informations suivantes à la personne concernée :

- l'identité du responsable du traitement et, le cas échéant, de son représentant ;
- les finalités du traitement auquel les données sont destinées ;
- toute information supplémentaire utile pour assurer un traitement loyal des données, notamment l'identité des destinataires des données à caractère personnel, l'existence d'un droit d'accès et de rectification.

Le responsable du traitement des données chargé de l'installation et de l'entretien du compteur devra préciser à l'intention des personnes concernées quelles sont les informations collectées par le compteur et à quoi elles servent.

Dans la mesure où des tiers interviennent dans le traitement des données à caractère personnel dans le but de fournir des services aux personnes concernées, celles-ci doivent également en être informées. Dans certaines circonstances, il pourrait être approprié d'autoriser une vérification ou un contrôle indépendant de l'accès aux données à caractère personnel et de leur utilisation par des tiers, afin de veiller à ce que les personnes concernées ne soient pas induites en erreur.

Droits de la personne concernée

Les responsables du traitement des données doivent respecter les droits des personnes concernées à accéder aux informations conservées à leur propos et, le cas échéant, à les rectifier ou à les supprimer. De toute évidence, dès lors qu'une partie intégrante du projet de système de relevés intelligents consiste dans la mise en place d'un « réseau domestique » (où le consommateur peut obtenir immédiatement du compteur intelligent des informations à propos de ses habitudes de consommation et des tarifs appliqués), il existe une possibilité de garantir aux personnes concernées l'exercice de leurs droits, par une utilisation aisée d'outils permettant un accès direct aux données.

Toutefois, certains aspects de la technologie ne sont pas de nature à faciliter l'accès des personnes concernées à leurs données. Par exemple, l'un des compteurs actuellement testés dans certains États membres n'est pourvu que d'un petit écran d'affichage en mode texte. Cet équipement ne permet pas au consommateur de consulter les informations déjà transmises par le compteur ni d'afficher des graphiques, comme les diagrammes de charge (qui sont conservés dans le compteur).

Cet affichage ne paraît donc pas suffisant pour servir à une

demande d'accès aux données de la part de la personne concernée.

Traitement des données à des fins de prévention et d'enquête pénale

La directive relative à la protection des données interdit tout traitement de données à caractère personnel excessif au regard des finalités poursuivies. Il est évident que les informations détaillées obtenues par les compteurs intelligents, qui donnent aux fournisseurs un aperçu des habitudes de consommation, pourraient permettre la détection d'activités suspectes et, dans certains cas, illégales. Le groupe de travail tient à rappeler au secteur que le fait qu'une telle possibilité existe ne justifie pas automatiquement le traitement à grande échelle de données à cette fin. Il est particulièrement important de noter que, dans la mesure où des données à caractère personnel se rapportent à une infraction supposée, ces données doivent être considérées comme sensibles et ne peuvent par conséquent être analysées par le responsable du traitement, à moins que l'article 8, paragraphe 5), de la directive ne s'applique.

Conclusion

L'arrivée de systèmes de relevés intelligents, qui ouvre la voie au réseau intelligent, apporte avec elle un modèle d'interrelations entièrement nouveau et complexe qui soulève des questions concernant l'application du droit en matière de protection des données. Les réponses au questionnaire de la direction générale de l'énergie ont fait apparaître une grande diversité de situations entre les États membres de l'UE, en ce qui concerne tant l'avancement dans la mise en place des systèmes que les modalités de fourniture d'énergie, ce qui complique encore le scénario. Il ne fait cependant aucun doute que le déploiement des compteurs intelligents s'opère à très grande échelle : il est prévu que la grande majorité des citoyens européens en auront un chez eux avant la fin de cette décennie.

Le présent avis explique dans quelle mesure le droit en matière de protection des données est applicable : il a été démontré que des données à caractère personnel sont traitées par les compteurs et que, par conséquent, les législations relatives à la protection des données s'appliquent.

Le présent avis a indiqué que les systèmes de relevés intelligents offrent un grand nombre de possibilités nouvelles pour traiter les données et fournir des services aux consommateurs. Quel que soit le traitement, qu'il soit similaire à ce qui existait auparavant ou sans précédent, le responsable doit être clairement identifié et doit avoir connaissance des obligations que lui impose la législation en matière de protection des données, notamment du point de vue de la prise en compte du respect de la vie privée dès la conception, de la sécurité et des droits des personnes concernées. Ces personnes doivent être correctement informées de la façon dont sont traitées leurs données et avoir conscience des différences fondamentales dans les modes de traitement pour être en mesure de donner valablement leur consentement.

Fait à Bruxelles, le 4 avril 2011

Pour le groupe de travail
Le président
Jacob Kohnstamm

7 Annexes

Groupe de travail « Article 29 » – « Avis 13/2011 sur les services de géolocalisation des dispositifs mobiles intelligents »

Adopté le 16 mai 2011

Table des matières

1. Introduction

Les informations géographiques jouent un rôle important dans notre société. La plupart des activités et décisions humaines ont une dimension géographique. Lorsque des informations sont liées à une position géographique, elles acquièrent généralement une plus grande valeur. Ces informations peuvent être de toutes sortes : financières, sanitaires ou autres données relatives au comportement du consommateur. En raison de la rapidité de l'évolution technologique des dispositifs mobiles intelligents associée à la généralisation de leur utilisation, une toute nouvelle catégorie de services basés sur la localisation se développe.

Le présent avis a pour objectif de clarifier le cadre juridique applicable aux services de géolocalisation proposés ou générés par les dispositifs mobiles intelligents capables de se connecter à l'internet et équipés de capteurs sensibles à la position tels que des systèmes de localisation GPS. Il peut notamment s'agir de services de cartographie et de navigation, de services géographiques personnalisés (y compris les points d'intérêt à proximité), de réalité augmentée, du géomarquage de contenu sur l'internet, de la possibilité de se tenir informé des allées et venues de ses amis, de la surveillance des enfants et de la publicité basée sur la localisation.

Le présent avis aborde également les trois principaux types d'infrastructure utilisés pour offrir des services de géolocalisation, à savoir le système GPS, les stations de base GSM et le système Wi-Fi. Une attention particulière est accordée à la nouvelle infrastructure basée sur la localisation de points d'accès Wi-Fi.

Le groupe de travail est bien conscient qu'il existe de nombreux autres services capables de traiter des données de localisation qui peuvent également susciter des inquiétudes en matière de protection des données. Il s'agit entre autres des systèmes de billetterie électronique, des systèmes de péage pour voitures et des services de navigation par satellite, du repérage de position à l'aide, par exemple, de caméras et de la géolocalisation d'adresses IP. Cependant, en raison de la rapidité de l'évolution technologique, notamment en matière de mappage de points d'accès sans fil, associée au fait que de nouveaux arrivants sur le marché se préparent à mettre au point de nouveaux services de localisation basés sur un mélange de données issues des stations de base et des systèmes GPS et Wi-Fi, le groupe de travail a décidé de clarifier de manière spécifique les conditions juridiques que doivent remplir ces services en vertu de la directive sur la protection des données.
Le présent avis commence par décrire les technologies concernées, puis identifie et évalue les risques d'atteinte à la vie privée, et enfin présente des conclusions concernant l'application des articles juridiques pertinents à divers responsables du traitement qui recueillent et traitent les données de localisation provenant de dispositifs mobiles. Il s'agit, par exemple, des fournisseurs d'infrastructure de géolocalisation, des fabricants de téléphones intelligents et des développeurs d'applications basées sur la géolocalisation.

