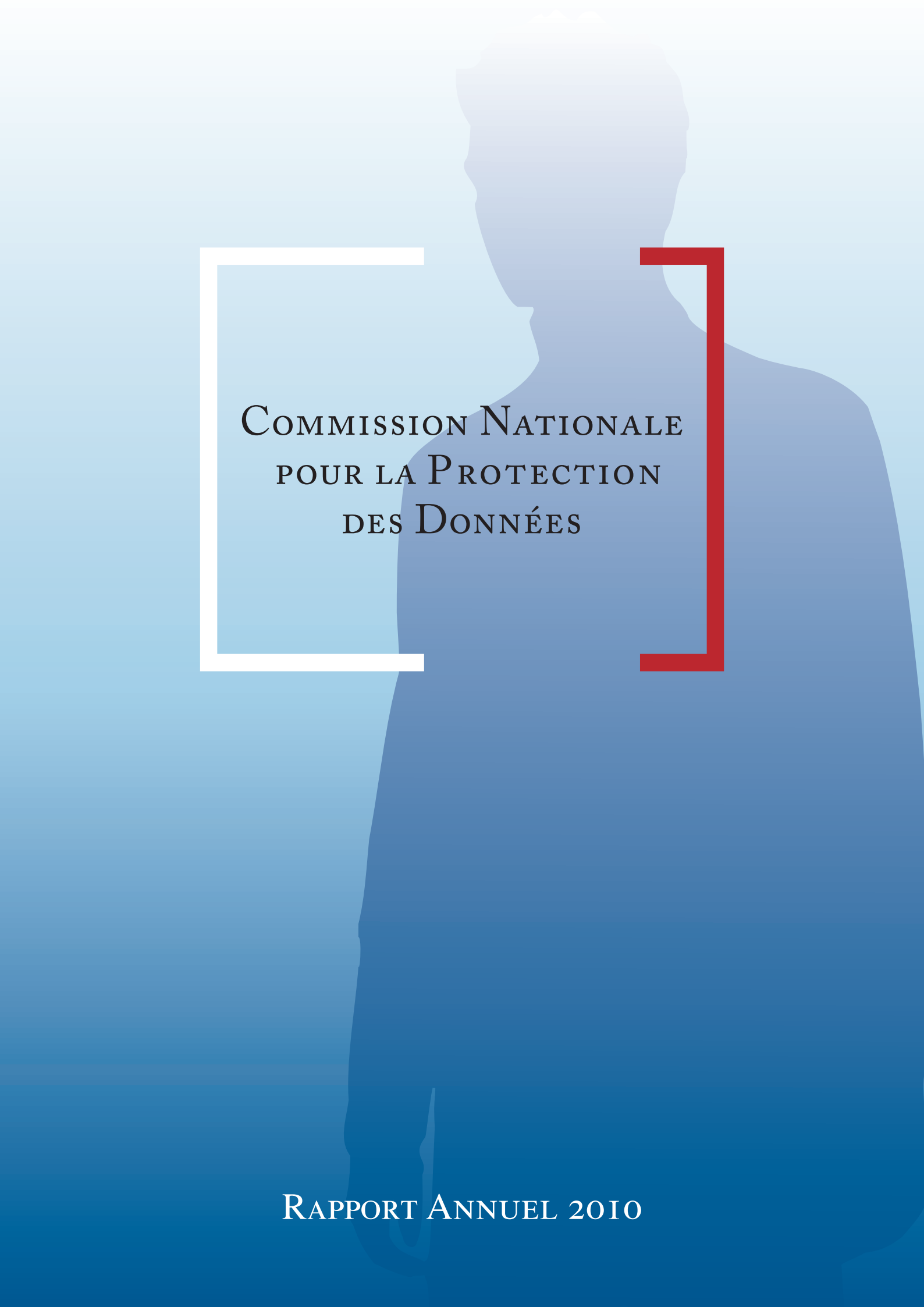


Commission Nationale pour la Protection des Données

Rapport Annuel 2010

Mission

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

Superviser et assurer la transparence par :

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

Informer et guider avec :

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

Conseiller et coopérer à travers :

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

Table des matières

ANNEXES :

Avis et décisions

Traitements standards susceptibles de faire l'objet d'une notification unique

Participations aux travaux européens

1 Avant-propos

À l'heure où nous affichons chaque jour un peu plus de notre vie privée sur Internet, et où nous nous accommodons plus ou moins consciemment d'être surveillés, tracés et localisés de plus en plus souvent (en ligne, sur le lieu de travail, en nous déplaçant, en achetant, en téléphonant...), la protection des données à caractère personnel prend une importance croissante. Elle vise à endiguer des excès, à prévenir les abus, à sensibiliser, à assurer un juste équilibre des intérêts et à concilier le rôle de plus en plus important pris par les TIC (Technologies de l'information et de la communication) dans notre société avec la préservation d'une sphère privée essentielle à la dignité humaine. 2010 a été une année bien chargée pour la Commission nationale pour la protection des données (CNPD) qui a pour mission de veiller au respect des règles légales en la matière.

Parmi les temps forts de l'année, citons en premier lieu l'avis sur la réforme du système de soins de santé dans lequel la Commission nationale a exprimé ses observations touchant en particulier les différents aspects relatifs au dossier de soins partagé, les rôles respectifs des intervenants impliqués, les droits des patients et la sécurité de la plateforme informatique. Dans le domaine de la santé, elle s'efforce par ailleurs de promouvoir et d'harmoniser l'application d'un ensemble de règles basiques de bonnes pratiques par les professionnels (cliniques, cabinets médicaux et fournisseurs de soins) concernant les données des patients tout en respectant les exigences du bon fonctionnement de ce secteur d'activités.

L'année 2010 ne saurait être évoquée sans qu'il soit aussi fait état de la prise de position de la Commission nationale par rapport au projet de loi n°6113 ayant pour objet la transposition de la directive sur la rétention des données. L'accès de la police et des autorités judiciaires aux données traitées par des fournisseurs de services de communications électroniques dans le but de la lutte contre le terrorisme et la criminalité grave reste controversé dans un certain nombre de pays européens et, même lorsque le principe d'une telle conservation obligatoire est accepté, des restrictions et mesures de sauvegarde s'imposent.

Par ailleurs, les représentants de la Commission nationale ont pris un rôle actif dans divers groupes de travail européens auprès du Conseil de l'Europe pour défendre le secret bancaire comme une forme non dépassée - si appliquée avec bon sens - de la protection de la vie privée des citoyens. Ils ont donné à considérer que l'échange automatisé de données relatives à l'épargne des non-résidents n'est pas la solution la plus respectueuse des droits fondamentaux, ni la plus efficiente pour assurer une imposition efficace des revenus transnationaux.

La Commission nationale a également avisé le projet de loi n°6243 portant modification de la loi modifiée du 30 mai 2005 sur la protection de la vie privée dans le secteur des communications électroniques. L'obligation de signaler les incidents de sécurité et les violations de la confidentialité des données traitées par les exploitants de réseaux et prestataires de services constitue l'innovation la plus importante de la révision de la directive « e-privacy » tout comme le renforcement des garanties de transparence et d'usage loyal des « cookies ».

Dans un souci de guidance et simplification administrative, la Commission nationale a adopté, au début de l'année, une notification-modèle pour les traitements de données à caractère personnel des communes, élaborée en concertation avec le Ministère de l'Intérieur, le SYVICOL et le SIGI. Celle-ci facilite dorénavant considérablement la déclaration des fichiers tenus par les administrations communales.

De plus, la Commission nationale a introduit en 2010 une nouvelle mesure afin d'accroître la transparence et l'information vis-à-vis des citoyens. Elle demande désormais aux titulaires d'autorisation d'exploitation de systèmes de vidéosurveillance d'afficher sur les panneaux d'information afférents des vignettes autocollantes spécifiques portant le numéro courant avec lequel le traitement figure dans le registre public. Ainsi, les citoyens seront en mesure de départager eux-mêmes les vidéosurveillances autorisées de celles qui ne le seraient éventuellement pas et se renseigner davantage sur les conditions et restrictions applicables en consultant la fiche du système en question dans le registre public accessible sur Internet.

Depuis la création de la CNPD, plus de 16.000 traitements de données lui ont été déclarés, dont 2300 pour des installations de vidéosurveillance. Le nombre de plaintes a plus que doublé par rapport à l'année 2008. En 2010, elle a reçu 145 plaintes ou demandes de vérification de licéité par des citoyens estimant que leurs droits n'ont pas été respectés. De plus, elle a dû intervenir à plusieurs reprises lorsque sont apparues des failles de sécurité dans des applications web de divers fournisseurs de service grand-public mettant en péril la confidentialité des données des utilisateurs.

Elle a continué d'accompagner les projets publics ayant un impact sur la protection des données et de la vie privée des citoyens comme, par exemple, le recensement général de la population, le plan national « e-Santé », la réforme du droit d'établissement, les radars automatiques sur le réseau routier, l'identifiant unique des personnes physiques, les projets de recherche clinique, les statistiques et études dans les domaines social et familial, ...

Elle a par ailleurs entrepris des actions de sensibilisation ponctuelles et participé à de nombreuses conférences et formations pour présenter les enjeux de la protection des données à un public plus spécialisé (LTB, INAP, École Supérieure du travail, LCGB, Université du Luxembourg, ABBL, etc.).

La Directive 2009/136/CE devrait être transposée prochainement en droit luxembourgeois par l'adoption du projet de loi n°6243 par la Chambre des Députés. Cette récente révision de la Directive 2002/58/CE introduit l'obligation pour les fournisseurs de services de communications électroniques de notifier les failles de sécurité à l'autorité nationale et, dans certaines circonstances, d'en informer également les personnes concernées. Pour faire face à cette nouvelle mission de surveillance, la petite équipe de la CNPD aura sans doute besoin d'un surcroît d'énergie. Elle compte aussi sur l'arrivée d'un nouveau collaborateur à compétence informatique et technologique qui devrait finalement lui être accordé.

En automne 2011, la Commission européenne présentera des propositions législatives concrètes pour la révision de la directive sur la protection des données (Directive 95/46/CE). Après l'entrée en vigueur du Traité de Lisbonne, le champ d'application s'élargira aux domaines prévus dans l'ancien « troisième pilier ». Le nouveau cadre légal modernisé n'aura pas seulement une approche plus horizontale et globale, mais les orientations d'ores et déjà annoncées par la Commission européenne s'inscrivent dans le souci d'une plus grande efficacité de la protection des citoyens qui devraient également être mieux en mesure de faire valoir leurs droits comme usagers d'Internet. Ces modifications auront sans doute une influence importante sur le rôle et les attributions des autorités de surveillance indépendantes.

***

Luxembourg, le 31 mai 2011

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

2 Les activités en 2010

Plusieurs domaines d'activités ont marqué le travail de la Commission nationale au courant de l'année 2010 :

- Le conseil et la guidance des 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

Lors de 56 réunions avec les acteurs du secteur public (contre 54 l'année précédente) et 54 avec ceux du secteur privé (contre 52 l'année précédente), la Commission nationale a poursuivi sa politique de conseil et de guidance au sujet de l'application des principes de la protection des données.

En 2010, elle était en relation avec les ministères, administrations et organes publics suivants :

- Ministère de la Santé : mise en œuvre du plan national « e-Santé » ;
- Ministère de l'Éducation nationale et de la Formation professionnelle : service « e-Restauration » (restauration scolaire-Restopolis) ;
- Ministère de la Justice : mise en œuvre de la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale ;
- Ministère des Classes Moyennes : droit d'établissement ;
- Direction de l'aviation civile : données médicales des pilotes et contrôleurs aériens ;
- Inspection générale de la sécurité sociale (IGSS) et Haut-commissariat à la protection nationale : traitement de données personnelles dans le cadre de leurs missions légales ;
- STATEC : préparation du recensement général de la population, avis sur le texte du questionnaire et le règlement grand-ducal afférent ;
- Département des Transports (Ministère du Développement durable et des Infrastructures) : volet « protection des données » dans le cadre de la mise en place de radars automatiques sur le réseau routier national ;
- Service des médias et des communications : cloud computing, transfert international de données et e-commerce ;
- Centre des Technologies de l'Information de l'État (CTIE) et Ministère de l'Intérieur : identifiant unique.

En ce qui concerne la recherche dans le domaine de la santé, la Commission nationale a collaboré avec le CRP-Santé et la biobanque de Luxembourg (IBBL : « Integrated BioBank of Luxembourg ») et a participé aux activités du Comité National d'Éthique de Recherche (CNER). Celui-ci a pour rôle essentiel de protéger les personnes participant à un projet de recherche (essai d'un nouveau médicament, d'une nouvelle technique médicale, recherche académique etc.). Les projets de recherche clinique doivent en général obtenir une autorisation préalable de la Commission nationale.

La Commission nationale a notamment rencontré le STATEC, le Cefis (Centre d'études et de formation interculturelles et sociales / anciennement Sesopi), le Ceps-Instead, l'Université du Luxembourg, l'OLAI (Office Luxembourgeois de l'Accueil et de l'Intégration / Ministère de la Famille) et le Ministère de la Santé au sujet de statistiques et études dans les domaines social et familial.

Un échange de vues a eu lieu sur les problèmes soulevés par le développement du cloud computing avec des acteurs du secteur des technologies de l'information comme les « data centers », Eurocloud Luxembourg et l'APSFS (Association des PSF de support affiliée

à la Fedil). L'objectif commun consiste à clarifier les conditions qui doivent être réunies pour qu'une telle architecture puisse être reconnue comme respectueuse des exigences légales en matière de protection des données. L'essor des « data centers » et du secteur des prestations IT au Grand-Duché va de pair avec la recherche de l'excellence et de la minimisation des risques de failles de sécurité susceptibles d'entacher la bonne image du secteur et d'ébranler la confiance des clients.

Il y a aussi eu des contacts avec l'Entente des Hôpitaux (CHL, Rehazenter, etc.), l'ILR et le CRP Henri Tudor. Des entrevues et concertations sur les pratiques touchant au droit de la protection des données ont eu lieu avec les Centres pénitentiaires de Schrassig et de Givenich.

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

Parmi les acteurs du secteur financier avec lesquels la Commission nationale était en relation, nous pouvons citer l'ABBL (Association des Banques et Banquiers, Luxembourg), la CSSF (Commission de Surveillance du Secteur Financier) et l'ACA (l'Association des Compagnies d'Assurances).

La Commission nationale a également eu de nombreuses entrevues avec des entreprises luxembourgeoises et internationales implantées au Luxembourg. Des réunions de travail ont eu lieu avec des entreprises internationales offrant des services en ligne comme Google, Skype, eBay et iTunes (Apple).

2.1.2 Demandes de renseignements

Le nombre des demandes de renseignements est resté stable à un niveau élevé avec 1618 requêtes en 2010 contre 1711 l'année précédente. Parmi ces demandes, 1405 ont été faites par téléphone.

Environ la moitié des demandes émanent d'entreprises actives dans le secteur privé. Les autres requêtes proviennent d'administrations publiques (18%), de professions libérales (14%) et de citoyens (16%).

Dans la plupart des cas, il s'agit de questions relatives à l'interprétation d'une disposition spécifique, à son application dans une hypothèse donnée ou de précisions relatives aux formalités à accomplir auprès de la Commission nationale.

Les sujets récurrents portent, entre autres, sur les conditions de mise en œuvre d'une vidéosurveillance, les circonstances dans lesquelles l'employeur peut surveiller l'usage d'Internet et de la messagerie électronique sur le lieu de travail ainsi que sur l'appréciation de la légitimité de l'accès d'une administration aux données traitées par une autre administration.

2.2 Supervision de l'application de la loi

2.2.1 Formalités préalables

2.2.1.1 Notifications préalables et autorisations

En règle générale, les fichiers et traitements contenant des données à caractère personnel doivent être déclarés auprès de la Commission nationale afin :

- D'assurer à l'autorité compétente une vision des réalités sur le terrain ;
- De permettre au public, dans l'intérêt d'une meilleure transparence, de consulter la liste des traitements déclarés dans le registre public à l'adresse *www.cnpd.public.lu/registre/application/index.html.*

Certains traitements courants et anodins sont dispensés de déclaration préalable (régime des exemptions). D'autres traitements, les plus sensibles en termes de protection des données, doivent, en revanche, être autorisés avant leur mise en œuvre. Les traitements en question sont expressément et limitativement énumérés par la loi modifiée du 2 août 2002 sur la protection des données.

Le nombre des formalités accomplies est resté plus ou moins constant par rapport à l'année passée (1.009 en 2010 contre 1.184 en 2009). En 2010, le nombre de notifications a diminué légèrement (295 contre 345 en 2009) tandis que les demandes d'autorisation sont passées de 542 à 607.