Le présent avis n'évaluera pas la technologie de géomarquage spécifique associée à ce que l'on appelle le Web 2.0, selon laquelle les utilisateurs intègrent des informations géoréférencées sur des réseaux sociaux tels que Facebook ou Twitter. Il ne rentrera pas non plus dans les détails de certaines autres technologies de géolocalisation qui sont utilisées pour interconnecter des dispositifs situés dans une zone relativement petite (centres commerciaux, aéroports, immeubles de bureaux, etc.), telles que les technologies Bluetooth, ZigBee, le gardiennage virtuel et les étiquettes RFID utilisant la technologie Wi-Fi, bien qu'une grande partie des conclusions

du présent avis relatives au motif légitime, à l'information et aux droits des personnes concernées s'appliquent également à ces technologies lorsqu'elles servent à établir la position géographique de personnes par l'intermédiaire de leurs dispositifs.

2. Contexte : les différentes infrastructures de géolocalisation

2.1 Données des stations de base

La zone couverte par les différents opérateurs de télécommunications est divisée en zones communément appelées « cellules ». Afin de pouvoir effectuer des appels téléphoniques ou se connecter à l'internet à l'aide du réseau 3G, le dispositif mobile doit se connecter à l'antenne (ci-après : la station de base) qui couvre cette cellule. Les cellules couvrent des zones de tailles différentes, ceci dépendant de l'interférence avec des montagnes ou de hauts bâtiments, par exemple.

Tant qu'un dispositif mobile est allumé, ce dernier est lié à une station de base particulière.

L'opérateur de télécommunications enregistre continuellement ces liens. Chaque station de base possède un identifiant unique et est enregistrée en association avec une position spécifique. L'opérateur de télécommunications ainsi qu'un grand nombre de dispositifs mobiles eux-mêmes sont capables d'utiliser des signaux provenant de cellules se chevauchant (stations de base voisines) pour estimer la position du dispositif mobile avec une meilleure précision. Cette technique est également appelée triangulation.

Il est possible d'améliorer davantage la précision à l'aide d'informations telles que la puissance reçue d'un signal radio (RSSI), la différence entre les temps d'arrivée (TDOA), et l'angle d'incidence (AOA). Les données des stations de base peuvent être utilisées de manière innovante, comme par exemple pour détecter des embouteillages. À chaque route correspond une vitesse moyenne pour chaque segment de la journée, mais lorsque les transferts à la station de base suivante prennent plus de temps que prévu, on peut supposer qu'il y a un embouteillage.

En résumé, ce procédé de positionnement permet d'obtenir rapidement une estimation approximative de localisation mais n'offre toutefois pas la précision des données GPS et Wi-Fi. La précision obtenue est d'environ 50 mètres dans des zones urbaines densément peuplées, mais peut être de plusieurs kilomètres en zone rurale.

2.2 La technologie GPS

Les dispositifs mobiles intelligents comportent un jeu de puces incorporé doté d'un récepteur GPS permettant de les localiser. La technologie GPS (Global Positioning System) utilise 31 satellites tournant chacun dans l'une des 6 différentes orbites autour de la terre[38]. Chaque satellite transmet un signal radio très précis. Le dispositif mobile peut déterminer sa position lorsque le capteur GPS capture au moins 4 de ces signaux. À la différence des données de stations de base, le signal n'est émis que dans un seul sens. Les entités qui gèrent les satellites ne peuvent pas suivre les appareils qui ont reçu le signal radio. La technologie GPS permet une localisation précise, entre 4 et 15 mètres. Le principal inconvénient du système GPS est que le démarrage est relativement lent[39]. Un autre inconvénient est qu'il fonctionne mal voire pas du tout en intérieur. Dans la pratique, la technologie GPS est donc souvent utilisée en association avec des données de stations de base et/ou des points d'accès Wi-Fi mappés.

2.3 La technologie Wi-Fi

2.3.1 Points d'accès Wi-Fi

Les points d'accès Wi-Fi sont utilisés depuis peu comme source d'informations de géolocalisation. La technologie utilisée est similaire à celle des stations de base. Les deux types de technologies se basent sur un identifiant unique (appartenant à la station de base ou au point d'accès Wi-Fi) qui peut être détecté par un dispositif mobile, puis envoyé à un service comportant un emplacement pour chaque identifiant unique.

L'identifiant unique attribué à chaque point d'accès Wi-Fi correspond à son adresse MAC. Une adresse MAC est un identifiant unique attribué à une interface réseau et qui est généralement enregistré sur des composants matériels tels que des puces de mémoire et/ou des cartes d'interface réseau d'ordinateurs, de téléphones, d'ordinateurs portables ou de points d'accès[40].

La raison pour laquelle les points d'accès Wi-Fi peuvent être utilisés comme source d'informations de géolocalisation est qu'ils signalent constamment leur existence. La plupart des points d'accès à l'internet à large bande sont également munis d'une antenne Wi-Fi par défaut.

Sur la plupart des points d'accès les plus couramment utilisés en Europe, la connexion est « activée » par défaut, même si l'utilisateur a connecté son ou ses ordinateurs au point d'accès à l'aide de câbles physiques. Tout comme une radio, le point d'accès Wi-Fi transmet continuellement son propre nom réseau et son adresse MAC, même si personne n'utilise la connexion et même dans le cas où les contenus de la communication sans fil sont chiffrés à l'aide du système WEP, WPA ou WPA2.

Il existe deux manières différentes de recueillir les adresses MAC de points d'accès WI-FI[41].

1. Le balayage actif : il consiste à envoyer des requêtes actives[42] à tous les points d'accès Wi-Fi avoisinants et à enregistrer les réponses. Ces réponses n'incluent pas les informations concernant des dispositifs connectés au point d'accès Wi-Fi.

2. Le balayage passif : il consiste à enregistrer les trames de balises périodiques transmises par chaque point d'accès (habituellement à raison de 10 fois par seconde). Une alternative non standard consiste en ce que des outils enregistrent plus largement toutes les trames Wi-Fi transmises par les points d'accès, dont celles qui ne diffusent pas de signaux de balise. Si ce type de balayage est effectué sans que les principes de respect de la vie privée soient pris en compte dès la conception, il peut mener à la collecte des données échangées entre les

[38] Le système de positionnement global est constitué de satellites lancés par les États-Unis d'Amérique à des fins militaires. La Commission européenne prévoit de lancer, d'ici 2014, Galileo, un réseau de 18 satellites procurant gratuitement un service de positionnement global par satellite à usage non militaire. Les deux premiers satellites devraient être lancés en 2011, et deux autres en 2012. Source : Commission européenne, « Commission presents midterm review of Galileo and EGNOS », 25 Janvier 2011, URL : http://ec.europa.eu/enterprise/newsroom/cf/itemlongdetail.cfm?displayType=news&tpa_id=0&item_id=4835

[39] Afin d'accélérer la détection initiale du signal GPS, il est possible de préinstaller ce que l'on appelle des « tables arc-en-ciel » contenant le positionnement escompté des différents satellites au cours des prochaines semaines.

[40] Un exemple d'adresse MAC est : 00-1F-3F-D7-3C-58. L'adresse MAC d'un point d'accès Wi-Fi est appelée BSSID (Basic Service Set Identifier).

[41] Les systèmes de balayage actif et passif ont été normalisés par l'IEEE 802.11 afin de détecter les points d'accès.

[42] Afin de recueillir des adresses MAC, le responsable du traitement envoie une trame de requête (« probe request ») à tous les points d'accès.

points d'accès et les dispositifs qui y sont rattachés. De cette manière, il serait possible d'enregistrer les adresses MAC des ordinateurs de bureau, des ordinateurs portables et des imprimantes. Ce type de balayage pourrait également entraîner l'enregistrement illicite du contenu des communications. Ce contenu peut être extrait facilement si le chiffrement Wi-Fi (WEP/WPA/WPA2) n'est pas activé sur le point d'accès Wi-Fi.

Il est possible de calculer la position d'un point d'accès Wi-Fi de deux manières différentes.

1. Statiquement/une seule fois : les responsables du traitement eux-mêmes recueillent les adresses MAC de points d'accès Wi-Fi en circulant dans des véhicules équipés d'une antenne. Ils enregistrent la latitude/longitude du véhicule à l'instant où le signal est capturé, ce qui leur permet de calculer la position des points d'accès, en fonction, entre autres, de l'intensité de signal.

2. Dynamiquement/en continu : les utilisateurs de services de géolocalisation recueillent automatiquement les adresses IP captées par leurs appareils Wi-Fi lorsqu'ils utilisent par exemple une carte en ligne pour déterminer leur propre position (Où suis-je ?). Le dispositif mobile envoie alors toutes les informations disponibles au fournisseur de services de géolocalisation, dont les adresses MAC, les identifiants SSID et l'intensité du signal. Le responsable du traitement peut utiliser ces observations continues afin de calculer et/ou d'améliorer les positions des points d'accès Wi-Fi contenus dans sa base de données avec des points d'accès Wi-Fi mappés.

Il est important de noter que les dispositifs mobiles n'ont pas besoin de se « connecter » à des points d'accès Wi-Fi pour recueillir des informations Wi-Fi. Ils détectent automatiquement la présence de points d'accès (en mode balayage actif ou passif) et recueillent automatiquement des données les concernant.

De plus, les téléphones mobiles demandant l'établissement de leur position géographique enverront non seulement des données Wi-Fi, mais aussi fréquemment d'autres informations de localisation qu'ils détiennent, dont des données GPS et des données de stations de base. Ceci permet au fournisseur de calculer la position de « nouveaux » points d'accès Wi-Fi et/ou d'améliorer les positions des points d'accès Wi-Fi qui étaient déjà inclus dans la base de données. De cette manière, la collecte d'informations concernant

les points d'accès Wi-Fi est décentralisée d'une manière très efficace, sans que les clients n'en soient nécessairement conscients.

En résumé, la géolocalisation basée sur les points d'accès Wi-Fi procure une localisation rapide et, grâce à des mesures effectuées en continu, de plus en plus précise.

3. Risques d'atteinte à la vie privée

Un dispositif mobile intelligent est très intimement lié une personne donnée. La plupart des personnes gardent généralement leurs dispositifs mobiles, à proximité immédiate, que ce soit dans leur poche ou leur sac, ou même sur leur table de chevet à côté du lit.

Il est rare que l'on prête un appareil de ce genre à une autre personne. La plupart des gens sont conscients que leur dispositif mobile contient tout un éventail d'informations extrêmement intimes pouvant aller de leurs courriers électroniques à des photos privées, en passant par leur historique de navigation et leur liste de contacts, par exemple.

Cela permet aux fournisseurs de services basés sur la géolocalisation d'obtenir une vision intime des habitudes et des schémas de comportement du propriétaire d'un tel appareil et d'établir des profils très détaillés. À partir d'un schéma d'inactivité la nuit, il est possible de déduire le lieu où dort le propriétaire, et à partir d'un schéma de trajets réguliers effectués le matin, de connaître la position d'un employeur. Le schéma peut également inclure des données issues des schémas de déplacement d'amis, sur la base de ce que l'on appelle le « graphique social[43] ».

Un schéma de comportement peut également inclure des catégories spéciales de données, dans le cas, par exemple, où elles révèlent des visites à des hôpitaux ou à des lieux de culte, la présence à des manifestations politiques ou à d'autres lieux spécifiques révélant des informations concernant la vie sexuelle par exemple. Ces profils peuvent être utilisés pour prendre des décisions pouvant affecter le propriétaire de manière significative.

La technologie des dispositifs mobiles intelligents permet une surveillance constante de données de localisation. Les téléphones intelligents peuvent collecter en permanence des signaux de stations de base et de points d'accès Wi-Fi. Sur le plan technique, la surveillance peut se faire en secret, sans en informer le propriétaire. Elle peut également se faire de manière semi secrète, lorsque les personnes « oublient » que le paramètre des services de localisation est « activé » ou n'en sont pas correctement informées, ou lorsque les paramètres d'accessibilité des données de localisation passent de « privé » à « public ».

Même lorsque les gens rendent intentionnellement leurs données de géolocalisation disponibles sur l'internet, par l'intermédiaire de services de géomarquage, l'accessibilité illimitée de ces données au niveau mondial crée de nouveaux risques (vol de données, cambriolage, voire agression physique ou harcèlement).

Comme dans le cas d'autres nouvelles technologies, le risque le plus important que comporte l'utilisation de données de localisation est le détournement d'usage, c'est-à-dire le fait que de nouvelles finalités, qui n'étaient pas prévues au moment de la collecte initiale des données, soient visées à mesure que de nouveaux types d'informations deviennent disponibles.

4. Cadre juridique

Le cadre juridique concerné est la directive sur la protection des données (95/46/CE). Il s'applique à chaque fois que des données à caractère personnel sont traitées suite au traitement de données de localisation. La directive vie privée et communications électroniques (2002/58/CE,

[43] Le « graphe social » se refère à la visibilité d'amis sur les sites de réseaux sociaux et à la capacité de déduire des traits de comportement à partir de données concernant ces amis.

telle que modifiée par la directive 2009/136/CE) s'applique uniquement au traitement des données de stations de base par les services et réseaux de communications électroniques publics (opérateurs de télécommunications).

4.1 Données de stations de base traitées par les opérateurs de télécommunications

Les opérateurs de télécommunications traitent continuellement des données de stations de base dans le cadre de la fourniture de services de communications électroniques publics[44]. Ils peuvent également traiter des données de stations de base afin d'offrir des services à valeur ajoutée. Ce cas a déjà été abordé par le groupe de travail dans l'avis 5/2005 (WP115). Bien que certains des exemples contenus dans l'avis soient inévitablement devenus caducs du fait que les appareils munis de capteurs et de technologies internet deviennent sans cesse plus petits, les conclusions et recommandations juridiques restent valables à l'égard de l'utilisation des données de stations de base.

1. Étant donné que les données de localisation issues des stations de base se rapportent à une personne physique identifiée ou identifiable, elles sont soumises aux dispositions sur la protection des données à caractère personnel prévues dans la directive 95/46/CE du 24 Octobre 1995.

2. La directive 2002/58/CE du 12 Juillet 2002 (telle que modifiée en novembre 2009 par la directive 2009/136/CE) est également applicable, selon la définition donnée à l'article 2, point c) de cette directive : « données de localisation » : toutes les données traitées dans un réseau de communications électroniques ou par un service de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public.

Si un opérateur de télécommunications offre un service de géolocalisation hybride, qui se base également sur le traitement d'autres types de données de localisation telles que des données GPS ou Wi-Fi, cette activité est considérée comme un service de communications électroniques public. L'opérateur de télécommunications doit obtenir le consentement préalable de ses clients s'il fournit ces données de géolocalisation à un tiers.

4.2 Données de stations de base, Wi-Fi et GPS traitées par des prestataires de services de la société de l'information

[44] Il convient de noter que la fourniture de hotspots Wi-Fi publics par des fournisseurs de télécommunications peut également être considérée comme un service de communications électroniques public et devrait donc principalement se conformer aux dispositions de la directive vie privée et communications électroniques.