Presque la moitié des notifications préalables provient d'organismes du secteur financier et un tiers émane d'entreprises commerciales et industrielles. Les ressources humaines et la gestion du personnel sont la finalité principale (plus d'un tiers des notifications) pour laquelle les entreprises envoient des notifications à la Commission nationale.

Quant aux autorisations préalables, la majorité des demandes provient d'acteurs issus des secteurs privé et public, souhaitant installer des systèmes de vidéosurveillance. Depuis 2003, la Commission nationale a reçu plus de 2.300 demandes d'autorisation en matière de vidéosurveillance. Dans le cadre de la vidéosurveillance, plus d'un quart des caméras est localisé dans l'enceinte de bâtiments et locaux commerciaux et administratifs et 20 % se trouvent dans les stations-service. Le nombre de demandes de vidéosurveillance reçues demeure à un niveau élevé, même s'il a diminué légèrement par rapport à l'année 2009.

En revanche, le nombre de demandes concernant la surveillance des conversations téléphoniques et de l'utilisation de l'outil informatique a augmenté. La Commission nationale a également observé une hausse en ce qui concerne la surveillance des trajets de service (géolocalisation de véhicules en service et d'autobus) et le contrôle électronique ou biométrique des accès.

Le nombre total des traitements de données déclarés à la Commission nationale depuis 2003 s'établit désormais à 16.243 avec 5.110 déclarants/responsables s'étant conformés aux devoirs de déclaration imposés par la loi (contre 4.772 fin 2009).

2.2.1.2 Les chargés de la protection des données

Les modalités de la fonction de chargé de la protection des données sont réglées dans l'article 40 de la loi modifiée du 2 août 2002 ainsi que dans le règlement grand-ducal du 27 novembre 2004.

Le responsable du traitement peut désigner un chargé de la protection des données pour son établissement, entreprise, association ou administration. Ce chargé peut être un salarié du responsable du traitement ou une personne physique ou morale externe. Cette désignation exempte le responsable de l'obligation de notifier ses traitements. Elle ne le dispense cependant pas pour autant d'introduire des demandes d'autorisation préalable. La Commission n'accepte que la désignation de personnes remplissant les qualités visées à l'article 40 de la loi et dont la fonction principale dans l'entreprise/organisation n'engendre pas de conflit d'intérêts avec celle du chargé.

Le chargé de la protection des données est une personne physique ou morale qui a été agréée pour cette fonction par la Commission nationale. L'agrément se fait sous certaines conditions. Il doit justifier à l'égard de la Commission nationale ses efforts de formation continue.

Un chargé est tenu d'assurer, de manière indépendante, l'application des dispositions légales et réglementaires en la matière et de soumettre à la Commission nationale un registre des traitements effectués par le responsable du traitement conformément aux dispositions relatives à la publicité des traitements telles que prévues à l'article 15 de la loi modifiée du 2 août 2002.

Il dispose par ailleurs d'un pouvoir d'investigation aux fins d'assurer la surveillance du respect des dispositions de la législation sur la protection des données par le responsable du traitement. La loi accorde également au chargé un droit d'information auprès du responsable du traitement et, corrélativement, la faculté d'informer le responsable du traitement sur les formalités à accomplir afin de se conformer aux dispositions de la législation sur la protection des données.

Depuis 2005, 43 organisations (entreprises et organismes publics) ont désigné un chargé de la protection des données. En 2010, 10 personnes ont été désignées par un responsable de traitement pour accomplir ce rôle.

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

Une autorisation préalable de la Commission nationale est nécessaire pour pouvoir effectuer un transfert de données du Luxembourg vers un pays tiers n'assurant pas un niveau de protection adéquat si le responsable de traitement ne peut invoquer une des dérogations légales (consentement de la personne concernée, nécessité pour l'exécution d'un contrat conclu dans

l'intérêt de la personne concernée, intérêt public important…) prévues à l'article 19 (1) de la loi modifiée du 2 août 2002.

Tous les pays de l'Espace économique européen (l'Union européenne, l'Islande, le Liechtenstein et la 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 des personnes concernées.

Si des données sont transférées de cette « sphère de sécurité » européenne vers un pays tiers, le destinataire doit offrir des garanties suffisantes. Ces garanties peuvent notamment résulter de clauses contractuelles appropriées. C'est la Commission européenne qui apprécie le caractère adéquat de la législation d'un pays non-membre de l'Union européenne. Elle a établi une liste publique avec les pays offrant un niveau de protection adéquat. Aux États-Unis, seules les entreprises qui ont volontairement adhéré aux accords « Safe Harbor » peuvent librement recevoir des données personnelles à partir de l'Europe.

En 2010, la Commission nationale a été saisie de 75 demandes d'autorisation pour le transfert de données vers des pays tiers sans protection adéquate. La plupart de ces demandes proviennent d'entreprises du secteur financier. En 2009, seulement 17 demandes avaient été adressées à la CNPD.

2.2.1.4 Approbation de règles d'entreprise contraignantes

Les « règles d'entreprise contraignantes » (en anglais : « Binding Corporate Rules » – BCRs) sont formalisées sous forme de charte (« Corporate Policy » ou code de conduite) qu'un groupe d'entreprises peut adopter et qui porte sur les transferts de données personnelles d'une filiale du groupe se situant au sein de Union européenne vers des pays tiers n'assurant pas un niveau de protection adéquat (dont la législation ne présente pas de garanties équivalentes à la directive européenne). Cette « charte de la protection des données à caractère personnel » doit revêtir un caractère obligatoire et doit être respectée par l'ensemble des entités du groupe ainsi que par leurs salariés.

Les BCRs représentent une alternative intéressante et flexible par rapport aux clauses contractuelles types élaborées par la Commission européenne et constituent des garanties suffisantes exigées par la directive pour exporter des données vers des pays hors Union européenne n'assurant pas un niveau de protection adéquat. En ce sens, elles constituent également une alternative aux accords « Safe Harbour » pour le transfert de données vers les États-Unis.

Les BCRs présentent un certain nombre avantages. Elles sont en conformité avec la Directive 95/46/CE et évitent aux entités d'une multinationale de devoir conclure une multitude de contrats pour chaque type de flux de données et pour chaque entité concernée. De plus, elles permettent d'uniformiser les pratiques relatives à la protection des données personnelles au sein d'un groupe. Rédigées par les entreprises elles-mêmes selon leurs besoins, les BCRs constituent souvent pour les multinationales un moyen plus flexible et adapté à la culture d'entreprise. Ces règles internes reflètent directement l'activité du groupe pour lequel elles ont été élaborées et sont adaptées spécifiquement aux types de données utilisées par un groupe donné. Pour les entreprises, elles représentent un guide interne en matière de gestion des données personnelles. À ceci s'ajoute l'avantage que les BCRs permettent de placer la protection des données au rang des préoccupations éthiques du groupe.

Un collaborateur de la Commission nationale a régulièrement participé aux réunions du sous-groupe « BCR » du Groupe de travail « Article 29 » à Bruxelles. Ces réunions ont permis aux différentes autorités nationales d'échanger leurs expériences et de concrétiser le concept des règles d'entreprise contraignantes. Au niveau national, la Commission nationale s'est vue reconnaître le rôle de chef de file pour la validation des BCRs du groupe eBay en 2009. L'aboutissement efficace de ce dossier s'inscrit favorablement dans la promotion du Luxembourg comme site d'activité pour des entreprises issues du secteur informatique ou actives dans le commerce en ligne.

En 2010, deux entreprises multinationales, ayant leur siège au Luxembourg, ont soumis pour analyse un projet de leur charte BCR à la Commission nationale.

2.2.2 Demandes de vérification de licéité et plaintes

Si une réclamation ou plainte adressée par un citoyen à une administration, entreprise ou association reste sans suite (ou si une telle réclamation s'avère difficile, voire impossible compte tenu des circonstances), la personne concernée peut s'adresser à la Commission nationale, dans le cadre de sa fonction d'autorité de contrôle, pour vérifier la licéité des traitements mis en œuvre.

En 2010, 145 plaintes et demandes de vérification de licéité ont été soumises à la Commission nationale (133 en 2009).

La majorité des plaintes a été déposée par des particuliers ou entreprises s'opposant à une transmission illégale de leurs données personnelles à des tiers ou dénonçant une collecte de données non autorisée.

Plus généralement, la surveillance illicite et l'installation illégale de systèmes de vidéosurveillance sur le lieu de travail ont provoqué un nombre déterminé d'objections de la part des salariés estimant que leur patron n'avait pas le droit de les filmer sans autorisation.

Une autre source de préoccupation constituent les services en ligne. Certains utilisateurs se plaignaient du non-respect de leurs demandes d'effacement ou de droit d'accès et de rectification des données. Dans ces cas, la Commission nationale s'efforce de garantir une coopération rapide et efficace avec les autorités de protection des données européennes lui transmettant des plaintes concernant des entreprises multinationales ayant leur siège au Luxembourg.

Quelques exemples de traitement de plaintes, demandes et questions du public

Collecte de données déloyale

Un jeu concours sur Internet organisé par une chaîne d'opticiens a été signalé à la Commission nationale. L'entreprise proposait une paire de lunettes gratuite en contrepartie de lui procurer 100 adresses e-mail valides, destinées à la prospection commerciale.

La Commission nationale a immédiatement contacté la société en l'informant qu'elle considérait une telle collecte d'adresses e-mails via un jeu concours promettant un gain comme déloyale, parce qu'elle se faisait à l'insu des personnes concernées qui, de ce fait, n'ont ni été informées, ni avaient donné leur consentement. L'utilisation de courriers électroniques à des fins de prospection commerciale n'est possible que si la personne a donné son consentement préalable ou si les coordonnées électroniques sont ceux de clients obtenues directement de leur part dans le cadre d'une vente d'un produit ou d'un service.

De ce fait, la Commission nationale a demandé à ladite société de suspendre immédiatement le jeu concours sur son site Internet, alors qu'elle estimait qu'il y avait violation de la loi modifiée du 2 août 2002. Le jeu en question a finalement été supprimé du site web après la mise en demeure adressée par la Commission nationale.

Réutilisation de données à des fins de prospection syndicale

La Commission nationale a été interpellée par plusieurs personnes qui se demandaient comment certaines organisations syndicales luxembourgeoises avaient pu obtenir leurs données de contact pour leur envoyer du matériel promotionnel avec une proposition d'adhésion alors qu'elles n'avaient jamais pris contact avec ces organisations.

Les plaignants ont eu des difficultés pour faire respecter leur droit d'opposition et pour faire cesser les envois non sollicités malgré plusieurs réclamations.

La Commission nationale a jugé nécessaire de rappeler aux syndicats mis en cause que la loi précitée confère aux personnes concernées le droit de s'opposer, sur demande et gratuitement, au traitement les concernant à des fins de prospection.

Après ces interventions, les organisations concernées ont définitivement supprimé les données des plaignants de leurs fichiers et ont accepté de fournir à l'avenir une réponse plus rapide aux personnes qui exercent leur droit d'accès ou d'opposition.

Transfert de données

À plusieurs reprises des concessionnaires automobiles luxembourgeois se sont demandé dans quelle mesure ils pourraient être obligés de fournir les fichiers de leurs

clients à leurs grossistes se trouvant à l'étranger. En effet, si les fournisseurs recevaient déjà communication des coordonnées des acquéreurs de véhicules, ceux-ci souhaitaient recevoir en plus les données concernant l'entretien, le service après-vente, la rentabilité et la satisfaction des clients.

La CNPD a estimé dans ce cas que la communication de ces données à caractère personnel concernant les clients des concessionnaires aux importateurs n'était légitime et loyal au sens de la loi modifiée du 2 août 2002 que si :

- le traitement mis en œuvre par les importateurs reste compatible avec les finalités pour lesquelles les données des clients sont collectées par les concessionnaires et que ces données ne soient pas utilisées à des fins autres par les importateurs ;
- seules les données nécessaires et non excessives à l'égard de la finalité du traitement envisagé sont transférées aux importateurs.

Ainsi, la Commission nationale a considéré que les concessionnaires pouvaient légitimement transmettre à leurs importateurs, pour des finalités de marketing ou d'enquêtes de satisfaction, les coordonnées des clients, les données relatives aux ventes de véhicules ainsi qu'aux prestations fournies dans le cadre de la garantie couvrant la voiture tout en notant que le client devait garder la possibilité de s'y opposer en vertu de l'article 30 de la loi modifiée du 2 août 2002. Par contre, les données relatives aux services d'entretien ou à d'autres prestations fournies (réparations, montage d'accessoires, etc.) ne devraient pas être communiquées aux importateurs, celles-ci apparaissant ou bien comme disproportionnées ou dépassant le cadre de la finalité initiale (relation contractuelle du concessionnaire avec le client).

2.2.3 Contrôles et investigations

À la suite de plaintes ou de demandes de vérification de licéité, la Commission nationale peut procéder à des investigations pour vérifier le respect des obligations légales. Elle peut recueillir toutes les informations nécessaires à l'accomplissement de sa mission de contrôle. Pour cette raison, elle dispose d'un accès direct aux locaux autres que les locaux d'habitation où a lieu le traitement ainsi qu'aux données faisant l'objet du traitement et procède aux vérifications utiles. Ainsi, elle a effectué plusieurs visites de lieux pour contrôler des systèmes de vidéosurveillance des sites commerciaux ou ceux débordant sur la propriété voisine ou sur la voie publique pour vérifier la licéité des systèmes de vidéosurveillance.

Dans le contexte des controverses suscitées en Europe au sujet de la collecte de données personnelles à travers les réseaux WLAN au moment des prises de vue pour le service « Street View » de Google, la Commission nationale a procédé, assistée par un expert externe, à l'inspection de la voiture Google pour s'assurer que les dispositifs pour la collecte de données WLAN étaient désactivés, respectivement enlevés (cette partie est commentée plus amplement au point 3.5 de ce rapport).

En 2010, la Commission nationale a par ailleurs dû intervenir plusieurs fois lorsque sont apparues des failles de sécurité, notamment pour garantir la confidentialité des données des utilisateurs.

Système de paiement en ligne d'un opérateur de téléphonie mobile

En mars, une faille de sécurité dans le système de consultation des factures en ligne (web-billing) chez un opérateur de téléphonie mobile a été signalée à la Commission nationale.

Une analyse technique approfondie révélait que le système présentait effectivement un niveau de sécurité insuffisant, puisque les modalités de l'authentification des titulaires étaient susceptibles d'être déjouées. Il était possible de passer des fichiers d'un client à l'autre, et ainsi de suite. Non seulement le coût de communication était visible, mais aussi les numéros d'appels composés par les clients apparaissaient en ligne.

Au vu du degré de sensibilité des données (numéros de téléphone, code PIN, etc.), la Commission nationale a envoyé immédiatement une mise en demeure à la société lui demandant de désactiver provisoirement la fonctionnalité en ligne.

Elle a pu constater avec satisfaction que l'opérateur de téléphonie mobile a mis en œuvre en l'espace de quelques heures seulement les mesures nécessaires

pour renforcer la sécurité et garantir qu'aucune donnée ne soit plus dorénavant accessible à des tiers non autorisés.

Messagerie électronique consultable par Internet

La Commission nationale est intervenue après qu'une faille de sécurité dans le système de courriel en ligne d'un des opérateurs et fournisseurs de services Internet lui a été signalée. À nouveau, la sophistication insuffisante des modalités du contrôle d'accès était en cause.

Quelques jours seulement après avoir été rendue attentive à la possibilité de contourner le système d'identification/authentification en place pour obtenir l'accès en consultation aux messages d'un client « webmail », la société a modifié le système de façon à rendre impossible l'accès non autorisé au moyen des subterfuges et manipulations frauduleuses comme celles qui avaient été signalées à la CNPD.

Faille de sécurité chez un exploitant de cinéma

La Commission nationale a été prévenue que le système de réservation en ligne du site d'un exploitant de cinéma présenterait une faille de sécurité potentielle.

Au moyen de manipulations informatiques, il était possible à des tierces personnes d'obtenir un accès non-autorisé à la base de données des clients inscrits sur le site.

La Commission nationale a demandé aux opérateurs du site en question de procéder d'urgence à une révision de l'application défectueuse en question afin de vérifier les risques de sécurité et si nécessaire de rendre impossible un accès non-autorisé aux données personnelles et pour la sécurité et la confidentialité des données des clients/utilisateurs.

L'exploitant a fait procéder à une analyse technique approfondie comportant des tests d'intrusion rigoureux et a fait parvenir à la Commission nationale un rapport détaillé faisant état des améliorations apportées à l'architecture et aux mesures de sécurité.

Site Internet d'une chaîne de supermarchés

La Commission nationale s'est vu signaler qu'il serait possible d'accéder sur le site d'une chaîne de supermarchés à des données relatives aux comptes clients des titulaires de cartes de fidélité.