4.2.1 Applicabilité de la directive vie privée et communications électroniques révisée

En règle générale, les sociétés qui fournissent des services et des applications de localisation sur la base d'une combinaison de données de stations de base, GPS et Wi-Fi sont des services de la société de l'information. À ce titre, elles sont explicitement exclues de la directive vie privée et communications électroniques, d'après la stricte définition du service de communications électroniques au point c) de l'article 2 de la directive-cadre révisée (non modifiée)[45].

La directive vie privée et communications électroniques ne s'applique pas au traitement des données de localisation par les services de la société de l'information, même lorsqu'un tel traitement est effectué par l'intermédiaire d'un réseau de communications électroniques public.

Un utilisateur peut choisir de transmettre des données GPS sur l'internet, lorsqu'il accède à des services de navigation sur l'internet, par exemple. Dans ce cas, le signal GPS est transmis au niveau « application » de la communication internet, indépendamment du réseau GSM. Le fournisseur de services de télécommunications joue simplement le rôle de transmetteur. Il ne peut pas accéder aux données GPS/ et/ ou Wi-Fi et/ou de stations de base communiquées échangées entre le dispositif mobile intelligent d'un utilisateur/abonné et un service de la société de l'information, à moins d'utiliser des moyens très intrusifs tels que le « deep packet inspection ».

4.2.2 Applicabilité de la directive sur la protection de la vie privée

Là où la directive vie privée et communications électroniques ne s'applique pas, la directive 95/46/CE s'applique selon l'article 1er, paragraphe 2 : « Les dispositions de la présente directive précisent et complètent la directive 95/46/CE aux fins énoncées au paragraphe 1 ».

D'après la directive sur la protection des données, on entend par données à caractère personnel toute information concernant une personne physique identifiée ou identifiable (personne concernée) ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale – article 2 de la directive. Le considérant 26 de ladite directive accorde une attention particulière au terme « identifiable » lorsqu'il énonce que « [considérant] que, pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne ; ».

Le considérant 27 de la directive expose les grandes lignes du vaste champ d'application de la protection : « [considérant] que le champ de cette protection ne doit pas en effet dépendre des techniques utilisées, sauf à créer de graves risques de détournement ; ».

Le groupe de travail a fourni des orientations détaillées quant à la définition des données à caractère personnel dans son avis 4/2007 sur le concept de données à caractère personnel.

Dispositifs mobiles intelligents

Les dispositifs mobiles intelligents sont inextricablement liés aux personnes physiques. Il est habituellement possible de les identifier directement et indirectement.

Premièrement, l'opérateur de télécommunications fournissant un accès à l'internet mobile et par GSM possède généralement

---

[45] Directive 2002/21/CE du 7 mars 2002, article 2, point c) : « service de communications électroniques » : le service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques, y compris les services de télécommunications et les services de transmission sur les réseaux utilisés pour la radiodiffusion, mais qui exclut les services consistant à fournir des contenus à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus ; il ne comprend pas les services de la société de l'information tels que définis à l'article 1er de la directive 98/34/CE qui ne consistent pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques.

un registre comportant le nom, l'adresse, et les coordonnées bancaires de chaque client, auxquels sont associés plusieurs numéros uniques du dispositif, tels que les numéros « IMEI » (identité internationale de l'équipement mobile) et « IMSI » (identité internationale de l'abonné mobile).

Deuxièmement, l'achat de logiciels supplémentaires pour le dispositif (applications ou « apps ») nécessite généralement un numéro de carte de crédit, des données d'identification directe venant ainsi s'ajouter à la combinaison du ou des numéros uniques et des données de localisation.

L'identification indirecte peut s'obtenir par l'intermédiaire de la combinaison du ou des numéros uniques du dispositif et d'une ou de plusieurs positions calculées.

Chaque dispositif mobile intelligent possède au moins un identifiant unique, à savoir l'adresse MAC. Le dispositif peut posséder d'autres numéros d'identification uniques, ajoutés par le développeur du système d'exploitation. Ces identifiants peuvent être transmis et traités ultérieurement dans le contexte de services de géolocalisation. Il est évident que la position d'un dispositif donné peut être calculée d'une manière très précise, surtout lorsque les différentes infrastructures de géolocalisation sont combinées. Cette localisation peut indiquer une maison ou un employeur. Il est notamment possible d'identifier le propriétaire du dispositif grâce à des observations répétées.

En analysant les moyens d'identification disponibles, il faut tenir compte du fait que les gens ont tendance à divulguer de plus en plus de données de localisation à caractère personnel sur l'internet, par exemple en publiant l'emplacement de leur maison ou de leur lieu de travail en combinaison avec d'autres données d'identification. Une telle divulgation de données peut également se faire à leur insu, lorsqu'ils font l'objet d'un géomarquage par d'autres personnes. Le lien peut ainsi être aisément établi entre un emplacement ou un schéma de comportement et une personne donnée.

De plus, d'après l'avis 4/2007 sur le concept de données à caractère personnel, il convient également de noter que l'attribution d'un identifiant unique, dans le contexte décrit ci-dessus, permet de repérer un utilisateur d'un dispositif spécifique, et donc de l'« isoler », même si son véritable nom n'est pas connu.

Points d'accès Wi-Fi

L'identification indirecte s'applique également aux points

d'accès Wi-Fi. L'adresse MAC d'un point d'accès Wi-Fi[46], lorsqu'elle est associée à sa position calculée, est inextricablement liée à la position du propriétaire du point d'accès.

Un responsable du traitement correctement équipé peut calculer la position d'un point d'accès Wi-Fi avec une précision de plus en plus grande en fonction de l'intensité de signal et des mises à jour régulières de la position par l'intermédiaire des utilisateurs de son service de géolocalisation.

À l'aide de ces ressources, il est possible d'identifier dans de nombreux cas le petit groupe d'appartements ou de maisons où vit le propriétaire du point d'accès. La facilité avec laquelle il est possible d'identifier ce propriétaire à partir de l'adresse MAC va dépendre de l'environnement :

- Dans des zones faiblement peuplées, dans lesquelles l'adresse MAC désigne une maison individuelle, le propriétaire de la résidence peut être déterminé directement à l'aide d'outils comme des registres de propriétaires, des annuaires de pages blanches, des listes électorales ou simplement un moteur de recherche[47].
- Dans des zones plus fortement peuplées, à l'aide de ressources comme l'intensité de signal et/ou les identifiants SSID (pouvant être détectés par quiconque possède un appareil Wi-Fi), il est possible de déterminer avec précision la position du point d'accès et ainsi, dans de nombreux cas, de déterminer l'identité de la ou des personnes vivant à l'endroit précis (maison ou appartement) où se trouve le point d'accès.
- Dans des zones très fortement peuplées, même à l'aide d'informations sur l'intensité de signal, la position possible du point d'accès qu'indiquera l'adresse MAC correspondra à plusieurs appartements Dans ces circonstances, il n'est pas possible, sans efforts déraisonnables, de déterminer avec précision l'identité de la personne vivant dans l'appartement où se trouve le point d'accès.

Le fait qu'à l'heure actuelle, dans certains cas, le propriétaire du dispositif ne peut pas être identifié à moins d'employer des moyens extrêmes ne compromet pas la conclusion générale selon laquelle la combinaison d'une adresse MAC d'un point d'accès Wi-Fi et de sa position calculée devrait être traitée de la même manière que des données à caractère personnel.

Dans ces conditions et compte tenu du fait qu'il est peu probable que le responsable du traitement des données fasse la distinction entre les cas où le propriétaire du point d'accès Wi-Fi est identifiable et les cas où il ne l'est pas, le responsable du traitement des données devrait traiter toutes les données concernant les routeurs Wi-Fi comme des données à caractère personnel.

Il est important de rappeler qu'il n'est pas nécessaire que la finalité du traitement de ces données de géolocalisation soit d'identifier les utilisateurs. L'intensité des efforts requis pour identifier les propriétaires des points d'accès Wi-Fi dépend fortement des moyens techniques dont dispose le responsable du traitement ou toute autre personne pour identifier lesdits propriétaires.

5. Obligations découlant de la législation sur la protection des données

5.1 Responsable du traitement des données

Dans le contexte des services de géolocalisation en ligne que procurent les services de la société de l'information, on distingue trois fonctions différentes, auxquelles sont associées des responsabilités distinctes en matière de traitement des données à caractère personnel. Il s'agit du responsable d'une infrastructure de géolocalisation ; du fournisseur d'application ou de service de géolocalisation spécifique et du développeur du système d'exploitation d'un dispositif mobile intelligent. En

[46] Les points d'accès Wi-Fi peuvent même être identifiables directement, si le fournisseur d'accès à l'internet conserve un registre des adresses MAC des routeurs Wi-Fi qu'il fournit à ses clients identifiés.

[47] La disponibilité de tels registres ou annuaires varie selon l'État membre.

pratique, les sociétés endossent souvent de nombreux rôles en même temps, par exemple lorsqu'elles combinent un système d'exploitation doté d'une base de données comprenant des points d'accès Wi-Fi mappés et une plate-forme publicitaire.

5.1.1 Responsables d'infrastructure de géolocalisation

Tout comme le font les opérateurs de télécommunications lorsqu'ils traitent la position d'un dispositif spécifique à l'aide de leurs stations de base, les propriétaires de bases de données comprenant des points d'accès Wi-Fi mappés traitent des données à caractère personnel lorsqu'ils calculent la position d'un dispositif mobile intelligent spécifique. Étant donné que les opérateurs et les propriétaires déterminent les finalités et modalités de ce traitement, ils sont considérés comme des responsables du traitement au sens de l'article 2, point d), de la directive sur la protection des données.

Il est important de souligner que le dispositif spécifique contribue à calculer sa position en transmettant au propriétaire de la base de données ses propres données de localisation (la plupart du temps une combinaison de données GPS, Wi-Fi et de stations de base) et les identifiants uniques des points d'accès Wi-Fi à proximité immédiate[48]. Un tel dispositif répond également au critère de l'article 4.1, point c) de la directive sur la protection des données, moyens situés sur le territoire d'un État membre.

Étant donné que l'adresse MAC d'un point d'accès Wi-Fi, combinée à sa position calculée, devrait être considérée de la même manière que des données à caractère personnel, la collecte de ces données entraîne également le traitement de données à caractère personnel. Quelle que soit la manière dont ces données sont collectées (une seule fois ou régulièrement), le propriétaire d'une telle base de données doit se conformer aux obligations découlant de la directive sur la protection des données.

5.1.2 Fournisseurs d'applications et de services de géolocalisation

Les dispositifs mobiles intelligents permettent l'installation de logiciels de tiers, appelés « applications ». De telles applications peuvent traiter les données de localisation (et autres données) d'un dispositif mobile intelligent indépendamment du développeur du système d'exploitation et/ou des responsables d'infrastructure de géolocalisation.

Comme exemples de tels services, on citera un service

[48] Le dispositif mobile peut transmettre les diverses données de géolocalisation qu'il reçoit au responsable du traitement qui calculera sa position, ou calculer sa position lui-même. Dans les deux cas, le dispositif consitue un équipement essentiel au traitement.

météorologique qui prévoit les risques de pluie dans les prochaines heures dans une région très spécifique, un service qui procure des informations sur les commerces à proximité, un service d'identification de téléphone égaré ou un service qui indique à l'utilisateur l'emplacement de ses amis.

Le fournisseur d'une application capable de traiter des données de géolocalisation est le responsable du traitement de données à caractère personnel résultant de l'installation et de l'utilisation de l'application. Il n'est évidemment pas nécessaire de toujours installer un logiciel séparé sur un dispositif mobile intelligent. Il est également possible d'accéder à de nombreux services de géolocalisation par l'intermédiaire d'un navigateur. Un service de ce genre peut par exemple consister en l'utilisation d'une carte en ligne pour guider une personne se déplaçant à pied dans une ville.

5.1.3 Développeur du système d'exploitation

Le développeur du système d'exploitation du dispositif mobile intelligent peut être un responsable du traitement des données de géolocalisation lorsqu'il est directement en interaction avec l'utilisateur et recueille des données à caractère personnel (en demandant un enregistrement initial de l'utilisateur et/ou en recueillant des informations de localisation aux fins de l'amélioration des services). En tant que responsable du traitement, le développeur doit appliquer les principes de la prise en compte du respect de la vie privée dès la conception pour éviter la surveillance secrète, soit par le dispositif lui-même, soit par les différents services et applications.

Un développeur est également le responsable du traitement des données qu'il détient si le dispositif possède une fonctionnalité « phone home » au moyen de laquelle il transmet des informations sur le lieu où il se trouve. Étant donné que dans ce cas le développeur décide des modalités et finalités de ce transfert de données, il est le responsable du traitement de ces données. Un exemple courant d'une telle fonctionnalité « phone home » est la mise à jour automatique du fuseau horaire en fonction de l'emplacement.

Troisièmement, le développeur est responsable du traitement lorsqu'il offre une plate-forme publicitaire et/ou un environnement de type « magasin en ligne » pour la vente d'applications et qu'il est capable de traiter des données à caractère personnel résultant (de l'installation et de l'utilisation) des applications de géolocalisation, indépendamment des fournisseurs d'application.

5.2 Responsabilités des autres parties

Il existe bien d'autres parties en ligne qui permettent de traiter (ultérieurement) des données de localisation, telles que les navigateurs, les sites de socialisation ou les supports de communication qui permettent le « géomarquage » par exemple. Lorsqu'elles intègrent des fonctions de géolocalisation dans leur plate-forme, ces parties ont une grande part de responsabilité dans la définition des paramètres par défaut de l'application (activation ou désactivation par défaut). Bien qu'elles ne soient des responsables du traitement que dans la mesure où elles traitent elles-mêmes des données à caractère personnel de manière active, ces parties ont un rôle essentiel à jouer pour garantir le caractère légitime du traitement de données effectué par des responsables du traitement tels que les fournisseurs d'applications spécifiques, par exemple lorsqu'il s'agit de la visibilité et de la qualité des informations concernant le traitement des données de géolocalisation.

5.3 Motif légitime

5.3.1 Dispositifs mobiles intelligents

Si des opérateurs de télécommunications veulent utiliser des données de stations de base afin de fournir un service à valeur

ajoutée à un client, conformément à la directive vie privée et communications électroniques révisée, ils doivent obtenir le consentement préalable du client. Ils doivent également s'assurer que le client est informé des modalités de ce traitement.

Étant donné le caractère sensible du traitement de (schémas de) données de localisation, le consentement préalable en connaissance de cause est également le principal motif conférant un caractère légitime au traitement de données quand il s'agit du traitement des emplacements d'un dispositif mobile intelligent dans le contexte des services de la société de l'information.

Conformément à la directive sur la protection des données, article 2, point h), le consentement doit être une manifestation de volonté, libre, spécifique et informée des souhaits de la personne concernée.

En fonction du type de technologie utilisée, le dispositif de l'utilisateur joue un rôle relativement actif dans le traitement des données de géolocalisation. Le dispositif est capable de transmettre des données de localisation de différentes sources à des tiers. L'existence de cette capacité technique ne signifie pas qu'un tel traitement de données est automatiquement légal. Dans le cas où les paramètres par défaut d'un système d'exploitation permettraient la transmission de données de localisation, une absence d'intervention de la part des utilisateurs ne devrait pas être assimilée à un libre consentement de ces derniers.