La société a confirmé avoir fait l'objet d'une attaque au moyen d'un subterfuge, mais a assuré, après vérification, qu'il était impossible que des scripts malveillants puissent rendre accessible la base de données elle-même. Aucune information relative au contenu de la base de données clients n'a pu être obtenue.

2.3 Information du public

2.3.1 Actions de sensibilisation du public

À l'occasion de la « Journée européenne de la protection des données », la Commission nationale a réalisé une campagne de communication dans la presse écrite et sur Internet pour attirer l'attention des citoyens sur l'importance du respect de la vie privée dans la société d'aujourd'hui. Cette campagne a été accompagnée d'un communiqué de presse qui a suscité une série d'articles et d'interviews de son Président.

Cette journée, organisée par le Conseil de l'Europe avec le soutien de la Commission européenne, a été l'occasion d'informer les citoyens du fait que la loi limite la collecte et conservation des renseignements à caractère personnel aux besoins légitimes ou à l'accord des personnes concernées et oblige les responsables de fichiers à assurer la proportionnalité, la sécurité et la confidentialité des données.

Par ailleurs, la Commission nationale a participé à une campagne de sensibilisation sur la sécurité des mots de passe, mise en place par de nombreux partenaires en collaboration avec le Ministère de l'Économie et du Commerce extérieur (service CASES).

L'action intitulée « *Mot de passe usé ? Les mots de passe c'est comme les brosses à dents…* » avait comme objectif de rendre les citoyens attentifs au fait qu'une sécurisation insuffisante de leur matériel informatique et un comportement trop laxiste en matière de protection des données peut avoir des conséquences néfastes.

Tout comme les brosses à dents, il est recommandé de choisir ses mots de passe avec soin, de ne pas les

partager, de les changer régulièrement et surtout de les utiliser. Les caractéristiques d'un bon mot de passe :

- Il comporte au minimum 8 caractères (plus il y en a, mieux c'est) ;
- Il est formé de chiffres, de lettres majuscules, de lettres minuscules et de symboles ;
- Il n'évoque pas un mot du dictionnaire ;
- Il ne repose pas sur une information personnelle ;
- Il est différent pour chaque application, fichier et système utilisé ;
- Il est aléatoire ;
- Il doit être changé souvent, au minimum tous les semestres, selon son utilisation.

Dans le cadre de cette campagne, la Commission nationale a distribué des dépliants de sensibilisation devant ses locaux se trouvant à l'avenue de la Gare à Luxembourg-Ville et a informé les passants intéressés sur l'importance de la protection de leurs données personnelles. Au total, les partenaires impliqués dans l'action ont distribué 45.000 brosses à dents auprès de la population lors de divers événements.

La Commission nationale a également participé à l'élaboration d'une brochure avec des conseils sur la protection des données intitulée « Voici comment sécuriser tes données sur Internet ». Cette brochure a été réalisée dans le cadre du projet BEE SECURE, mis en œuvre par le Service National de la Jeunesse (SNJ) et CASES – Security made in Lëtzebuerg. À destination des jeunes et réalisée en langues allemande et française, cette brochure donne des informations et recommandations aux jeunes sur la manière de sécuriser leurs données sur la Toile.

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

La Commission nationale est régulièrement intervenue dans les médias pour se prononcer sur des sujets relatifs à la protection des données. Ainsi, en 2010, la Commission nationale a été mentionnée 124 fois dans la presse nationale et son Président ou les membres effectifs ont été interviewés 32 fois.

Parmi les thèmes traités par les médias dans le domaine de la protection des données et de la vie privée, citons les suivants : la journée européenne de la protection des données, la rétention des données, la vidéosurveillance dans les lieux publics, Google Street View, le recensement général de la population, le secret bancaire et la réforme des soins de santé.

2.3.3 Outil de communication : le site Internet

Le site web de la Commission nationale a fait peau neuve en 2010 : l'ergonomie, l'accessibilité, la maniabilité et le graphisme ont ainsi été améliorés. Ce vecteur de communication privilégié de la Commission nationale est destiné aussi bien au grand public qu'aux responsables de traitements souhaitant accomplir leurs formalités en ligne.

Le site offre aux citoyens une information de base sur la protection des données et des explications sur l'étendue et les possibilités de mise en œuvre de leurs droits en la matière dans des rubriques spécifiques. L'actualité nationale et internationale est traitée par le biais d'articles et vise à informer les visiteurs du site de manière permanente sur les évolutions en matière de protection des données. Les citoyens intéressés peuvent élargir leurs connaissances en la matière par la consultation des dossiers thématiques.

Le site constitue par ailleurs une plateforme interactive pour l'accomplissement en ligne des formalités prescrites par la loi, la consultation du registre public des traitements (« fichier des fichiers ») et les réactions des citoyens. L'accès aux informations contenues sur le site a été optimisé. Afin de guider les entreprises de la manière la plus claire possible, la Commission nationale y met à disposition des rubriques et formulaires dédiés.

2.3.4 Formations et conférences

La Commission nationale a donné 21 formations et conférences en 2010, contre 23 en 2009. Ces exposés constituent une manière alternative à la presse pour présenter les enjeux de la protection des données à un public plus spécialisé. Elle a effectué des cours de formation au sujet de la protection des données personnelles auprès des élèves du Lycée Technique de Bonnevoie (LTB) et de l'Institut National d'Administration Publique (INAP). Comme les années précédentes,

plusieurs cours ont aussi été donnés à l'École Supérieure du Travail (EST). Elle est encore intervenue dans un séminaire sur la protection des données auprès du Comité fédéral « Industrie » du LCGB avec le thème « La protection des données et de la vie privée au lieu de travail ».

En février 2010, le Président de la Commission nationale, Monsieur Gérard Lommel, a participé à une table-ronde sur le sujet « données de santé accessibles sur un serveur unique », à laquelle ont également participé le CRP-Henri Tudor et Monsieur le Ministre de la Santé, Mars Di Bartolomeo. Lors de cette conférence, organisée par l'AMMD (Association des Médecins et Médecins-Dentistes du Grand-Duché de Luxembourg), la CNPD a eu l'opportunité de présenter les enjeux du point de vue de la protection des données.

Le Président de la Commission nationale est par ailleurs intervenu en tant que paneliste à la table-ronde « Nouvelles normes OCDE en matière d'échange d'informations; premières expériences européennes. » à l'occasion de la conférence « Private Banker 2010 ». Plus de 150 directeurs de banques privées, gérants de fortune et assureurs vie luxembourgeois ont participé à cette journée de débats.

Monsieur Lommel a aussi fait une présentation dans le cadre du cycle de conférences des « Midis de l'Europe » organisé par le Bureau d'information du Parlement européen à Luxembourg, la Représentation de la Commission européenne au Luxembourg, le Mouvement Européen Luxembourg et le Centre européen des consommateurs. Le Président est revenu sur les enjeux de la protection des données au niveau privé et public dans un monde de plus en plus interconnecté et sur le rôle et les activités de la CNPD.

Depuis 2007, la Commission nationale intervient dans le cadre de la formation « Management de la sécurité des systèmes d'information » (MSSI) à l'Université du Luxembourg. L'objectif de cette formation consiste à sensibiliser les responsables de la sécurité des systèmes d'information à la problématique de la protection des données à caractère personnel.

Outre les formations et conférences précitées, il y a lieu de relever l'intervention de la Commission nationale lors de la réunion « Datenschutz/Datensicherheit », organisée par la Deutsche Bank Luxemburg. Le Président de la Commission nationale a répondu aux questions des chargés de la protection des données et d'experts IT de banques allemandes concernant le traitement de données à l'étranger et l'applicabilité de diverses lois et dispositions. Enfin, la Commission nationale a participé à la conférence de presse du STATEC sur le recensement général de la population.

2.3.5 Études et publications

2.3.5.1 Étude de Deloitte Luxembourg sur la sécurité des réseaux WLAN

En liaison avec la Commission nationale, la société Deloitte Luxembourg a effectué une étude analysant la sécurité des accès sans fil dans les villes de Luxembourg et d'Esch-sur-Alzette.

L'étude a révélé que les bornes Wi-Fi, offrant un haut niveau de confort et de mobilité, ne sont pas toujours suffisamment protégées : 37,3% des accès analysés n'étaient ainsi pas assez sécurisés.

Un des objectifs de cette étude était de sensibiliser la population aux risques associés avec l'utilisation des réseaux sans fil. Parmi ces risques, nous pouvons citer les suivants :

- Capture des données de localisation ou d'autres données personnelles sur l'utilisateur du réseau ;
- Accès non détecté et non autorisé à des réseaux privés ou d'entreprise par des utilisateurs externes ;
- Contournement des pare-feu et filtrage des courriers entraînant une perte de protection contre les attaques de virus et de spam ;
- Accès à des fichiers personnels non reconnus et connexions d'utilisateurs au réseau sans fil non détectées, en particulier dans les lieux publics.

Afin de minimiser ces risques, la Commission nationale recommande de sécuriser son réseau sans fil et de se protéger contre des intrusions non désirées en suivant ces conseils:

- « *Désactivez votre point d'accès s'il n'est pas utilisé ;*

- *Sécurisez l'accès à votre réseau sans fil en utilisant un bon mot de passe ;*
- *Utilisez un chiffrement fort pour sécuriser votre point d'accès ;*
- *Évitez l'identification de votre réseau ».*

2.3.5.2 Participation à l'élaboration d'un livre blanc sur le cloud computing

En 2010, IBM Luxembourg a publié un « White Paper » sur la faisabilité de l'exploitation du cloud computing au Luxembourg, en particulier pour le secteur financier.

Le cloud computing consiste à fournir des ressources informatiques à la demande d'une entreprise pour un prix proportionnel à la solution demandée. L'entreprise peut ainsi disposer, à la demande, sur des serveurs distants, de capacités de stockage et de puissance informatique sans bénéficier matériellement de l'infrastructure correspondante.

Dans le cadre de ce White Paper, la CSSF et la CNPD ont été interrogées sur leur vision respective de l'adoption du cloud computing par les entreprises, particulièrement au regard des traitements des données confidentielles.

2.4 Avis et recommandations

La Commission nationale est demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement de données, de même que sur toutes les mesures réglementaires ou administratives émises sur base de la loi modifiée du 2 août 2002.

Elle a émis six avis en 2010 :

- Avis concernant le projet de loi n° 6113 portant modification des articles 5 et 9 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de l'article 67-1 du Code d'instruction criminelle et le projet de règlement grand-ducal déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou de réseaux de communications publics (Délibération n° 85/2010 du 26 avril 2010) ;
- Avis relatif au projet de loi n° 6148 portant modification de : 1. La loi modifiée du 22 juin 2000 concernant l'aide financière de l'État pour études supérieures ; 2. La loi modifiée du 4 décembre 1967 concernant l'impôt sur le revenu ; 3. La loi du 21 décembre 2007 concernant le boni pour enfant ; 4. La loi du 31 octobre 2007 sur le service volontaire des jeunes ; 5. Le Code de la sécurité sociale (Délibération n° 186/2010 du 9 juillet 2010) ;
- Avis concernant l'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 (Délibération n° 238/2010 du 26 juillet 2010) ;
- Avis relatif au projet de loi n° 6172 portant réforme du mariage et de l'adoption et modifiant certaines dispositions légales (Délibération n° 269/2010 du 24 septembre 2010) ;
- Avis relatif au projet de loi n° 6243 portant modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques (Délibération n° 330/2010 du 10 novembre 2010) ;
- Avis relatif au projet de loi n° 6196 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 (Délibération n° 345/2010 du 24 novembre 2010).

Les documents sont intégralement reproduits dans les annexes du présent rapport.

2.5 Participation aux travaux européens

Comme les années précédentes, la Commission nationale a participé en 2010 à différents groupes de travail au niveau européen. Représentée par un ou par plusieurs de ses membres, elle a assisté à plus de 40 réunions de travail sur le plan international, contre 30 en 2009. Ces réunions se démarquent souvent par un niveau élevé de technicité et nécessitent par conséquent

une préparation approfondie et un suivi régulier des matières traitées.

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 autorités nationales européennes en matière de protection des données ainsi que le Contrôleur européen à la protection des données (CEPD). Dans ce cadre, la Commission nationale a participé aux sous-groupes suivants :
  - « Technologies » ;
  - « Règles d'entreprise contraignantes » ;
  - « Data controller, processor and applicable law » ;
  - « Programme et organisation » ;
  - « Future of Privacy » ;
  - « Biometrics and E-government ».
- Du Comité consultatif de la Convention 108 du Conseil de l'Europe (T-PD) ;
- Du « Groupe de Berlin », dédié à la protection des données privées dans le secteur des communications électroniques ;
- Du séminaire européen biannuel d'échanges d'expériences dans le traitement des cas pratiques (« Case Handling Workshop »).

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

De plus, la Commission nationale était représentée aux conférences suivantes sur le plan international :

- 32ème Conférence internationale des commissaires à la protection des données et de la vie privée (Jérusalem) ;
- European Privacy and Data Protection Commissioners' conference (Prague) – « Spring Conference » ;
- Data Retention Conference (Bruxelles) ;
- 4e Conférence des Commissaires à la protection des données personnelles de la Francophonie ;
- Conférence « Privacy & Scientific Research : from Obstruction to Construction » (Bruxelles);
- Conference for the 30th Anniversary of the CRID « An Information Society for All: A Legal Challenge » (Namur).

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

2.5.1.1 Programme de travail 2010-2011

Pour la période 2010-2011, le groupe de travail « Article 29 » s'est fixé comme objectif de préparer des analyses et avis de nature à éclairer la Commission européenne dans l'élaboration du futur cadre juridique global en prenant en compte l'essor des nouvelles technologies, les difficultés liées à la mondialisation et les changements institutionnels engendrés par le Traité de Lisbonne. Parmi les défis technologiques, citons le « cloud computing » (informatique dématérialisée), le profilage (y compris la publicité comportementale en ligne), les moteurs de recherche et le droit à l'oubli, les sites de socialisation ou encore l'évaluation de l'impact de l'identification par radiofréquence (RFID) sur la protection de la vie privée.

Le groupe de travail suggère de préciser et de renforcer le rôle de tous les acteurs dans le domaine de la protection des données: personnes concernées, responsables du traitement des données et autorités chargées de la protection des données. Il veut également assurer la prise en compte du respect de la vie privée dès la conception dans tous les domaines, ce qui peut donner lieu à l'implication de nouveaux acteurs.

2.5.1.2 Avis du groupe « Article 29 »

Au cours de l'exercice 2010, le groupe a émis plusieurs

avis à l'adresse de la Commission européenne et a adopté un certain nombre de documents de travail. Parmi ceux-ci, relevons ci-après les documents les plus importants.

Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant »

La notion de responsable du traitement des données et son interaction avec la notion de sous-traitant des données jouent un rôle central dans l'application de la Directive 95/46/CE. Ces notions déterminent la ou les personnes chargées de faire respecter les règles de protection des données, la manière dont les personnes concernées peuvent exercer leurs droits, le droit national applicable et la compétence des autorités chargées de la protection des données.

Les modes d'organisation différenciés dans les secteurs public et privé, le développement des TIC ainsi que la mondialisation du traitement des données rendent plus complexes les traitements des données à caractère personnel et appellent à préciser ces notions, pour garantir la bonne application et le respect de la directive dans la pratique.

La notion de responsable du traitement est autonome, en ce sens que son interprétation relève principalement de la législation européenne sur la protection des données, et fonctionnelle, car elle vise à attribuer les responsabilités aux personnes qui exercent une influence de fait, et elle repose par conséquent sur une analyse factuelle plutôt que formelle.

La définition énoncée dans la directive s'articule en trois volets : l'aspect individuel (« *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme* ») ; la possibilité d'une responsabilité pluraliste (« *qui seul ou conjointement avec d'autres* ») ; et les éléments essentiels qui permettent de distinguer le responsable du traitement des autres acteurs (« *détermine les finalités et les moyens du traitement de données à caractère personnel* »).

Cet avis analyse également la notion de sous-traitant, dont l'existence dépend d'une décision prise par le responsable du traitement, lequel peut choisir de traiter les données au sein de son organisation ou de déléguer tout ou partie des opérations de traitement à une organisation extérieure. Pour agir en qualité de sous-traitant, il convient, d'une part, d'être une personne morale distincte du responsable du traitement et, d'autre part, de traiter les données à caractère personnel pour le compte de ce dernier.

Le groupe de travail « Article 29 » reconnaît la difficulté d'appliquer les définitions de la directive dans un environnement complexe qui permet d'envisager maints scénarios faisant intervenir des responsables du traitement et des sous-traitants, seuls ou conjointement avec d'autres, avec différents degrés d'autonomie et de responsabilité.