Dans la mesure où les développeurs de systèmes d'exploitation et d'autres services de la société de l'information traitent eux-mêmes activement des données de géolocalisation (par exemple lorsqu'ils obtiennent des informations de localisation à partir du dispositif ou par son intermédiaire), ils doivent également chercher à obtenir le consentement préalable en connaissance de cause des utilisateurs. Il convient de préciser qu'un tel consentement ne peut pas être obtenu librement en obligeant les utilisateurs à accepter les conditions générales, ni en leur proposant des possibilités de non-participation. Par défaut, les services de localisation devraient être désactivés, et les utilisateurs devraient pouvoir choisir de les activer pour certaines applications spécifiques.

Consentement des travailleurs

Le consentement en tant que motif légitime de traitement est problématique dans le contexte professionnel. Le groupe de travail, dans son avis sur le traitement des données à caractère personnel dans le contexte professionnel a écrit : « si le consentement du travailleur est nécessaire et que l'absence de consentement peut entraîner un préjudice réel ou potentiel pour le travailleur, le consentement n'est pas valable au titre de l'article 7 ou de l'article 8, dans la mesure où il n'est pas donné librement. Si le travailleur n'a pas la possibilité de refuser, il ne s'agit pas de consentement. (…) Une pierre d'achoppement peut exister si le consentement est une condition d'emploi. Le travailleur peut, en théorie, refuser de donner son consentement, mais il peut perdre alors une opportunité d'emploi. Dans ces circonstances, le consentement n'étant pas donné librement, n'est donc pas valable »[49]. Au lieu de chercher à obtenir le consentement, les employeurs devraient déterminer s'il est possible de prouver la nécessité de surveiller l'emplacement exact des travailleurs pour une finalité légitime et mettre en balance cette nécessité avec les droits et libertés fondamentaux des travailleurs. Dans le cas où la nécessité peut être dûment justifiée, la base juridique d'un tel traitement pourrait se fonder sur l'intérêt légitime du responsable du traitement [article 7, point f) de la directive sur la protection des données]. L'employeur doit toujours rechercher le moyen le moins intrusif, éviter une surveillance continuelle et par exemple choisir un système qui envoie une alerte lorsqu'un travailleur traverse une frontière virtuelle définie au préalable. Un travailleur doit pouvoir éteindre tout appareil de surveillance en dehors des heures de travail et la manière de le faire doit lui être expliquée. Les dispositifs de surveillance des véhicules ne sont pas des dispositifs de surveillance du personnel. Leur fonction est de repérer ou de contrôler la position des véhicules dans lesquels ils sont installés. Les employeurs ne devraient pas les considérer comme des dispositifs leur permettant de repérer ou contrôler le comportement ou les allées et venues de chauffeurs ou autres membres du personnel, par exemple en envoyant des alertes en rapport avec la vitesse du véhicule.

Consentement des enfants

Dans certains cas, le consentement des enfants doit être donné par les parents ou autres représentants légaux. Cela implique par exemple que le fournisseur d'une application de géolocalisation doit notifier les parents de la collecte et de l'utilisation de données de géolocalisation concernant leurs enfants et obtenir leur consentement avant de recueillir et d'utiliser ultérieurement les informations concernant leurs enfants. Certaines applications de géolocalisation sont spécifiquement conçues pour la surveillance parentale, par exemple en révélant en permanence la position du dispositif sur un site Web, ou en émettant une alerte si l'appareil quitte un territoire délimité au préalable. L'utilisation de telles applications pose problème. Le groupe de travail « article 29 », dans son avis 2/2009[50] sur la protection de données d'enfants à caractère personnel, a écrit : Il ne devrait jamais arriver que, pour des raisons de sécurité, les enfants soient confrontés à une surveillance excessive limitant leur autonomie. Dans ce contexte, un équilibre doit être trouvé entre la protection de l'intimité et de la vie privée des enfants, et leur sécurité.

Le cadre juridique prévoit que les parents sont responsables de la protection du droit à la vie privée de leurs enfants. Pour le moins, si les parents estiment que l'utilisation d'une telle application est justifiée dans des circonstances spécifiques, les enfants doivent en être informés et doivent pouvoir participer, dès que cela s'avère raisonnablement possible, à la décision d'utiliser une telle application.

[49] WP 148, avis 8/2011 sur le traitement des données à caractère personnel dans le contexte professionnel.
[50] WP 160, Avis 2/2009 sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier des écoles).

7 Annexes

Le consentement doit être spécifique, pour chacune des différentes finalités pour lesquelles les données sont traitées. Le responsable du traitement doit faire savoir de manière très claire si son service se limite à donner une réponse à la question volontaire « Où suis-je en ce moment précis ? », ou si son objectif est de créer des réponses aux questions « Où êtes-vous, où avez-vous été et où serez-vous la semaine prochaine ? ». En d'autres termes, le responsable du traitement doit accorder une attention particulière au consentement donné pour des finalités auxquelles la personne concernée n'est pas préparée, comme par exemple pour l'établissement de profils et/ou le ciblage comportemental.

Si les finalités du traitement changent de manière significative, le responsable du traitement doit solliciter une nouvelle fois le consentement spécifique. Par exemple, s'il a été initialement mentionné par une société qu'elle ne partagerait pas de données à caractère personnel avec une autre société, mais qu'elle souhaite à présent les partager, elle doit solliciter activement le consentement préalable de chaque client. Une absence de réponse (ou tout autre type de scénario de non-participation) ne suffit pas.

Il est important d'effectuer une distinction entre le consentement donné pour un service ponctuel et celui donné dans le cadre d'un abonnement régulier. Par exemple, afin d'utiliser un service de géolocalisation spécifique, il peut être nécessaire d'activer les services de géolocalisation du dispositif ou du navigateur. Si cette fonctionnalité de géolocalisation est activée, les sites Web peuvent tous lire les informations de localisation de l'utilisateur de ce dispositif mobile intelligent. Afin de prévenir les risques de surveillance secrète, le groupe de travail « article 29 » considère qu'il est essentiel que le dispositif avertisse continuellement l'utilisateur que la géolocalisation est activée, par exemple par l'intermédiaire d'une icône visible en permanence.

Le groupe de travail recommande aux fournisseurs d'applications ou de services de géolocalisation de solliciter une nouvelle fois le consentement de la personne (même lorsqu'aucune modification n'a été apportée à la nature du traitement) après un délai approprié.

Par exemple, il y aurait lieu de cesser de traiter les données de localisation dans le cas où une personne n'aurait pas activement utilisé le service au cours des 12 derniers mois. Même dans le cas où le service est utilisé, la nature du traitement de ses données à caractère personnel doit lui être rappelée au moins une fois par an (ou plus souvent si la nature

du traitement le justifie) et un moyen de renoncer facilement à participer au traitement de données doit lui être proposé.

Enfin, la personne concernée doit surtout pouvoir retirer son consentement très facilement, sans aucun effet négatif sur l'utilisation de son appareil. Indépendamment des directives européennes sur la protection des données, le World Wide Web Consortium (W3C) a élaboré un projet de norme pour l'API de géolocalisation qui souligne la nécessité d'un consentement préalable, libre, exprès et éclairé[51]. Le W3C explique notamment la nécessité de respecter le retrait du consentement, en conseillant aux personnes chargées de la mise en œuvre de la norme de considérer que « le contenu hébergé à une adresse URL donnée évolue de telle façon que les autorisations de localisation déjà accordées ne s'appliquent plus en ce qui concerne l'utilisateur. Ou alors, les utilisateurs auront simplement changé d'avis ».

Exemple de meilleure pratique pour les fournisseurs d'applications de géolocalisation

Une application qui souhaite utiliser des données de géolocalisation informe clairement l'utilisateur des raisons pour lesquelles elle souhaite utiliser les données, et demande un consentement sans équivoque pour chacune de ces raisons qui peuvent différer les unes des autres. L'utilisateur choisit activement le niveau de granularité de géolocalisation (par exemple à l'échelle d'un pays, d'une ville, d'un code postal, ou à l'échelle la plus précise possible). Une fois que le service de localisation est activé, une icône indiquant que les services de localisation sont activés est visible en permanence sur chaque écran. L'utilisateur peut retirer son consentement à tout moment, sans avoir à quitter l'application. L'utilisateur est également en mesure de supprimer facilement et de manière définitive toute donnée de localisation stockée sur le dispositif.

5.3.2 Points d'accès Wi-Fi

Sur la base de la directive sur la protection des données, les sociétés peuvent avoir un intérêt légitime à recueillir et à traiter les adresses MAC et les positions calculées de points d'accès Wi-Fi dans le but spécifique d'offrir des services de géolocalisation.
Le motif légitime de l'article 7, point f) de la directive sur la protection des données requiert un équilibre entre les intérêts légitimes du responsable du traitement et les droits fondamentaux des personnes concernées. Étant donné la nature semi statique des points d'accès Wi-Fi, le mappage de points d'accès Wi-Fi représente en principe une menace moins grande à l'égard de la vie privée des propriétaires de ces points d'accès que celle du repérage en temps réel des positions de dispositifs mobiles intelligents. L'équilibre à trouver entre les droits du responsable du traitement et les droits de la personne concernée est dynamique. Afin que les responsables du traitement réussissent à laisser leurs intérêts légitimes prévaloir avec le temps sur les intérêts des personnes concernées, ils doivent élaborer et mettre en œuvre des garanties, comme le droit de renoncer facilement et de façon définitive à participer à la base de données, sans avoir à fournir de données à caractère personnel supplémentaires au responsable du traitement d'une telle base de données. Ils peuvent par exemple utiliser un logiciel pour détecter automatiquement qu'une personne est connectée à un point d'accès spécifique[52].

[51] API de géolocalisation du W3C : http://www.w3.org/TR/geolocation-API/

[52] Exemple d'utilisation possible :
1. Une personne concernée se rend sur une page Web spécifique, sur laquelle elle peut entrer l'adresse MAC de son point d'accès Wi-Fi.
2. Si l'adresse MAC apparaît dans la base de données avec les points d'accès Wi-Fi mappés, le responsable du traitement peut faire apparaître une page de vérification contenant un script qui demande la table ARP du dispositif internet. En théorie, il est possible de voir les adresses MAC de réseau WLAN par l'intermédiaire de la commande « ARP –a ». À l'aide du code contenu dans le navigateur, tel que Java, cette table ARP peut être produite en arrière-plan.
3. Si l'adresse MAC n'apparaît pas dans la table ARP, il est déterminé que l'utilisateur connecté au réseau local sans fil est également celui ayant accès à l'adresse MAC de réseau WLAN locale. Le responsable du traitement vérifie ainsi automatiquement et facilement la demande de suppression.

De plus, la collecte et le traitement d'identifiants SSID ne sont pas nécessaires pour pouvoir offrir des services de géolocalisation. Par conséquent, la collecte et le traitement d'identifiants SSID sont des procédés disproportionnés lorsqu'il s'agit d'offrir des services de géolocalisation basés sur le mappage de la position de points d'accès Wi-Fi.

5.4 Informations

Les différents responsables du traitement doivent s'assurer que les propriétaires de dispositifs mobiles intelligents sont dûment informés des éléments clés du traitement, conformément à l'article 10 de la directive sur la protection des données, tels que leur identité en tant que responsables du traitement, les finalités du traitement, le type de données, la durée du traitement, les droits des personnes concernées d'accéder à leurs données, de les rectifier ou de les supprimer et leur droit de retirer leur consentement.

La validité du consentement est inextricablement liée à la qualité des informations concernant le service. Les informations doivent être claires, exhaustives, compréhensibles pour un large public non initié, et accessibles facilement et en permanence.

Les informations doivent toucher un public très large. Les responsables du traitement ne peuvent supposer que leurs clients sont des personnes techniquement compétentes, simplement parce qu'elles possèdent un dispositif mobile intelligent. Les informations doivent être adaptées à l'âge si le responsable du traitement sait qu'il s'adresse à un public jeune.

Si des fournisseurs d'applications de géolocalisation comptent calculer les positions d'un dispositif plus d'une fois, ils doivent tenir leurs clients informés aussi longtemps qu'ils traitent des données de localisation. Ils doivent également permettre à leurs clients de prolonger ou de révoquer leur consentement. Afin d'atteindre ces objectifs, les fournisseurs d'applications devraient travailler en étroite collaboration avec le développeur du système d'exploitation. Sur le plan technique, le développeur est le mieux placé pour créer un rappel visible en permanence indiquant que des données de localisation sont en cours de traitement. Le développeur est également le mieux placé pour faire en sorte qu'aucune des applications proposées ne surveille en secret l'emplacement des dispositifs mobiles intelligents. Si le développeur du système d'exploitation a créé une fonctionnalité « phone home » ou un autre moyen pour obtenir l'accès à des données stockées sur le dispositif, ou qu'il obtient l'accès à des données de localisation par d'autres moyens,

par l'intermédiaire d'annonceurs tiers par exemple, il doit informer la personne concernée au préalable des raisons (spécifiques et légitimes) pour lesquelles il traite ces données et de la durée du traitement.

L'obligation de tenir informées les personnes concernées s'applique également aux responsables de bases de données comportant des points d'accès Wi-Fi géolocalisés. Ils doivent informer le grand public de manière adéquate sur leur identité et les finalités du traitement ainsi que sur d'autres données pertinentes. La simple mention d'une éventuelle collecte de données concernant des points d'accès Wi-Fi dans une déclaration de confidentialité spécifique à l'intention des utilisateurs d'une application de géolocalisation n'est pas suffisante. Il existe suffisamment de moyens, en ligne et hors ligne, permettant d'informer le grand public.

5.5 Droits des personnes concernées

Les personnes concernées sont en droit d'obtenir, de la part des différents responsables du traitement, un accès aux données de localisation obtenues à partir de leurs dispositifs mobiles intelligents, ainsi que des informations sur les finalités du traitement et les destinataires ou catégories de destinataires à qui les données ont été divulguées. Les informations doivent être fournies dans une version directement lisible, à savoir, sous la forme de positions géographiques, et non pas de numéros abstraits de stations de base, par exemple.

Les personnes concernées sont également en droit d'accéder aux profils possibles basés sur ces données de localisation. Si les informations de localisation sont stockées, les utilisateurs devraient être autorisés à mettre à jour, rectifier ou effacer ces informations.

Le groupe de travail recommande aux responsables du traitement de chercher des moyens sécurisés permettant de fournir un accès direct en ligne aux données de localisation et aux profils possibles. Il est essentiel qu'un tel accès soit fourni sans demander de données à caractère personnel supplémentaires pour vérifier l'identité des personnes concernées.

5.6 Délais de conservation

Les fournisseurs de services de géolocalisation et d'application devraient déterminer un délai de conservation pour les données de localisation dont la durée n'excède pas celle nécessaire aux fins pour lesquelles les données ont été collectées ou font l'objet d'un traitement ultérieur. Ils doivent s'assurer que les données de géolocalisation, ou les profils fondés sur ces données, sont effacées après une période de temps justifiée.