Dans son analyse, il souligne la nécessité d'attribuer les responsabilités de sorte à garantir, comme il se doit, le respect des règles de protection des données dans la pratique. Il estime cependant n'avoir aucune raison de penser que la distinction actuelle entre responsables du traitement et sous-traitants ne serait plus pertinente ni réaliste dans cette perspective.

Par conséquent, le groupe de travail espère que les explications figurant dans son avis, illustrées par des exemples concrets tirés de l'expérience quotidienne des autorités chargées de la protection des données, donneront des indications utiles pour l'interprétation de ces définitions fondamentales de la directive.

Avis 2/2010 sur la publicité comportementale en ligne

La publicité comportementale (« Behavioural advertising ») est basée sur l'observation continue du comportement de l'utilisateur à travers des sites Web multiples. Requêtes dans un moteur de recherche, clics, production de contenu en ligne, visites successives de sites et autres informations concernant l'individu sont analysés pour établir un profil spécifique et lui proposer des publicités qui pourraient l'intéresser.

Nous pouvons citer l'exemple d'un individu consultant la météo sur Internet et s'étonnant d'y trouver, comme par hasard une publicité pour un modèle de voiture dont il rêvait. Et ce même phénomène s'est reproduit sur un autre site. Non, ce n'est pas une coïncidence. Ce ciblage personnalisé des annonces publicitaires est rendu possible par des systèmes de publicité comportementale. Quelques jours ou semaines

avant, il a probablement visité un site consacré à sa voiture favorite ou cliqué sur une annonce publicitaire présentant cette voiture.

Les réseaux de publicité (reliant les annonceurs aux éditeurs de sites Web) placent un « cookie » sur l'ordinateur de l'utilisateur lorsque celui-ci visite pour la première fois un site faisant partie de ce réseau. Dans ce cas, on parle de « third party cookies » parce qu'ils sont placés par une partie tierce différente de l'éditeur du site. Lors d'une prochaine visite sur le même site ou sur un autre site partenaire du réseau, le réseau de publicité reconnaît l'utilisateur grâce au cookie sauvegardé auparavant. Après des visites répétées, le réseau de publicité peut créer un profil spécifique de l'utilisateur sur base de ses actions en ligne (sites visités, interactions, mots clés, publication de contenus, etc.) et utiliser ces informations pour lui proposer des publicités personnalisées.

Depuis quelques années, on observe une montée en puissance de ce type de publicité, soulevant pourtant des questions importantes en matière de vie privée et de protection de données personnelles. À ce jour, l'internaute ne se voit pas expliquer le but et le fonctionnement exact des cookies que les différents sites se proposent de placer sur un ordinateur « pour lui assurer un service adapté à ses préférences ». Cette information devrait leur être fournie par les exploitants de chaque site qui en fait usage. En pratique, il se voit obligé de site en site à autoriser les cookies de tous les sites sans en connaître l'utilité et les tenants et aboutissants. C'est pourquoi la grande majorité des utilisateurs s'est résolue à régler les paramètres par défaut de leur navigateur de façon à accepter les cookies pour ne pas être pénalisés par des avertissements répétés sollicitant leur acceptation à tout bout de champ, rendant la navigation difficile et les sites infonctionnels.

Actuellement, trois des quatre navigateurs dominant le marché acceptent par défaut tous les cookies. Selon le groupe, le fait que l'utilisateur ne change pas les paramètres par défaut ne peut pas être considéré comme un consentement valide. L'internaute n'est souvent même pas conscient de cette possibilité d'« opt-out » et ne comprend pas comment les données utilisées par les régies publicitaires sont collectées et utilisées.

De ce fait, le document rappelle aux réseaux publicitaires utilisant des « cookies » qu'ils doivent adapter leurs pratiques aux nouvelles règles européennes sur la vie privée en ligne. La directive « ePrivacy » a introduit l'obligation pour les régies publicitaires d'obtenir le consentement préalable actif (principe d'« opt-in ») des utilisateurs avant d'installer des cookies sur leur ordinateur ou de les accéder. Le groupe « Article 29 » demande aux réseaux publicitaires et aux fournisseurs de navigateurs de développer et d'implémenter des mécanismes simples et effectifs pour recueillir le consentement actif à la publicité comportementale en ligne.

Avis 3/2010 sur le principe de la responsabilité

Le document formule une articulation concrète du principe de responsabilité appliqué à l'entité qui est reconnue déterminante dans la mise en œuvre des traitements de données. Il passe en revue les mesures dont celle-ci doit justifier s'être acquitté pour garantir le respect des obligations définies dans la Directive 95/46/CE, et qu'elle doit prouver aux autorités qui le demandent dans le cadre de leur mission de supervision.

L'avis examine en particulier l'hypothèse des groupes d'entreprises ou d'organisations dont les activités de partenariats et de sous-traitance les appellent à échanger et partager régulièrement des données. Il analyse finalement l'impact d'une démarche d' « accountability » sur les règles relatives aux flux internationaux de données, les exigences en matière de notification, les sanctions et envisage enfin l'élaboration de programmes de certification ou de labels.

Avis 4/2010 sur le code de conduite européen de la FEDMA relatif à l'exploitation de données à caractère personnel dans le cadre d'opérations de marketing direct

En juin 2003, le groupe de travail a adopté un avis sur le code de conduite européen de la FEDMA relatif à l'exploitation de données à caractère personnel dans le cadre d'opérations de marketing direct. Toutefois, ce code ne permettait pas de résoudre l'ensemble des problèmes spécifiques aux activités en ligne. De ce fait, le groupe de travail a invité la FEDMA à élaborer une annexe traitant ces questions.

À la suite de nombreuses réunions communes, la FEDMA a envoyé une version définitive de l'annexe relative au marketing en ligne, qui est à présent conforme aux directives 95/46/CE et 2002/58/CE actuellement applicables, ainsi qu'à la législation nationale en vigueur. Cette annexe traite de nombreux aspects importants du secteur en ligne (par exemple, les campagnes de recrutement de nouveaux membres par des membres existants, la protection des enfants et la possibilité de se désabonner) et apporte dès lors une valeur ajoutée aux directives en proposant des solutions claires aux questions qui se posent dans le secteur du marketing en ligne.

Avis 5/2010 sur la proposition 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)

Selon la recommandation de la Commission européenne sur la mise en œuvre des principes de respect de la vie privée et de la protection des données dans les applications reposant sur l'identification par radiofréquence, les États membres doivent veiller à ce que les exploitants d'applications RFID réalisent une évaluation des incidences sur la protection de la vie privée et des données (EIP) des applications RFID avant leur mise en œuvre. Les États membres doivent également veiller à ce que les opérateurs d'applications RFID mettent les rapports d'évaluation ainsi établis à la disposition de l'autorité compétente. Le 31 mars 2010, les représentants du secteur ont remis leur proposition au groupe « Article 29 » en vue de son approbation.

Compte tenu de l'absence d'une méthode claire et exhaustive d'évaluation des risques, le groupe de travail n'a pas approuvé le document proposé sous sa forme actuelle. Il convient de souligner que l'inclusion d'une procédure appropriée d'évaluation des risques est de nature à faciliter sensiblement la prise en compte de la plupart des autres problèmes relevés dans cet avis. Ainsi, l'obligation pour un exploitant d'application RFID de réaliser une évaluation des risques lui permettrait notamment d'inventorier les risques liés au suivi non autorisé d'étiquettes RFID portées par des personnes. De plus, dans le secteur de la distribution, il pourrait être utile de présenter des arguments solides pour démontrer que certaines des étiquettes RFID (utilisées dans une application spécifique) qui restent opérationnelles au-delà du point de vente, ne présentent pas de risque probable pour la vie privée ou la protection des données à caractère personnel.

Début 2011, le groupe « Article 29 » a approuvé la proposition de cadre révisé et la Commission européenne a signé un accord avec l'industrie pour protéger la vie privée des consommateurs lors de l'usage de puces RFID au sein de l'Union européenne. En vertu de l'accord (« Privacy and Data Protection Impact Assessment Framework for RFID Applications »), les entreprises effectueront une évaluation complète des risques et prendront les mesures nécessaires pour déterminer les risques décelés 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, qui peut être appliqué dans tous les secteurs industriels qui utilisent des puces, a été établi.

Avis 7/2010 sur la communication de la Commission européenne relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers

Les autorités de protection des données européennes restent critiques quant à la volonté de la Commission européenne d'échanger les données des dossiers passagers (ou *PNR:* « Passenger Name Records ») avec des pays hors Union européenne.

En réaction à la communication de la Commission européenne de septembre 2010, le groupe de travail a exprimé dans son avis qu'il n'est pas convaincu de la nécessité de collecter un grand nombre de données à caractère personnel relatives aux passagers aériens entrant ou sortant de l'UE. Selon le groupe « Article 29 », il n'existe aucune preuve ou statistique objective démontrant clairement la valeur des données PNR dans le cadre de la lutte contre le terrorisme au plan international et les formes graves de criminalité transnationale. De ce fait, il est impossible d'évaluer clairement la nécessité ou la proportionnalité de l'utilisation des données PNR à des fins répressives. En outre, la partie dans la communication de la Commission européenne concernant le transfert de données à des pays hors Union européenne devrait être améliorée.

Avis 8/2010 sur le droit applicable

Le groupe de travail a analysé dans ce document de travail les critères de rattachement pour la détermination du droit national applicable conformément à la Directive 95/46/CE. L'article 4 de la directive européenne sur la protection des données détermine quelle(s) loi(s) nationale(s) peu(ven)t s'appliquer aux traitements de données à caractère personnel. Selon le groupe de travail, les dispositions de la directive ne sont pas faciles à comprendre et à implémenter. Le point de départ pour déterminer le droit applicable est le lieu où le responsable de traitement a son établissement.

La complexité des questions liées au droit applicable s'accentue aussi en raison de la globalisation et du développement des nouvelles technologies. Les entreprises offrant des services permanents (24 heures sur 24) sont souvent actives dans plusieurs pays. À l'ère d'Internet et du numérique, il est devenu beaucoup plus facile de proposer des services à distance à ses clients et de collecter et partager des données dans un environnement virtuel. Avec le cloud computing, il est difficile de déterminer la localisation des données et de l'équipement utilisé (et par conséquent le droit applicable).

Délimiter l'application du droit de l'UE aux traitements de données à caractère personnel permet de clarifier le champ d'application de la législation européenne sur la protection des données, tant dans l'UE (et dans l'EEE) que dans un contexte international plus large. Une bonne compréhension du droit applicable contribuera à garantir simultanément la sécurité juridique pour les responsables du traitement et un cadre clair pour les personnes concernées et les autres parties prenantes.

Le groupe « Article 29 » propose une analyse des éléments clés dont on doit tenir compte pour déterminer le droit applicable et illustre les différentes hypothèses qui peuvent se présenter dans son avis avec de nombreux exemples. Le groupe s'est interrogé aussi sur les éventuelles améliorations à apporter dans le contexte de la révision de la Directive 95/46/CE : l'avis suggère notamment qu'il serait utile de clarifier le libellé de la directive et d'améliorer la cohérence entre les différentes parties de l'article 4.

Voici un exemple pour illustrer la problématique du droit applicable :

- Lorsque des données à caractère personnel sont traitées par une entreprise dont l'unique établissement est situé au Luxembourg, c'est le droit national luxembourgeois qui s'applique à ses traitements, indépendamment du lieu où ils sont effectués.

- Cependant, la détermination du droit applicable devient plus difficile si une même entreprise est établie sur le territoire de plusieurs États membres. Si un citoyen luxembourgeois reçoit une carte de fidélité dans un magasin à Luxembourg-Ville faisant partie d'une chaîne italienne, ses données sont collectées par le magasin au Luxembourg et la loi luxembourgeoise s'applique. Toutefois, si la maison-mère de la chaîne en Italie utilise ces données pour offrir au même client luxembourgeois des promotions par le biais du marketing direct, la législation italienne s'applique pour cette partie du traitement. Le marketing direct se fait « dans le cadre des activités » de la maison-mère italienne.

Cet exemple est utilisé par le groupe de travail pour montrer que le contexte dans lequel le traitement des données est effectué peut être déterminant pour entraîner l'application du droit national d'un seul Etat membre bien que l'entreprise soit établie sur le territoire de plusieurs Etats membres à la fois. Le lieu et la nature des activités courantes jouent un rôle important pour définir le contexte. Lorsque ce critère n'aboutit pas à distinguer les activités respectives des différents établissements, chacun doit se conformer au droit national de son siège.

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

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

Révision de la Convention sur la protection des données

Le Comité des Ministres du Conseil de l'Europe a adopté une résolution sur « la protection des données et de la vie privée au troisième millénaire ». Celle-ci donne

le feu vert pour une révision de la « Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ». L'année 2011 marquera le 30ème anniversaire de la Convention n° 108, ouverte à la signature le 28 janvier 1981.

Les ministres ont noté dans leur résolution qu'aujourd'hui les nouvelles technologies permettent l'observation, l'enregistrement et l'analyse de la plupart des activités quotidiennes de manière facile et rapide. Pour certains citoyens, cela peut créer le sentiment d'être surveillés en permanence et avoir un effet sur l'exercice de leurs droits fondamentaux. Pour cette raison, il est important de moderniser cette Convention n°108 afin de garder un cadre fort pour la protection des données et de la vie privée.

Adoption d'une recommandation sur le profilage

Lors de la réunion des 47 États membres du Conseil de l'Europe à Ankara, les ministres de la Justice ont adopté une nouvelle recommandation sur le profilage.

Le profilage est basé sur l'observation du comportement des individus et sur la collecte et l'utilisation de leurs données personnelles. Différents types de données sont concernés, tels que les recherches des internautes, les habitudes d'achat, les activités, le mode de vie et le comportement des consommateurs, les informations concernant l'utilisation du téléphone portable, y compris les données de géolocalisation, ainsi que celles provenant en particulier des réseaux sociaux, des systèmes de vidéosurveillance, des systèmes biométriques et des systèmes d'identification par radiofréquence (RFID). Les données ainsi collectées sont traitées par des logiciels de calculs, de comparaison et de corrélation statistique dans le but de dégager des profils qui peuvent être utilisés de différentes manières. Les nouvelles technologies de l'information et de la communication permettent de réaliser ces opérations à un coût faible et à grande échelle, souvent sans que l'intéressé en ait connaissance.

D'un côté, le profilage peut présenter des avantages à la fois pour l'utilisateur, pour l'économie et pour la société dans son ensemble, notamment en permettant une meilleure segmentation des marchés, en permettant l'analyse du risque ou de la fraude ou en adaptant l'offre à la demande par la fourniture de meilleurs services. De l'autre côté, la création et l'utilisation de profils sont susceptibles de porter gravement atteinte à la dignité de la personne et peuvent avoir pour conséquence de la priver de manière injustifiée de l'accès à certains biens ou services.

Selon le Conseil de l'Europe, la technique de profilage devrait donc toujours être entourée de précautions et de garanties particulières pour permettre une protection effective des droits des personnes concernées. Par exemple, si un réseau publicitaire observe ce que fait un individu sur Internet pour lui proposer des publicités personnalisées, l'internaute doit en être informé préalablement. En outre, il faut éviter que des personnes soient victimes d'une discrimination ou d'une stigmatisation sur la base de profils. Chacun devrait pouvoir contester toute décision prise uniquement en fonction des résultats de profilage.

Cette recommandation est le premier texte international à énoncer des normes minimales de protection de la vie privée dans le cadre du profilage, destinées à être mises en œuvre par le biais de la législation nationale et de l'autorégulation.

2.5.3 Le « Groupe de Berlin »

L' « International Working Group on Data Protection in Telecommunications », plus communément appelé « Groupe de Berlin », a adopté trois documents en 2010 lors de ses réunions biannuelles à Grenade en Espagne et à Berlin. Depuis sa création, le Groupe de Berlin a adopté de nombreux documents de travail visant une meilleure prise en compte de la protection de la vie privée dans les services de télécommunications et dans les médias.

« The Granada Charter of Privacy in a Digital World »

Le groupe de travail a adopté cette charte lors de sa 47ème réunion à Grenade. La charte contient un code de conduite destiné aux utilisateurs, fournisseurs et pouvoirs publics. Ces principes visent à faciliter la libre circulation de l'information tout en respectant la dignité, la protection de la vie privée et la protection des données personnelles des individus.

Document de travail sur l'utilisation du « Deep Packet Inspection » à des fins de marketing

En informatique, le « Deep Packet Inspection » (DPI) est une technologie qui automatise l'analyse du contenu (au-delà de l'en-tête) d'un paquet transmis sur un réseau (paquet IP le plus souvent) de façon à en tirer des statistiques.