Dans le cas où il a été prouvé qu'il est nécessaire pour le développeur du système d'exploitation et/ou le responsable d'une infrastructure de géolocalisation de recueillir des données d'historique de localisation anonymes dans le but de mettre à jour ou d'améliorer leur service, il convient de faire preuve d'une extrême prudence pour éviter de rendre ces données identifiables (indirectement). En particulier, même si le dispositif mobile est identifié à l'aide d'un identifiant unique (UDID) attribué de manière aléatoire, un tel numéro unique ne devrait être stocké que pour une période maximale de 24 heures à des fins opérationnelles. Après cette période, l'identifiant UDID devrait être anonymisé davantage en tenant compte du fait qu'une véritable anonymisation est de plus en plus difficile à obtenir et que la combinaison des données de localisation peut tout de même aboutir à une identification. Un tel UDID ne devrait ni pouvoir être associé à de précédents ou futurs UDID attribués au dispositif, ni être associé à un quelconque identifiant fixe de l'utilisateur ou du téléphone (tel qu'une adresse MAC, un numéro IMEI ou IMSI, ou tout autre numéro de compte).

En ce qui concerne des données

relatives à des points d'accès Wi-Fi, une fois que l'adresse MAC d'un point d'accès Wi-Fi est associée à une nouvelle position, sur la base des observations continues de propriétaires de dispositifs mobiles intelligents, la position précédente doit être immédiatement supprimée, pour éviter toute utilisation ultérieure des données à des fins inappropriées, telles que des démarches commerciales visant des personnes ayant modifié leur position.

6. Conclusions

Les technologies de géolocalisation qui utilisent les données de stations de base, les données GPS et les points d'accès Wi-Fi mappés, permettent à toutes sortes de responsables du traitement de localiser des dispositifs mobiles intelligents pour des finalités allant de la publicité comportementale à la surveillance des enfants.

Étant donné que les téléphones intelligents et les tablettes électroniques sont inextricablement liés à leur propriétaire, les schémas de déplacement des dispositifs donnent une vision détaillée de l'intimité de la vie privée des propriétaires. L'un des principaux risques est que les propriétaires ignorent qu'ils transmettent leur position et à qui ils les transmettent. Un autre risque est que l'autorisation donnée à certaines applications d'utiliser les données de localisation n'est pas valable, car les informations concernant les éléments clés du traitement sont incompréhensibles, désuètes ou inadéquates.

Les obligations diffèrent en fonction des parties intéressées, qui vont des développeurs des systèmes d'exploitation aux fournisseurs d'application et parties telles que les sites de socialisation qui intègrent dans leurs plates-formes des fonctions de localisation destinées à des dispositifs mobiles.

6.1 Cadre juridique

- Le cadre juridique de l'UE pour l'utilisation de données de géolocalisation provenant de dispositifs mobiles intelligents est fourni principalement par la directive sur la protection des données. Les données de localisation provenant de dispositifs mobiles intelligents sont des données à caractère personnel. La combinaison de l'adresse MAC unique et de la position calculée d'un point d'accès Wi-Fi devrait être traitée de la même manière que des données à caractère personnel.
- De plus, la directive 2002/58/CE révisée sur la vie privée et les communications électroniques ne s'applique qu'au traitement

de données de stations de base par des opérateurs de télécommunications.

6.2 Responsables du traitement

- Il est possible de distinguer trois types de responsables du traitement : les responsables d'infrastructure de géolocalisation (notamment les responsables de points d'accès Wi-Fi mappés) ; les fournisseurs d'applications et de services de géolocalisation ; et les développeurs de système d'exploitation de dispositifs mobiles intelligents.

6.3 Motif légitime

- Étant donné que les données de dispositifs mobiles intelligents révèlent des détails intimes sur la vie privée de leur propriétaire, le principal motif légitime applicable est le consentement préalable en connaissance de cause.
- Le consentement ne peut pas être obtenu par l'intermédiaire de l'acceptation des conditions générales.
- Le consentement doit être spécifique pour chacune des différentes finalités pour lesquelles les données sont traitées, par exemple l'établissement de profils et/ou le ciblage comportemental par le responsable du traitement. Si les finalités du traitement changent de manière significative, le responsable du traitement doit chercher à obtenir une nouvelle fois le consentement spécifique.
- Par défaut, les services de localisation doivent être désactivés. Le fait de proposer la possibilité de renoncer au transfert de données ne constitue pas un mécanisme adéquat pour obtenir le consentement en connaissance de cause d'un utilisateur.
- Le consentement pose problème en ce qui concerne les travailleurs et les enfants. En ce qui concerne les travailleurs, les employeurs ne peuvent utiliser cette technologie que lorsqu'il est possible de prouver qu'elle est nécessaire pour une finalité légitime, et que les mêmes objectifs ne peuvent pas être atteints à l'aide de moyens moins intrusifs. En ce qui concerne les enfants, c'est à leurs parents de juger si l'utilisation d'une telle application est justifiée dans certaines circonstances. Les parents doivent à tout le moins informer leurs enfants, et dès que raisonnablement possible, permettre à leurs enfants de participer à la décision d'utiliser une telle application.
- Le groupe de travail recommande de limiter la portée du consentement dans le temps et de recontacter les utilisateurs au moins une fois par an. Il recommande également de détailler suffisamment le consentement en ce qui concerne la précision des données de localisation.
- Les personnes concernées doivent pouvoir retirer facilement leur consentement, sans aucune conséquence négative pour l'utilisation de leur dispositif.
- En ce qui concerne le mappage de points d'accès Wi-Fi, les sociétés peuvent avoir un intérêt légitime à recueillir et à traiter les adresses MAC et les positions calculées de points d'accès Wi-Fi dans le but spécifique d'offrir des services de géolocalisation. La mise en balance des droits du responsable du traitement, d'une part, et des droits des personnes concernées, d'autre part, nécessite que le responsable du traitement accorde aux utilisateurs le droit de renoncer de manière aisée et définitive à participer à la base de données, sans exiger la fourniture de données à caractère personnel supplémentaires.

6.4 Les informations

- Les informations doivent être claires, exhaustives, compréhensibles pour un large public non initié et accessibles facilement et en permanence.
- La validité du consentement est inextricablement liée à la qualité des informations concernant le service.
- Les tiers, tels que les navigateurs et les sites de socialisation ont un rôle

essentiel à jouer lorsqu'il s'agit de la visibilité et de la qualité des informations concernant le traitement des données de géolocalisation.

6.5 Droits des personnes concernées

- Les différents responsables du traitement d'informations de géolocalisation provenant de dispositifs mobiles doivent permettre à leurs clients d'accéder à leurs données de localisation dans une version directement lisible et les autoriser à les rectifier ou à les supprimer sans recueillir une quantité excessive de données à caractère personnel.
- Les personnes concernées ont également le droit d'accéder aux éventuels profils, de les rectifier et de les supprimer en fonction de ces données de localisation.
- Le groupe de travail recommande la création d'un accès en ligne (sécurisé).

6.6 Délais de conservation

- Les fournisseurs d'applications ou de services de géolocalisation doivent mettre en œuvre des politiques de conservation garantissant que des données de géolocalisation ou des profils découlant de telles données sont supprimés après une période de temps justifiée.
- Si le développeur du système d'exploitation et/ou le responsable du traitement de l'infrastructure de géolocalisation traitent un numéro unique tel qu'une adresse MAC ou un identifiant UDID en rapport avec des données de localisation, le numéro d'identification unique ne peut être stocké que pour une période maximale de 24 heures, à des fins opérationnelles.

Fait à Bruxelles, le 16 mai 2011

Pour le groupe de travail
Le président
Jacob Kohnstamm

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