L'utilisation de cette technologie, en particulier par les fournisseurs d'accès Internet, peut porter atteinte à la vie privée des internautes. Techniquement, ils ont la possibilité d'accéder à tout le contenu de communication d'un utilisateur donné. Le groupe de travail a émis de fortes réserves pour toute utilisation du DPI autre que le maintien de sécurité des systèmes d'information et des réseaux à l'intérieur d'une organisation. Dans ce contexte, le groupe de travail a demandé aux fournisseurs d'accès Internet de s'abstenir d'utiliser la technologie DPI pour la publicité comportementale en ligne.

Document de travail sur le traitement des données personnelles avec les équipements mobiles

Le développement d'appareils mobiles (Smartphones, ordinateurs portables, PDA, etc.), combiné avec la disponibilité constante des réseaux de communication publics, rend le traitement de données confidentielles dans des environnements non sécurisés de plus en plus facile.

Dans ce document, le « Groupe de Berlin » a énuméré les risques liés à l'utilisation des appareils mobiles et a fait de nombreuses recommandations adressées aux fournisseurs et utilisateurs de ces appareils.

2.5.4 Le séminaire biannuel européen « Case Handling Workshop »

Le séminaire « Case Handling Workshop » est organisé deux fois par an sur invitation à tour de rôle des différentes autorités de contrôle. L'objectif est de réunir les autorités de protection des données pour partager leurs expériences et bonnes pratiques sur des sujets pertinents. En 2010, les séminaires ont eu lieu à Bruxelles (18 et 19 mars) et à Manchester (20 et 21 septembre).

Parmi les sujets traités, il y a lieu de relever les suivants :

- Recherche scientifique ;
- Marketing direct ;
- Transport/Mobilité : géolocalisation, systèmes de paiement électroniques dans les transports publics et sur les autoroutes… ;
- Publicité comportementale en ligne ;
- Protection des données dans le secteur financier ;
- Investigations, contrôles, audits ;
- Surveillance sur le lieu de travail.

3 Les temps forts de 2010

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 Protection des données dans le domaine de la santé

3.1.1 Sensibilisation et guidance

Dans le domaine de la santé et de la recherche médicale, l'enjeu de confiance des patients et du public dans la confidentialité et sécurité des données est d'autant plus important que les données sont hautement sensibles et que l'évolution de l'organisation et le progrès scientifique nécessitent davantage d'échanges et de partages de données par des intervenants successifs et équipes multidisciplinaires. La Commission nationale a donc intensifié la concertation avec les acteurs des secteurs médicaux et de la recherche clinique. Les échanges de vues portaient essentiellement sur l'élaboration et la standardisation des règles de bonne pratique à adopter pour parvenir à une optimisation de la protection des données des patients tout en respectant les contraintes opérationnelles des prestataires de soins et des chercheurs. Si des efforts sont encore à faire, cette approche promet d'être fructueuse car les différents intervenants font preuve d'une grande sensibilité pour la problématique de la protection des données dans leurs activités.

De plus, depuis que le législateur a décidé que les traitements de données de santé ne sont plus, sauf exception, soumis à l'autorisation préalable, la nécessité de promouvoir les bonnes pratiques de protection des données s'est accrue.

Une entrevue avec l'Entente des Hôpitaux Luxembourgeois (EHL), début avril, a permis à la Commission nationale de se faire une idée sur les tenants et aboutissants du projet de création d'un centre informatique sectoriel des hôpitaux et a donné lieu à une intensification de la collaboration entre les deux acteurs. Un calendrier de rencontres a été élaboré et des décisions concrètes ont été prises sur la mise en place de standards communs. Dans le cadre de ces réunions et à travers les groupes de travail spécialisés, la Commission nationale a donné des recommandations à l'EHL et aux directions des principaux établissements hospitaliers au sujet des bonnes pratiques de préservation de la vie privée des patients – ne serait-ce que dans le contexte de l'élaboration d'un projet-pilote. La Commission nationale reconnaît que dans ce secteur d'activités, devenu de plus en plus complexe et multidisciplinaire, l'efficacité des flux d'informations peut présenter une importance essentielle comme dans aucun autre domaine.

Elle s'est employée par ailleurs à convaincre l'EHL de l'intérêt de voir instituer un chargé de la protection au sens de l'article 40 de la loi du 2 août 2002 dans chaque établissement. Cet intermédiaire privilégié de la Commission est tant un spécialiste de la protection des données pouvant fournir des renseignements justes aux établissements qu'un interlocuteur professionnel du secteur qui intègre parfaitement les spécificités et les exigences médicales. L'institutionnalisation des chargés de la protection dans les secteurs médicaux et paramédicaux contribuera utilement à l'uniformisation de standards importants de protection des données.

Sous l'égide de l'EHL et en collaboration avec les responsables des différents établissements, les parties ont convenu d'étudier les bonnes pratiques ayant trait aux différents aspects du fonctionnement quotidien des hôpitaux, par exemple la gestion des accès au dossier électronique du patient, et de travailler à des propositions d'harmonisation des règles observées concernant le stockage et les flux internes de données et les échanges avec des tiers.

3.1.2 L'accessibilité des données, gage d'une meilleure efficacité des soins de santé

Après de longues discussions avec l'organisation représentative des médecins et suite aux amendements gouvernementaux ayant permis de mettre fin à la controverse, la Chambre des Députés a voté le projet de loi portant réforme du système de soins de santé en décembre 2010 (Mémorial A – N°242 – Loi du 17 décembre 2010). L'introduction du « dossier de soins partagé » et de l'échange systématique de données relatives à la santé entre les acteurs du secteur se trouvent parmi les changements majeurs de cette réforme.

L'échange de données dans le cadre du dossier de soins partagé avait déjà été au cœur des débats d'une table-ronde « Vers un serveur unique des résultats d'analyses », organisée par l'AMMD en février 2010 en présence de la CNPD et à laquelle ont également participé le CRP-Henri Tudor et Monsieur le Ministre de la Santé Mars Di Bartolomeo. Lors de son intervention à cette conférence, la Commission nationale a eu l'occasion de présenter les enjeux du point de vue de la protection des données et d'expliquer les risques potentiels pour la vie privée des patients dans une discussion avec des docteurs, des représentants de laboratoires et de cliniques et le Ministère de la Santé.

Un dossier patient électronique consultable et mis à jour en réseau a déjà fait son apparition depuis plusieurs années au sein des établissements hospitaliers. L'introduction d'un dossier similaire mais global rassemblant des renseignements issus d'examens, d'analyses, de soins et de traitements prescrits et prodigués par différentes instances médicales n'en constituera qu'un développement naturel. Il ouvre par ailleurs la perspective d'une amélioration aussi bien qualitative des soins que du rapport coût/efficacité du système de santé publique et de la sécurité sociale.

La communication des prescriptions et la consultation des résultats d'analyses à travers une application en réseau ainsi que l'informatisation du carnet (historique des examens) radiologique représenteront les premières concrétisations du plan « e-Santé » au Luxembourg.

La Commission nationale s'est toujours déclarée ouverte à l'égard d'un recours plus poussé aux technologies de l'information et de la communication dans le secteur de la santé en demandant seulement que l'équilibre entre la protection de la vie privée et les intérêts thérapeutiques, de gestion et de financement des soins reste préservé. Si le système ne doit pas se révéler plus intrusif pour le patient que les méthodes classiques de documentation et de suivi du patient, les risques nouveaux induits par la concentration et l'accessibilité croissante des données de santé diverses avec leur historique doivent être contrebalancés par des règles protectrices, rigoureuses et transparentes mises en œuvre au moyen de mesures techniques et organisationnelles aptes à faire respecter le droit à l'autodétermination du patient sur ses données.

3.1.3 Avis sur le projet de loi n° 6196 (réforme du système de soins)

Le 24 novembre 2010, la Commission nationale s'est prononcée au sujet du projet de loi n° 6196 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 (délibération n° 345/2010). Elle s'est concentrée en particulier sur les différents aspects relatifs au dossier de soins partagé.

Le souci du législateur d'une approche optimale du suivi médical – et notamment de la continuité des soins aux patients – doit nécessairement obtenir l'adhésion et la confiance du public. En effet, en leur donnant les garanties inscrites dans la loi, les patients adhéreront plus aisément à la mise en place et au fonctionnement du dossier de soins partagé. La Commission nationale s'est ainsi attachée à apprécier les implications sur la relation entre le patient et son médecin et des risques d'interception par des tiers. L'avis contient des recommandations visant à intégrer les dispositions relatives à la protection des données, au respect du secret médical et à la prévention des risques d'interception ou d'utilisation abusive du dossier, susceptibles d'exister compte tenu de la concentration d'informations de santé et du nombre important des destinataires potentiels.

Tout d'abord, la Commission nationale notait qu'elle avait été consultée en amont à plusieurs reprises par le Ministère de la Santé au cours de l'élaboration du programme e-Santé et s'est montrée satisfaite que les auteurs du projet de loi aient suivi sa recommandation d'inscrire la création et la mise en place d'un dossier médical partagé dans une loi.

Elle a relevé que le projet de loi définissait avec précision les finalités du dossier de soins partagé, à savoir la sécurité, la continuité des soins, la coordination des soins et une utilisation efficiente des services de santé. Concernant le critère de légitimation, la Commission nationale a considéré que le projet de loi apportait des garanties appropriées suffisantes en matière de protection de la vie privée et des données personnelles.

La question de la responsabilité du traitement

À la lecture des articles du projet de loi, la Commission nationale a constaté que les différentes obligations qui incombent au responsable du traitement étaient réparties entre différents intervenants du dossier de soins partagé (chaque médecin qui consulte le dossier, le médecin qui y inscrit des informations, le médecin référent et l'Agence nationale des informations partagées dans le domaine de la santé).

La Commission nationale a recommandé de préciser clairement dans le texte qui est à considérer comme responsable et pour quel volet et a donné à considérer s'il ne serait pas plus opportun, reprenant la recommandation du groupe « Article 29 », qu'une seule personne soit responsable envers les patients de l'usage correct des demandes d'accès.

Afin de régler la problématique soulevée par la Commission nationale, le Conseil d'État a exigé, sous peine d'opposition formelle, de compléter l'article 60ter par un paragraphe 4 nouveau, libellé comme suit : *« (4) L'Agence constitue le responsable de traitement des données à caractère personnel au sens de l'article 4 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement de données à caractère personnel »*. La commission parlementaire s'est ralliée à ce texte.

Le rôle du patient dans la tenue du dossier

Ensuite, la Commission nationale a examiné le principe de l' « autodétermination du patient » à tous les stades du fonctionnement du dossier médical partagé. Si, comme le projet de loi le prévoit, un dossier électronique est ouvert d'office pour chaque patient, ce dernier peut jouer un rôle actif en choisissant, s'il le souhaite, un médecin référent qui sera chargé légalement de son suivi régulier dans le cadre de la continuation des soins.

Lors de la consultation du dossier, le patient a la possibilité de verrouiller le partage entre professionnels de la santé de toutes ou d'une partie des informations qui le concernent. Ce droit d'opposition (ou opt-out) est une garantie appropriée acceptable au sens de la Directive 95/46/CE. La Commission nationale a regretté que le projet de loi n'ait pas attribué au patient de droit de regard lors de l'inscription des données le concernant et elle a proposé d'attribuer au patient la faculté de ne pas porter à la connaissance de certains praticiens certains groupes d'informations qui le concernent. De plus, la Commission nationale s'était demandé si le patient ne devrait pas aussi avoir également la faculté d'attribuer un accès modulaire des informations qui le concernent selon les médecins appelés à consulter son dossier et selon la nature des informations enregistrées. Ces points ont été réglés par l'ajout de l'amendement numéro 7 de la commission parlementaire intégrant les propositions de la Commission nationale et permettant une granularité des niveaux d'accès aux données de la plateforme tenant non seulement compte de la catégorie du prestataire, mais aussi de la sensibilité attachée par le patient à certaines données de santé.

L'accès au dossier par les professionnels de santé

La concentration de façon quasi-exhaustive des informations relatives au parcours de santé d'un patient dans un dossier électronique global, accessible à travers une plateforme d'échanges nationale, pourrait susciter l'intérêt de tiers tels que, par exemple, l'employeur, les industries pharmaceutiques, les compagnies d'assurances, les autorités répressives, etc. Pourtant, toute relation entre un patient et son médecin doit être placée sous le sceau du principe de confidentialité et du respect du secret médical. La Commission nationale a dès lors suggéré de modifier le projet de loi pour insister sur le caractère secret des informations partagées entre un patient et le prestataire de soins de santé dans le cadre de finalités précises. Cette modification a été reprise par la commission parlementaire dans le texte définitivement adopté.

Selon la Commission nationale, la liste des catégories de personnes pouvant consulter le dossier de soins partagé doit rester limitée et cette liste ne devrait pas être élargie à l'avenir. En outre, le dossier doit être régulièrement mis à jour et ne doit contenir que des données justes et nécessaires. De même, elle a réclamé que soit inscrite dans la loi la mise en place d'un tiers de confiance chargé de veiller à la « pseudonymisation » des données avant leur utilisation à des fins statistiques.

Droit d'information et droit d'accès du patient

L'amendement parlementaire numéro 7 précise que le patient dispose d'un droit d'information sur les accès et les personnes ayant accédé à son dossier de soins partagé. La commission parlementaire a souligné qu'il s'agissait en l'occurrence d'une garantie essentielle supplémentaire pour le patient, qui est, de plus, susceptible de renforcer l'acceptation du système auprès du grand public. La loi assure ainsi au patient d'être informé sur les consultations successives de son dossier. En d'autres termes, la traçabilité des consultations du dossier peut également être une traduction concrète du droit d'information du patient sur l'identité des personnes ayant accédé à son dossier. Cette mesure technique est un outil précieux pour que le patient puisse exercer pleinement son droit d'accès mais aussi pour vérifier *a posteriori* toute consultation du dossier en dehors des hypothèses pour lesquelles il a été institué. Il permet encore d'assurer les praticiens de l'exactitude des informations.

Les mesures de sécurité

La Commission nationale a estimé dans son avis que les patients accepteront plus facilement le nouveau système de dossiers de soins partagés s'ils sont convaincus que les mesures de sécurité assurent la confidentialité, le respect du secret médical et préviennent les éventuels détournements de finalités. Pour cette raison, l'exigence d'un niveau de sécurité particulièrement élevé de la plateforme électronique nationale d'échanges et de partage des données de santé devait, aux yeux de la Commission nationale, être inscrite dans le texte même de la loi. La commission parlementaire a suivi cette recommandation. Les modalités et conditions détaillées pourront toutefois faire l'objet d'un règlement grand-ducal. Lors de l'examen des dispositions de ce règlement grand-ducal, la Commission nationale sera attentive à ce que l'authentification des personnes qui accèdent aux dossiers de soins partagés - tant les patients que les professionnels de santé - soit forte.

La Commission nationale avait d'ailleurs noté dans son avis que l'Agence nationale des informations partagées dans le domaine de la santé était notamment chargée d'une mission technique et administrative pour mettre en place l'architecture technique et organisationnelle du dossier de soins partagé. Elle a donc une responsabilité particulière en matière de sécurité du système. Compte tenu de l'avis du Conseil d'État et de la Commission nationale, la commission parlementaire, après un large échange de vues, a adopté l'amendement numéro 6 ayant pour objet d'informer les patients et prestataires de manière appropriée sur le fonctionnement du système avant l'ouverture d'un dossier de soins partagé. Il conviendra, dans les mesures à préciser ultérieurement dans les dispositions réglementaires, de préciser les modalités de cette information.

3.2 Modification de la loi sur la vie privée dans le secteur des communications électroniques

Les technologies de l'information et de la communication, notamment Internet et les messageries électroniques, requièrent des exigences spécifiques pour garantir le droit au respect de la vie privée.

La Directive 2002/58/CE (directive « vie privée et communications électroniques ») du Parlement européen et du Conseil du 12 juillet 2002 représente le dispositif législatif appelé à encadrer le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques. Cette directive fait partie du « Paquet Télécom » et contient des règles essentielles destinées à assurer la confiance des utilisateurs envers les services et les technologies des communications électroniques.

Le « Paquet Télécom » a été modifié en décembre 2009, notamment par la Directive 2009/136/CE, pour faire face à de nouveaux défis liés au développement rapide de l'Internet. Ceux-ci concernent l'interdiction des « spams », le régime de l'accord préalable de l'utilisateur (« opt-in »), l'installation de « cookies » et la prévention de violations de données à caractère personnel. Grâce à la réforme du secteur des télécommunications dans l'Union européenne, les citoyens européens jouissent désormais d'un choix élargi découlant de l'intensification de la concurrence sur les marchés européens des Télécoms, d'une meilleure couverture en ce qui concerne les connexions Internet à haut débit dans l'ensemble de l'Union européenne et de droits mieux établis quant au respect de la vie privée dans leurs télécommunications.

La Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 a rendu obligatoire pour les États

membres l'introduction de la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications et prévoit un certain nombre de conditions et modalités afférentes (en laissant une marge de transposition substantielle aux législateurs nationaux qui doivent fixer la durée de conservation des données à une période de 6 mois au minimum et 24 mois au maximum). Elle modifie la directive de 2002, qui prévoyait une rétention des données facultative.

La loi du 24 juillet 2010 (projet de loi n°6113) a transposé en droit national la Directive 2006/24/CE. La transposition de la Directive 2009/136/CE est actuellement à l'étude dans le projet de loi n°6243.

3.2.1 La rétention des données

La directive sur la rétention des données (Directive 2006/24/CE) a été transposée en droit national par la loi du 24 juillet 2010. L'objectif de cette directive est de conserver pendant un certain délai les données que traitent les opérateurs de télécommunications et les fournisseurs d'accès à Internet pour les besoins de la recherche, de la détection et de la poursuite d'infractions. Une des difficultés majeures de cette transposition était le maintien de l'équilibre entre, d'une part, l'accès aux données traitées par des fournisseurs de communications électroniques dans le cadre de la lutte contre le terrorisme et la criminalité grave, et d'autre part, la protection de la vie privée des citoyens.

Le bilan 2010 pour le monde de la communication électronique n'avait rien de réjouissant. En effet, les titres des journaux affichaient des dizaines de sites piratés, des données personnelles et bancaires volées et des services en ligne indisponibles.

Non seulement des sites renommés ont été victimes d'attaques comme celui du Fond Monétaire International (FMI), du Gouvernement français où des milliers d'e-mails ont été piratés sur les sites *.gouv.fr*, du RSA, la division sécurité d'EMC, des ordinateurs du Ministère des Finances qui était bien la plus importante attaque jamais enregistrée à l'encontre d'une administration française, mais des groupes de hackers ont également été responsables du vol de données personnelles sur les sites de Sony PlayStation, de Citigroup et bien d'autres.

De plus, les hackers se sont regroupés en cyber-armées comme *LulzSec* ou *Anonymous* par exemple pour lancer en commun des attaques contre les plus grands acteurs du monde.

Pour aller à l'encontre de ces activités criminelles, la directive sur la rétention des données a été conçue par la Commission européenne.

Avis relatif au projet de loi n°6113

La Commission nationale a rendu fin avril 2010 au gouvernement son avis concernant le projet de loi n° 6113 relatif à la rétention des données des communications électroniques portant modification des articles 5 et 9 de la loi du 30 mai 2005 relative à la protection des données dans le secteur des télécommunications et à l'article 67-1 du Code d'instruction criminelle.

Dans sa prise de position, la Commission nationale a noté que la conservation des données des connexions et des données de localisation des téléphones mobiles prévue dans le contexte de la prévention du terrorisme et de la criminalité organisée constitue une atteinte sans précédent au droit au respect de la protection de la vie privée. Les informations qui doivent être retenues par les opérateurs de réseaux accessibles au public et fournisseurs de services de communications électroniques au-delà de la durée nécessaire pour des raisons techniques, opérationnelles et de facturation, sont celles de tout un chacun et sont susceptibles de révéler foule d'informations sur ses contacts sociaux, ses déplacements et sa vie privée. Il est donc d'une importance cruciale qu'une dérogation au principe constitutionnel du secret des correspondances et des communications reste circonscrite dans des limites claires et étroites qui correspondent aux motifs qui sont à la base de la Directive 2006/24/CE qu'il s'agit de transposer dans notre législation nationale, à savoir la lutte contre le terrorisme et la criminalité organisée.

Le principe de proportionnalité visé à l'article 8, paragraphe (2) de la Convention européenne des Droits de l'Homme (l'intrusion de l'État dans la vie privée des citoyens n'est admissible que dans la mesure prévue par la loi et quand cela est nécessaire dans un État démocratique pour les intérêts publics importants, notamment la sécurité publique) commande que le législateur s'impose de la retenue et prudence lorsqu'il introduit des exceptions et limitations aux libertés et droits fondamentaux des individus.

Cela s'applique à la durée obligatoire de la conservation des données des communications électroniques (la CNPD se félicite que le projet de loi maintient la durée de 6 mois telle qu'elle a également été retenue en Allemagne et aux Pays-Bas). Cela s'applique également aux conditions de l'accès aux données conservées par les autorités policières et judiciaires pour les besoins des enquêtes, de l'instruction et de la poursuite des infractions pénales.

À ce sujet, la Commission nationale a demandé que l'accès de la police soit subordonné explicitement à une autorisation judiciaire préalable tel que cela résulte d'ores et déjà de l'application de l'article 67-1 du Code d'instruction criminelle et s'est opposée au maintien de la faculté d'accès de la police sans ordonnance du juge d'instruction dans le cadre de l'enquête de flagrant délit. Elle a estimé qu'il serait ainsi assuré (comme le demande d'ailleurs le groupe « Article 29 ») que les données conservées ne pourront pas servir à des recherches généralisées à grande échelle de type « Rasterfahndung » et qu'il sera évité que la population n'ait un sentiment diffus d'une surveillance à son insu à travers ses données de connexion et de localisation tenues à la libre disposition de la police. Il est à noter que la Commission Consultative des Droits de l'Homme s'est exprimée dans le même sens dans son avis du 29 juin 2010.

L'avis a soulevé finalement l'importance des exigences en termes de mesures de sécurité à mettre en œuvre pour cette conservation massive de données relatives à tous les citoyens en vue d'empêcher des atteintes illégitimes aux données à caractère personnel et de prévenir des abus.

Loi du 24 juillet 2010

Le projet de loi n°6113 est devenu la loi du 24 juillet 2010. Celle-ci apporte quelques changements à la législation antérieure.

Un des changements les plus remarquables est la délimitation des infractions pénales visées. La loi du 24 juillet prévoit que les données retenues ne peuvent être utilisées que pour la poursuite d'infractions pénales qui comportent une peine correctionnelle dont le maximum est supérieur ou égal à un an d'emprisonnement. Auparavant, la loi du 30 mai 2005 ne donnait pas de précisions à ce sujet. L'établissement par le législateur d'une liste d'infractions aurait été préférable aux yeux de la Commission nationale. De plus, elle considère que le seuil retenu n'est pas assez élevé compte tenu du nombre très important d'infractions concernées. Un seuil de deux ans au moins aurait plus correspondu aux motifs de la directive. Il est à noter que certains pays ont choisi un seuil de peine de cinq ans.

Des nouvelles garanties ont été introduites par la loi du 24 juillet 2010. Ainsi, l'article 5-1 dispose que « *(1) Les données conservées au titre des articles 5 et 9 sont soumises aux exigences prévues aux articles 22 et 23 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. (2) Les données sont détruites lorsque la durée de conservation prend fin, à l'exception des données auxquelles on a pu légalement accéder et qui ont été préservées* ». Une autre garantie apportée par la loi énoncée dans l'article 5-2 qui précise que la Commission nationale transmet annuellement à la Commission de l'Union européenne des statistiques sur la conservation des données au titre des articles 5 et 9. À cet effet, les fournisseurs de services ou opérateurs conservent et transmettent à la Commission nationale, sur demande de celle-ci, les informations comprenant notamment :

- *« les cas dans lesquels des informations ont été transmises aux autorités compétentes conformément à la législation nationale applicable,*
- *le laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission,*
- *les cas dans lesquels les demandes de données n'ont pu être satisfaites. »*

La Commission nationale se félicite par ailleurs que la possibilité de déléguer les opérations de stockage à un sous-traitant ait été abandonnée par le législateur. L'arrêt de la Cour constitutionnelle fédérale allemande du 2 mars 2011 s'est prononcé également contre un système de ce type où les opérateurs devraient se dessaisir de ces données au profit d'un organe tiers qui les tiendrait à disposition des autorités répressives. Dans

son avis, la Commission nationale avait noté qu'une telle sous-traitance n'était pas prévue par la Directive 2006/24/CE et qu'elle était réservée quant à cette possibilité vu le caractère confidentiel et la quantité des données concernées. Une multiplication des acteurs appelés à gérer les données et d'autres risques (confidentialité des données, transfert des données à l'étranger, abus et détournement de finalités, etc.) ont amené le législateur à ne pas retenir ce point dans le texte final.

Prise de position critique du groupe « Article 29 »

Sur le plan européen, le groupe « Article 29 » a critiqué la manière dont les dispositions de la Directive 2006/24/CE ont été appliquées dans les différents pays membres de l'Union européenne. Les 27 pays membres doivent transposer cette directive en droit national, mais le groupe « Article 29 » est d'avis que ce processus ne se fait pas partout de la même manière et que certaines dispositions nationales disparates vont même à l'encontre du droit communautaire.

Ainsi, le groupe a relevé que certaines lois nationales permettraient une durée de rétention bien supérieure à la période maximale prévue par la directive (24 mois). De plus, la suppression de données « périmées » ne se ferait pas toujours de manière automatique. Le groupe a critiqué encore le fait que l'étendue des données stockées dépasserait souvent le cadre fixé par la directive, par exemple, par le stockage des adresses des sites Internet visités ou des en-têtes de courriers électroniques. En outre, les fournisseurs de service auraient, dans certains cas, rendu accessibles les données stockées à d'autres fins que celles fixées limitativement par la directive et les lois nationales.

En vue de remédier à cette situation, le groupe a mis en avant plusieurs propositions : il a suggéré ainsi par exemple d'harmoniser et de sécuriser davantage les procédures selon lesquelles les données sont rendues accessibles aux autorités ; il a aussi souhaité que la durée générale de rétention des données soit raccourcie. Il a également demandé d'assurer que les dispositions nationales ne dépasseraient pas le cadre fixé par la directive. Finalement, la notion de « criminalité grave » devrait être définie de manière plus précise et restrictive dans les législations nationales.

3.2.2 Transposition de la Directive 2009/136/CE

La Commission nationale a émis son avis sur le projet de loi n°6243 portant modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

L'objet central de ce dernier consiste dans la transposition en droit luxembourgeois de la Directive 2009/136/CE qui fait partie du nouveau « Paquet Télécom » par lequel le droit communautaire a été adapté à l'évolution technologique rapide du secteur qui s'est encore accélérée depuis l'adoption de la précédente directive de 2002. En outre, la directive a voulu consolider l'indépendance des autorités nationales de régulation du secteur des télécommunications et le principe d'un Internet ouvert et neutre tout en renforçant la protection des consommateurs par des garanties nouvelles portant entre autres sur le respect de leur vie privée.

Obligation de signaler les violations de sécurité et de confidentialité

La principale innovation que le projet de loi se propose d'introduire par un ajout à l'article 3 de la loi modifiée du 30 mai 2005 porte sur l'obligation pesant dorénavant sur les fournisseurs de services de communications électroniques accessibles au public d'avertir immédiatement la Commission nationale pour la protection des données 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 de les affecter défavorablement au niveau de la protection de leur vie privée et des données les concernant.

De telles dispositions se proposent en effet d'induire une vigilance accrue de la part des responsables des traitements de données, de promouvoir l'amélioration continue des procédures internes et de favoriser l'investissement dans des ressources techniques visant à assurer la sécurité des données à caractère personnel et à prévenir des accès non autorisés et des pannes susceptibles de ternir l'image de marque de l'entreprise ou de l'organisation en question et de lui faire perdre la confiance de ses utilisateurs et clients. L'introduction de cette obligation constitue donc une avancée majeure

sur le plan de la protection de la vie privée dans le secteur des communications électroniques.

Un rôle important reviendra dorénavant à notre Commission nationale dans la mise en œuvre des nouvelles règles. Dans ce domaine, notre Commission s'efforcera d'allier de façon non bureaucratique mais pragmatique et ouverte au dialogue constructif avec les acteurs concernés, la guidance, le contrôle et la promotion d'une approche vigilante et anticipatrice. Les ressources de la Commission nationale, en particulier au niveau de collaborateurs à compétence informatique et technologique, devront elles aussi évoluer de façon à lui permettre d'assumer convenablement ces nouvelles responsabilités.

Le projet de loi examiné présente encore deux innovations importantes.

Renforcement des garanties de transparence et d'usage loyal des « cookies »

L'une d'entre elles découle directement de la transposition de la directive et a trait aux témoins de connexions sur Internet (généralement appelés « cookies ») et renforce les garanties de transparence et d'usage loyal de ces techniques qui se sont quasi généralisées avec l'évolution d'Internet. Les offres de services en ligne (souvent non payants) utilisent cette méthode pour personnaliser autant que possible la navigation de l'internaute et l'interaction avec lui (y compris le placement de publicités tenant compte de ses intérêts). L'exigence de loyauté et de transparence et la possibilité qui doit lui être offerte d'accepter ou de refuser le recours aux « cookies » s'étend aussi bien au placement sur le terminal de l'usager (stockage d'informations de connexion) qu'à l'accès ultérieur à ces témoins (informations stockées) par le site web d'origine et/ou par d'autres sites partenaires ou similaires.

Le projet de loi reprend fidèlement le texte exact de l'article de la directive et du considérant afférent. Cette démarche apparaît judicieuse et fondée parce qu'elle reprend à son compte l'adage raisonnable de bonne légistique « Toute la directive, rien que la directive », mais aussi parce que des négociations sont actuellement en cours sur le plan communautaire avec les principales entreprises multinationales du secteur sur les pratiques recommandables et les moyens techniques les plus conviviaux et efficaces pour atteindre les objectifs d'information appropriée et de choix laissé au consommateur/usager, formulés par la directive.

Il s'est avéré que les notices compliquées sur les principes suivis en matière de respect de la vie privée (« privacy ») par les opérateurs de sites web et services sur Internet sont souvent trop longues, incompréhensibles et peu accessibles pour contribuer utilement à l'éclairage du choix de l'internaute et qui réagit souvent par impulsion. Peut-être que la liberté de l'internaute de contrôler la collecte et l'usage des informations le concernant devra trouver des façons de s'exprimer plus modernes, simples, intuitives, qui tiennent compte des situations où le visiteur d'un site web et usager de ces services a implicitement mais sans ambiguïté accepté la finalité du traitement de ses données (par opposition à celles où une information plus explicite est nécessaire pour un consentement éclairé).

Le législateur luxembourgeois est donc bien inspiré de reprendre textuellement, comme le prévoit le projet de loi, les termes de la directive et de ne pas gêner la flexibilité évolutive par des dispositions spécifiques originales pour laisser les bonnes pratiques se dégager à travers les initiatives en cours de la Commission européenne et du groupe de travail « Article 29 » afin de amener les principaux représentants du secteur en question à s'adapter aux exigences du droit européen.

Transmission des données d'identification en cas d'appel d'urgence

Finalement, le projet de loi vise à insérer un certain nombre de modifications et d'ajouts aux articles 4, 5 et 7 de la loi modifiée du 30 mai 2005 pour assurer l'accès de la Police et des Centres d'appels d'urgence aux données d'identification et de localisation des appelants et s'est proposé d'abroger l'article 41 de la loi modifiée du 2 août 2002 qui n'a jamais donné lieu à une application effective en raison des difficultés techniques rencontrées par l'ILR dans sa mise en œuvre pratique. Cet article prévoit la mise en place auprès de l'ILR d'une banque de données consolidée des abonnés de tous les réseaux de téléphonie fixe et mobile actualisée une fois par jour.

Il s'est avéré entre-temps que le modèle, qui avait inspiré le législateur de 2002, n'est pratiqué à grande échelle que dans un seul État membre de l'Union européenne. Aussi les rédacteurs du projet de loi ont-ils opté pour remplacer ce système de stockage centralisé des données d'identification et de localisation des abonnés pour les besoins du recours en cas d'urgence par la Police grand-ducale et les services de secours par un système de transmission décentralisé au cas par cas aux opérateurs des numéros d'urgence (112, 113, etc.) des données d'identification et de localisation concernant les appelants.

Les dispositions proposées reflètent les systèmes similaires pratiqués dans la plupart des autres pays européens.

3.3 Protection des données à caractère personnel et secret bancaire

Dans la mouvance des accords du G20 de Washington (de novembre 2008) formalisés lors du sommet de Londres le 2 avril 2009, l'un des points retenus pour refonder le système financier international et favoriser la sortie de crise visait à isoler et combattre les paradis fiscaux qui refusent la coopération avec d'autres États en matière fiscale.

Dans ce contexte, une pression sans précédent était exercée sur tous les pays qui connaissent un secret bancaire absolu de façon à les obliger à faire évaluer leur législation et à accepter de fournir une assistance internationale administrative en matière fiscale.

Il se trouve que d'aucuns ont tendance à assimiler sans nuance toute forme de reconnaissance du droit de l'épargnant à la confidentialité des informations relatives à son patrimoine et à ses comptes et transactions bancaires à un encouragement de l'évasion fiscale et à priver le citoyen de toute protection de sa vie privée dans ce domaine.

Les représentants de la Commission nationale se sont néanmoins employés à défendre dans les enceintes du Conseil de l'Europe, de l'OCDE et des institutions européennes le point de vue selon lequel le droit positif applicable en Europe (la Directive 95/46/CE et la Convention 108 du Conseil de l'Europe) exige que l'État protège aussi la sphère privée patrimoniale du citoyen de façon raisonnable.

À ce sujet, le Président de la Commission nationale, Monsieur Gérard Lommel, est intervenu en tant que paneliste à la table-ronde « Nouvelles normes OCDE en matière d'échange d'informations ; premières expériences européennes » à l'occasion de la conférence « Private Banker 2010 ». Plus de 150 spécialistes et décisionnaires de banques privées, gérants de fortune et assureurs-vie luxembourgeois ont participé à cette journée de débats.

Les pouvoirs d'investigation directe du fisc à l'égard des établissements financiers sont limités par le secret bancaire (« Abgabenordnung » Art. 178 et règlement grand-ducal). Le Luxembourg considérait que ce principe s'oppose aussi à tout échange de renseignements international autre que via l'entraide judiciaire en matière pénale. Suite au sommet du G20 en avril 2009, un assouplissement de la position traditionnelle du Luxembourg s'est imposé.

À la lumière des développements internationaux concernant le renforcement de la coopération internationale en matière fiscale, le Luxembourg a décidé, en date du 13 mars 2009, de se rallier intégralement au standard de l'OCDE en matière d'échanges de renseignements sur demande entre administrations fiscales (article 26, paragraphe 5 du modèle standard de convention fiscale concernant le revenu et la fortune – version 2005). Il importe de relever que, de manière générale, une telle Convention a pour objet, d'une part, l'élimination de la double imposition juridique, à savoir celle résultant du fait, pour un même contribuable, d'être imposé au titre d'un même revenu ou d'une même fortune par plus d'un État, et d'autre part, de prévenir la fraude fiscale. Aussi légitime et nécessaire que la lutte contre la fraude fiscale soit, elle ne doit pas priver complètement de protection la grande majorité de la population qui n'a rien à se reprocher.

Avec cette décision, le gouvernement a toutefois exclu clairement la voie de l'échange automatisé généralisé et choisi de se limiter à l'assistance administrative mutuelle par l'échange de renseignements sur demande qui présuppose la « pertinence vraisemblable » des données

à communiquer à l'État requérant et exclut aussi la possibilité « d'aller à la pêche aux renseignements » ou de demander des renseignements dont il est peu probable qu'ils soient pertinents pour élucider les affaires fiscales d'un contribuable.

Dans son avis relatif au projet de loi n°6072 (Délibération 410/2009 du 20 novembre 2009), la Commission nationale a reconnu qu'une telle pratique restait compatible avec le respect des principes de finalité et de proportionnalité inscrits dans la Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 et à l'article 8 de la Charte des droits fondamentaux de l'Union européenne.

Il ne suffit donc pas, pour l'autorité de l'État requérant, de fournir simplement des éléments généraux destinés à orienter les autorités de l'État requis vers un cercle de personnes plus ou moins large ou plus ou moins restreint. Au contraire, l'État requérant doit bien fournir un certain nombre d'indications précises quant à la dénomination, aux coordonnées ou au nom de la personne qui, d'après cette même autorité de l'État requérant, est ou devrait être en possession des renseignements demandés, sans que des noms ou dénominations incomplètes, l'absence d'adresse ou de numéro de registre de commerce ou des approximations ou des inexactitudes de forme dans la dénomination, les coordonnées ou le nom, ne puissent constituer un obstacle à l'exécution de la demande.

Par ailleurs, la demande n'est possible pour des cas précis et spécifiques, sous condition que l'État requérant ait épuisé au préalable les sources habituelles de renseignements prévues par la procédure interne. L'État requérant doit justifier et prouver à suffisance de droit à l'État requis qu'il s'est assuré au préalable que les renseignements demandés ne puissent pas être obtenus par d'autres moyens que celui de l'échange de renseignements prévu par la convention. Les renseignements, une fois collectés, ne peuvent être utilisés qu'à la seule et unique fin de répondre à la demande de renseignements étrangère. Le secret bancaire est ainsi préservé en régime interne, mais se trouve assoupli pour la coopération administrative internationale encore que celle-ci permet seulement la demande ponctuelle de renseignements en cas d'indices suffisants.

Ainsi, l'échange d'informations entre autorités fiscales des différents pays doit être limité au cas par cas et à des hypothèses dans lesquelles il y a des éléments objectifs et indices concrets qui le justifient. La pêche aux informations est contraire aux principe de proportionnalité du droit à la protection des données et le modèle de l'échange automatisé et généralisé des données des clients transnationaux des institutions financières a pour effet de discriminer les places financières des petits pays, le marché unique et la libre prestation de service transnationale au sein de l'Espace économique européen. « *Der gläserne Sparer* » est un spectre inconciliable avec le principe de la protection des données solidement ancré dans l'acquis communautaire et les droits fondamentaux des citoyens de l'Union européenne. Les entorses et exceptions à ces principes doivent rester l'exception et s'appliquent de façon restrictive et spécifique en tenant compte des principes de nécessité/proportionnalité ancrés dans l'article 8, paragraphe (2) de la Convention européenne des Droits de l'Homme.

Le Bureau du Comité Consultatif de la Convention 108 du Conseil de l'Europe (T-PD) auquel appartient le Président de la CNPD, s'est employé à faire reconnaître également ces principes lors de la révision de l'article 22 de la Convention concernant l'assistance administrative mutuelle en matière fiscale (STCE N°127) qui a été négociée au sein de l'OCDE et du Conseil de l'Europe.

Il a pour le moins obtenu que le nouveau texte ne privilégie plus l'assistance fournie sous forme d'échange automatisé par rapport à celle limitée au cas par cas sur demande motivée qui est pratiquée par les États les plus soucieux de préserver la protection de la vie privée des épargnants.

S'il est vrai que la nouvelle convention (commune à l'OCDE et au Conseil de l'Europe) n'exige plus que l'État requérant devra se conformer entièrement aux règles de l'État requis qui lui fournit des données à caractère personnel (une de ces règles pouvant être le secret bancaire), il doit cependant accepter toutes les limitations qui résultent des exigences, découlant de son droit national en matière de protection des données (par exemple les limitations relatives aux finalités d'utilisation, de divulgation et de transmission à des tiers), lui communiquées par l'État requis s'il étend prévaloir cette stipulation.

3.4 L'affaire « Google Street View »

« Google Street View » est une application en ligne permettant de se déplacer virtuellement dans certaines grandes villes du monde grâce à des images fixes prises sur 360 degrés par un véhicule spécialement équipé. Ce service controversé de navigation virtuelle a suscité une vive polémique depuis sa création et a valu à Google des critiques dans plusieurs pays, particulièrement concernant la protection de la vie privée.

Au Luxembourg, la Commission nationale s'était vue obligée de suspendre les prises d'images pour le service « Street View » en mai 2009 : à défaut d'avoir obtenu toutes les assurances quant au respect de certaines conditions qui faisaient l'objet des discussions avec Google depuis 2008 (annonce publique préalable des périodes de prises de vues ; floutage des personnes et plaques d'immatriculation ; respect du droit d'opposition ; abstention de toute commercialisation ultérieure ou transmission à des tiers des images ; garanties relatives à la sécurité des données préalablement à la mise en ligne). Après avoir rempli les requis de notification en août 2009, Google a repris l'enregistrement d'images dans sept communes luxembourgeoises (pour plus de détails concernant l'affaire « Street View » en 2009, se reporter au point 3.2. du rapport annuel 2009).

Avertissement à Google au sujet de la collecte de données Wi-Fi lors des prises de vues pour « Street View » en 2009

Après une enquête technique de l'autorité de protection des données de Hambourg en mai 2010, la société américaine a dû reconnaître avoir collecté « par inadvertance » des données personnelles en scannant les réseaux Wi-Fi non protégés. Google a expliqué avoir inclus sans le savoir un code informatique expérimental dans le dispositif d'exploitation de ses voitures de collecte de données pour « Street View ». Cette annonce a déclenché l'ouverture d'investigations par les autorités de protection des données ou même par la police dans de nombreux pays. Cela a amené Google à suspendre temporairement ses activités en Europe. L'entreprise américaine a ensuite proposé de détruire les données personnelles collectées ou de les transmettre aux autorités nationales si ces dernières l'exigeaient.

En France, la CNIL (Commission Nationale de l'Informatique et des Libertés) a notamment demandé à Google de lui communiquer l'ensemble des données recueillies sur le territoire national par les véhicules « Street View », à partir des bornes Wi-Fi. Lors de son investigation, l'autorité de contrôle a découvert que Google a bien enregistré des mots de passe d'accès à des boîtes mail et des extraits de contenus de messages électroniques, à l'insu des personnes. Pour cette raison, la CNIL a même condamné Google à verser une amende de 100.000 euros en mars 2011.

N'ayant pas à sa disposition les mêmes moyens techniques que les autorités de contrôle d'autres pays pour analyser les enregistrements de données captées au Luxembourg à l'occasion des campagnes de prises de vues, la Commission nationale a demandé à Google de détruire les données Wi-Fi concernant le Grand-Duché.

Par lettre du 24 août, elle a, par ailleurs, adressé un avertissement à Google au sujet de la collecte des données Wi-Fi lors des prises de vues pour « Street View » au Luxembourg en 2009. Elle a demandé à Google Inc. de de s'en tenir dorénavant strictement aux conditions fixées.

L'autorité de contrôle luxembourgeoise a réclamé une transparence totale concernant les opérations de prises de vues et le traitement des données et tenait en particulier à être informée en détail sur la collecte (période des prises de vues mobiles en relation avec l'enregistrement de la position GPS), la finalité (cartographie illustrée et vue à 360° des rues et villes sur Internet et téléphone portable etc.), l'utilisation et la publication des données. Ces informations devraient également être communiquées au public de manière appropriée.

De plus, la Commission nationale a demandé qu'une voiture de Google soit mise à sa disposition pour inspection avant que les prises de vues recommencent au Luxembourg afin de pouvoir garantir qu'à l'avenir aucune donnée personnelle ne puisse être collectée à travers des bornes Wi-Fi privées.

Un mois plus tard, la CNPD a procédé à l'inspection d'une des voitures utilisées pour collecter les images. Elle a pu s'assurer que la voiture inspectée n'était plus

pourvue des équipements controversés de détection de réseaux Wi-Fi qui interceptaient des données privées transmises. Elle a en outre reçu des réponses satisfaisantes et détaillées des spécialistes de Google à ses questions sur le fonctionnement de la collecte des données. La voiture mise à disposition était celle (immatriculée en Belgique) qui devait parcourir à nouveau le Grand-Duché lors de la reprise des prises de vues.

Droit d'opposition des individus concernant la publication des façades et alentours des habitations

Le droit d'opposition contre la publication d'images portant sur une habitation a été un élément important des discussions avec Google Inc. dès le début et fait partie des conditions de notification à respecter par la société américaine. La Commission nationale tient à faire respecter ce droit d'opposition, attribué aux personnes pour des raisons prépondérantes et légitimes.

La prise de position de Google, du moins telle que reproduite dans la presse le 5 novembre 2010, a soulevé l'interrogation de la CNPD sur le point de savoir si Google tenait à respecter les conditions de notification. Une porte-parole du département Presse de Google Benelux avait en effet déclaré que Google entendrait ne pas prendre en considération d'éventuelles oppositions à la publication d'images de leur habitation lui étant adressées préalablement à la mise en service de « Street View » au Grand-Duché. Google avait invité les résidents luxembourgeois à se servir exclusivement de la fonctionnalité électronique mise à disposition pour s'opposer ou signaler en ligne des images problématiques lors de la navigation sur Internet.

Cette décision de Google a amené la Commission nationale, dans sa délibération n°329/2010 du 5 novembre 2010, à interdire à Google Inc. de prendre des images pour son service « Street View » aussi longtemps qu'elle ne respecte pas les oppositions exprimées préalablement à la mise en ligne des images par des personnes concernées. À défaut d'assurances sur le respect des oppositions préalables, la poursuite de la collecte de données et notamment du captage d'images d'habitations porte atteinte aux libertés et droits fondamentaux des personnes concernées. Dès lors, la Commission nationale a estimé nécessaire de prononcer une sanction administrative en application de l'article 33 paragraphe (1) lettre (c) de la loi modifiée du 2 août 2002.

Lors des prises de vues en automne 2009, de nombreux citoyens s'étaient en effet adressés directement à la CNPD pour faire valoir leur droit d'opposition. Celle-ci a ensuite transmis ces objections au représentant de Google au Luxembourg. La Commission nationale avait mis à disposition des citoyens une lettre-type sur son site Internet afin de faciliter les démarches pour faire valoir leur droit d'opposition contre la publication d'enregistrements portant sur une habitation ou d'autres données personnelles sur le site de « Google Street View ».

En Allemagne, 244.000 citoyens avaient fait usage de ce droit en demandant que la photo de leur habitation soit rendue floue ou retirée du service de Google. Le géant américain de l'Internet s'était engagé à rendre méconnaissables au moyen d'un traitement automatisé performant les visages des personnes tout comme les immatriculations de véhicules avant la publication des prises de vues sur Internet et à tenir compte de façon appropriée des réclamations reçues.

Les discussions menées avec Google sur l'application concrète de ces principes aux prises de vue du Grand-Duché n'ont pas progressé en raison du report du calendrier de mise en ligne de Street View en Europe.

3.5 Recensement général de la population en 2011

Au-delà de la loi électorale du 18 février 2003, les recensements de la population sont prévus par le règlement (CE) N° 763/2008 du Parlement européen et du Conseil du 9 juillet 2008. En amont du recensement général prévu pour le 1er février 2011, la Commission nationale a eu plusieurs réunions avec le STATEC au sujet du contenu du questionnaire de recensement et des modalités de la collecte et du traitement des réponses qui forment l'objet du projet de règlement grand-ducal prescrivant un recensement général de la population, des logements et des bâtiments du Grand-Duché au 1er février 2011.

Dans son analyse, la Commission nationale a formulé un certain nombre de recommandations de nature à favoriser l'anonymisation des informations recueillies, l'obligation de confidentialité pesant sur les recenseurs et de minimiser les questions portant sur des données sensibles. Le STATEC a tenu compte de façon appropriée de toutes les remarques faites par la Commission nationale lors des diverses réunions de travail. De ce fait, la Commission nationale a donné son assentiment à la version définitive du questionnaire le 18 juin 2010. Le 27 septembre 2010, la Commission nationale a également donné son assentiment concernant le règlement grand-ducal mentionné ci-dessus.

Le recensement de la population est une opération de grande ampleur qui n'a lieu que tous les dix ans. Il sert à obtenir des données détaillées sur le nombre de résidents, la situation socio-économique et les conditions de logement de la population vivant au Grand-Duché. C'est par ailleurs la seule source statistique fournissant des chiffres fiables par unité territoriale (localité, commune, canton...). Grâce aux données collectées, les communes et l'État pourront planifier les besoins en infrastructures de demain. Il y a donc un intérêt légitime d'effectuer ce recensement, dont les résultats donneront une image détaillée de l'état et de l'évolution socio-économique du Luxembourg et constitueront de ce fait un outil d'analyse et de savoir, et aussi un point de repère essentiel pour les décideurs politiques et économiques.

Une alternative au recensement pour obtenir les données requises serait l'utilisation des divers fichiers administratifs existants (comme celui du Centre commun de la sécurité sociale, celui de l'Administration des Contributions directes et le Répertoire national des personnes physiques). À noter que dans le cas du recours à des registres administratifs et à leur interconnexion, des questions supplémentaires se poseraient en matière de protection des données et du respect de la vie privée. S'y ajouterait le problème du droit du citoyen de disposer lui-même de ses données : tandis que le recensement classique fournit la possibilité de maintenir un certain contrôle sur les réponses et l'étendue des informations renseignées, l'enlèvement du cloisonnement entre les différents fichiers publics pourrait traduire une transparence totale du citoyen.

Par ailleurs, toute interconnexion de données qui n'est pas expressément prévue par un texte légal ou réglementaire doit être autorisée par la Commission nationale sur demande conjointe présentée par les responsables des traitements en cause. De manière générale, il faut limiter les interconnexions entre différentes bases de données. À ceci s'ajoute que la collecte indirecte via les fichiers publics présenterait le risque que les données ne soient plus actuelles, erronées ou qu'elles soient utilisées pour d'autres finalités. En outre, selon le STATEC, au Luxembourg, il n'existe pas de fichiers administratifs exploitables pour donner une vue complète sur la situation socio-économique du pays. Une autre alternative au recensement seraient les enquêtes par sondage. Cette solution ne permettrait cependant pas d'obtenir des résultats fiables pour certaines sous-populations (p.ex. localités, communes).

La distribution et la collecte des bulletins se font par les agents recenseurs. L'agent est tenu au secret statistique des documents collectés. L'article 11 du règlement grand-ducal interdit aux fonctionnaires, aux agents recenseurs et à toute autre personne collaborant aux travaux de recensement de divulguer les renseignements qu'ils viendraient à connaître du chef de leur mission ou intervention. L'article 458 du Code pénal leur est applicable sans préjudice d'éventuelles sanctions disciplinaires. L'agent recenseur n'a pas le pouvoir de contrôler la véracité des réponses fournies et ne peut entrer dans un logement que s'il y est invité. Pour les citoyens ne voulant pas remettre leur bulletin à l'agent recenseur parce qu'ils s'inquiètent que celui-ci puisse prendre connaissance de leurs données à caractère privé, il existe deux alternatives : soit opter pour une réponse par voie électronique via le « guichet unique » en ligne, soit envoyer le formulaire directement au STATEC par courrier.

Lors de la saisie informatique des données, les nom et adresse des citoyens seront détachés du formulaire de recensement pour le rendre anonyme. Ces données ne feront donc pas partie du fichier informatique constitué sur base du recensement. L'anonymisation peut se faire sous le contrôle de la Commission nationale. Cela vaut également pour les ménages ayant répondu par voie électronique. Les données transmises (nom, prénom, adresse) seront conservées au Centre des technologies de l'information de l'État pendant une période courte.

Après vérification de l'enregistrement correct des personnes et envoi au STATEC, les données nominatives seront supprimées après une journée au maximum. L'identification des répondants sert à éviter que des ménages répondent deux fois au questionnaire et de garantir l'exhaustivité du recensement, qui a un but purement statistique et dont les données ne pourront pas être utilisées à des fins administratives ou fiscales.

Les questions sur l'utilisation des langues à la maison et au travail, les formes d'énergie utilisées, la mobilité, le niveau d'éducation ou la profession exercée correspondent aux variables obligatoires du règlement (CE) No 763/2008 du Parlement européen et de Conseil du 9 juillet 2008 ou à des fortes recommandations d'organisations internationales. Ces questions constituent également une base importante pour permettre une analyse socio-économique de la population. Le questionnaire du recensement ne comporte par ailleurs pas de questions qui révèlent des données à caractère sensible comme l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données relatives à la santé et à la vie sexuelle ou les données génétiques. Une autre mesure pour protéger la vie privée du recensé est de ne pas demander la date de naissance, mais uniquement la période de naissance (avant ou après le 1er février) pour déterminer l'âge de la personne recensée.

3.6 Simplification des démarches administratives

La loi impose aux entreprises luxembourgeoises l'accomplissement d'une déclaration préalable pour chaque traitement de données, notamment dans un intérêt de transparence vis-à-vis des citoyens (la Commission nationale entretient un registre public des traitements de données). Quoique les traitements les plus courants soient dorénavant exemptés de cette obligation (sous condition de remplir certains requis en matière de protection des données), un certain nombre de traitements restent soumis au devoir de notification préalable à la Commission nationale ou doivent même, dans certains cas plus spécifiques, être autorisés par elle.

Si la CNPD reste attachée au principe de transparence vis-à-vis des citoyens, elle s'efforce néanmoins à limiter à un strict minimum l'impact négatif des formalités sur l'activité journalière des entreprises. Dans ce sens, elle mise notamment sur trois aspects : la disponibilité rapide des informations, la guidance et le pragmatisme.

L'accessibilité et la simplicité de l'information constituent des éléments clés pour simplifier la démarche de l'entreprise ; dans cette optique, le site Internet de la CNPD a fait peau neuve au début de l'année 2010 et l'accès aux informations proposées a été optimisé. Afin de guider les entreprises de la manière la plus claire possible, elle y met à disposition des rubriques et formulaires dédiés.

À côté de sa présence sur le web, la Commission nationale s'efforce de guider aussi bien que possible les entreprises dans tous les stades de l'accomplissement d'une procédure ou démarche administrative. Dans un but d'accélérer l'acheminement de l'information (« politique des chemins courts ») tout en prenant en compte les requis en matière de confidentialité, elle offre maintenant également la possibilité aux entreprises de signer les documents par une signature électronique certifiée (LuxTrust ou similaire). Dans ce cas, il n'est plus nécessaire d'introduire matériellement la déclaration ou demande sous forme de papier, la transmission électronique (sécurisée) par le web étant suffisante.

D'un point de vue organisationnel, la CNPD a réussi à raccourcir considérablement les délais d'instruction des dossiers et de prise de décision. Elle s'efforce, de manière générale, à réduire les formalités administratives au strict nécessaire et à prendre en compte la situation particulière de chaque dossier.

3.7 Davantage de transparence concernant les fichiers communaux

Les communes assurent de nombreuses missions d'intérêt général. À côté de leur rôle classique d'administration de la collectivité locale, de gestion des infrastructures et de l'office social, elles offrent aussi un nombre croissant de services de plus en plus diversifiés aux citoyens, notamment les activités de loisirs, les services de téléalarme et de repas sur roues ou encore les antennes collectives.

Dans le cadre de ces missions, les communes utilisent et tiennent à jour de multiples fichiers comportant des données à caractère personnel. Les traitements afférents tombent dans le champ d'application de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel et doivent être déclarés à la CNPD.

Comme les dispositions légales et les pratiques établies sont semblables d'une commune à l'autre, les modalités de traitements des données sont identiques pour une mission ou un service donné.

Dans un souci de simplification administrative, la Commission nationale a adopté une notification-modèle pour les traitements des données à caractère personnel des communes, élaborée en concertation avec le Ministère de l'Intérieur, le SYVICOL et le SIGI, dont les applications informatiques mises à disposition aux communes permettent de traiter les données en conformité avec les modalités précisées dans ladite notification unique. Celle-ci facilite la déclaration des fichiers tenus par les administrations communales.

Désormais, les communes pourront notifier leurs traitements de données à la Commission nationale sous la forme d'un simple engagement formel de conformité. Par ailleurs, cette décision unique, énumérant les conditions et restrictions à respecter lors de la mise en œuvre des traitements, contribue à l'information des citoyens et peut servir comme guide de référence et outil pratique pour les fonctionnaires communaux. Les administrations communales attacheront une grande importance aux mesures organisationnelles et techniques destinées à assurer la confidentialité et la sécurité des données. Elles veilleront à soigner l'information des citoyens quant aux fichiers dans lesquels des renseignements personnels sont susceptibles de figurer (en intégrant systématiquement dans les correspondances afférentes (formulaires et questionnaires) une notice indiquant la finalité du traitement et les éventuels destinataires auxquels les données sont communiquées).

3.8 Information améliorée du public en matière de vidéosurveillance

Afin d'accroître la transparence vis-à-vis des citoyens, la Commission nationale remet désormais à toutes les entreprises et autres entités auxquelles elle a accordé une autorisation en matière de vidéosurveillance des vignettes d'information spécifiques.

Ces vignettes, qui renseignent le numéro de l'autorisation relative au système de vidéosurveillance en question, sont destinées à être apposées sur les écriteaux informant le public de la présence de caméras conformément aux dispositions de la loi modifiée du 2 août 2002 sur la protection des données.

Au-delà de l'indication que le dispositif fait bien l'objet d'une autorisation de la part de la CNPD, les vignettes fournissent aux citoyens la possibilité de vérifier par eux-mêmes, dans le registre public des traitements des données accessible via le site Internet de la Commission nationale (*www.cnpd.lu*), les modalités du traitement en question, l'étendue de l'autorisation et les conditions et limitations imposées le cas échéant par la CNPD.

4 Perspectives

En 2010, la Commission européenne a publié ses orientations stratégiques concernant la révision de la Directive 95/46/CE sur la protection des données personnelles. L'actuelle directive de l'UE doit être mise à jour pour tenir compte de l'évolution technologique rapide et des effets de la mondialisation, qui ont modifié en profondeur notre environnement et nous posent de nouveaux défis en matière de protection des données à caractère personnel. Ladite directive, vieille de 16 ans, a été élaborée avant la démocratisation d'Internet, le développement des réseaux sociaux, l'apparition de nouvelles technologies comme la géolocalisation ou les puces RFID, la vidéosurveillance, le cloud computing et la publicité comportementale en ligne.

Les citoyens vivent dans un monde où les données relatives à leurs habitudes d'achat, leur parcours sur Internet et autres activités sont collectées, analysées, combinées – souvent à leur insu. Grâce à des logiciels de calcul toujours plus performants, il est possible de définir à moindre coût le profil de tout un chacun.

Dans le cadre de la révision de la directive de 1995, les modifications apportées devront donner plus de visibilité, de transparence et plus de contrôle aux citoyens sur ce qui est fait de leurs données. Lors d'une session de navigation sur Internet, les utilisateurs devraient être en mesure de donner leur « consentement éclairé » au traitement des données les concernant et de bénéficier du « droit à l'oubli » lorsque ces informations ne sont plus nécessaires ou qu'ils en demandent la suppression.

La promotion de l'utilisation des technologies d'amélioration de la confidentialité (« PET : Privacy Enhancing Technologies »), ainsi que la prise en compte du principe du respect de la vie privée dès la conception (« Privacy by design ») pourraient jouer un rôle important dans ce contexte pour responsabiliser davantage les responsables du traitement afin qu'ils mettent en place des politiques et mécanismes efficaces pour assurer le respect des règles en matière de protection des données.

Une autre mesure visant une responsabilisation accrue des responsables du traitement est l'instauration d'une notification obligatoire des violations aux traitements de données. La notification, instaurée par la récente révision de la directive « vie privée et communications électroniques », n'est applicable que dans le secteur des télécommunications. Compte tenu du risque que des violations de données se produisent dans d'autres secteurs, la Commission européenne a annoncé qu'elle examinera les modalités d'une extension à d'autres secteurs de l'obligation de notifier les atteintes aux données à caractère personnel.

L'introduction de l'obligation pour les fournisseurs de services de communications électroniques de notifier les failles de sécurité à la Commission nationale constitue une avancée majeure sur le plan de la protection de la vie privée. De plus, ils sont obligés d'informer leurs abonnés dès lors que l'incident constaté est susceptible de les affecter défavorablement au niveau de la protection de leur vie privée et des données les concernant. Un rôle important revient dorénavant à notre Commission nationale dans la mise en œuvre de ces nouvelles règles. Ses ressources, en particulier au niveau des collaborateurs à compétence informatique et technologique, devront elles aussi évoluer de façon à lui permettre d'assumer convenablement ses nouvelles responsabilités.

L'entrée en vigueur du Traité de Lisbonne a également changé la donne. La Commission européenne peut dorénavant définir les règles en matière de protection des données dans le domaine de la coopération policière et judiciaire en matière pénale. La rétention des données aux fins d'enquêtes de police devrait aussi relever du nouveau cadre légal. Les données conservées à cet effet peuvent inclure des informations concernant les transferts bancaires, l'achat de billets d'avion, l'enregistrement et le contrôle de sécurité à l'aéroport, la navigation sur Internet, l'envoi de mails et les appels téléphoniques. Ces données sont collectées par des entreprises privées à des fins commerciales et contractuelles et peuvent être utilisées par les pouvoirs publics dans le cadre d'enquêtes sur le terrorisme et la criminalité grave.

Un autre défi repose sur la recherche d'une harmonisation plus poussée des règles de protection des données au niveau de l'Union européenne. Les disparités qui caractérisent actuellement la mise en œuvre des règles européennes relatives à la protection des données et le défaut de clarté quant

à l'identification du pays dont les règles s'appliquent, entravent la liberté de circulation des données à caractère personnel entre les États membres au sein du marché intérieur et majorent les coûts. La simplification de ce système permettrait de réduire considérablement la charge administrative.

Dans le cadre de données transférées en dehors de l'Union européenne, il s'agit d'améliorer et de rationaliser les procédures actuelles, y compris les instruments juridiquement contraignants et les « règles d'entreprise contraignantes » (« BCR : Binding Corporate Rules »), afin de parvenir à une approche de l'UE plus uniforme et cohérente à l'égard des pays tiers et des organisations internationales.

Enfin, la Commission européenne a annoncé vouloir assurer un contrôle plus concret de l'application des règles en renforçant et en harmonisant davantage le rôle et les pouvoirs des autorités nationales chargées de la protection des données et du groupe de travail « Article 29 ».

Les défis sont énormes considérant la globalisation et le transfert de données personnelles sur le plan international, le développement des nouvelles technologies, en particulier en ligne et les développements dans le secteur de la police et de la justice. Les efforts pour moderniser et renforcer les différents cadres réglementaires - pas seulement celui de l'Union européenne, mais aussi celui du Conseil de l'Europe et de l'OCDE - devront se développer en synergie.

5 Ressources, structures et fonctionnement de la Commission nationale

5.1 Rapport de gestion relatif aux comptes de l'exercice 2010

Dépenses de fonctionnement

Le total des frais de fonctionnement encourus par l'établissement public au cours de l'exercice 2010 s'élève à 1.498.405,67€. L'augmentation par rapport à l'exercice précédent ne s'élève qu'à 1,03% et reste en dessous des prévisions budgétaires qui incluaient un renforcement en personnel n'ayant pas encore reçu l'aval de la CER (un poste d'ingénieur informaticien).

Les charges relatives au personnel permanent ont progressé légèrement par rapport à l'exercice 2010 principalement du fait du renforcement des effectifs par une employée à durée déterminée au service juridique - renforcement dû au congé de paternité accordé à un des juristes jusqu'en octobre 2011. Néanmoins, compte tenu du fait que le poste d'employé administratif au secrétariat est resté inoccupé pendant six mois, les dépenses sont restées en dessous des prévisions.

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'État à Belval-Ouest) ont augmenté de 13,15%.

La Commission nationale a dû recourir également 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, bien qu'il eut été sans doute préférable pour la continuité du service, d'acquérir et de conserver depuis 2002, les compétences afférentes au sein de l'établissement public.

Parmi les dépenses d'honoraires et frais d'experts et prestataires externes pour un montant de 150.148,63€ figurent également les honoraires d'avocats et factures de la fiduciaire qui tient la comptabilité et établit le bilan de l'établissement public.

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

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

Les dépenses d'information du public et de communication (36.180€) ont dépassé légèrement les montants prévus alors que le coût des annonces de presse publiées dans le cadre de la campagne menée à l'occasion de la journée européenne du 28 janvier 2010 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.

Dans un souci de simplification administrative, la Commission nationale, par le biais d'une notification unique (une forme simplifiée de notification), a défini les modalités des traitements de données à caractère personnel mis en œuvre par les communes du Grand-Duché de Luxembourg dans le cadre de l'exercice des missions qui leur sont conférées. Désormais, les communes pourront notifier leurs traitements de données à la Commission nationale sous la forme d'un simple engagement formel de conformité.

Avec les autorisations accordées en matière de vidéosurveillance, la Commission nationale a fait parvenir des vignettes que les requérants peuvent apposer sur les écriteaux rendant le public attentif à la mise en œuvre d'une vidéosurveillance. Les vignettes jointes à l'autorisation ne sont pas destinées à substituer ces supports d'information, mais à les compléter en étant placées à proximité des caméras, signalant ainsi que le dispositif de vidéosurveillance en question a été autorisé par la Commission nationale.

Le niveau des mesures de sécurité organisationnelle et technique qui représentent un volet important des garanties appropriées pour la protection des données personnelles est vérifié dans chaque dossier d'autorisation préalable. Cet aspect a donné lieu par ailleurs au cours de l'exercice 2010 à diverses investigations dont la Commission a pris l'initiative depuis 2005 même en dehors des plaintes et demandes

de vérification qui lui ont été soumises. Pour les contrôles sur place, audits et vérifications à effectuer dans ce domaine, la Commission nationale a eu recours à un expert externe spécialisé dans les questions de sécurité informatique et de bonnes pratiques organisationnelles pour un montant de 16.617,50€.

Les frais relatifs à la gestion et maintenance des systèmes et réseaux pour un montant de 27.129,51€ sont restés conformes aux estimations budgétaires.

Les amortissements comptabilisés en 2010 atteignent un montant total 16.090,46€. 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 ainsi qu'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 53.749,02€ est resté quelque peu en dessous de nos prévisions. En outre des produits financiers (intérêts créditeurs) ont pu être enregistrés à hauteur de 3.759,68€.

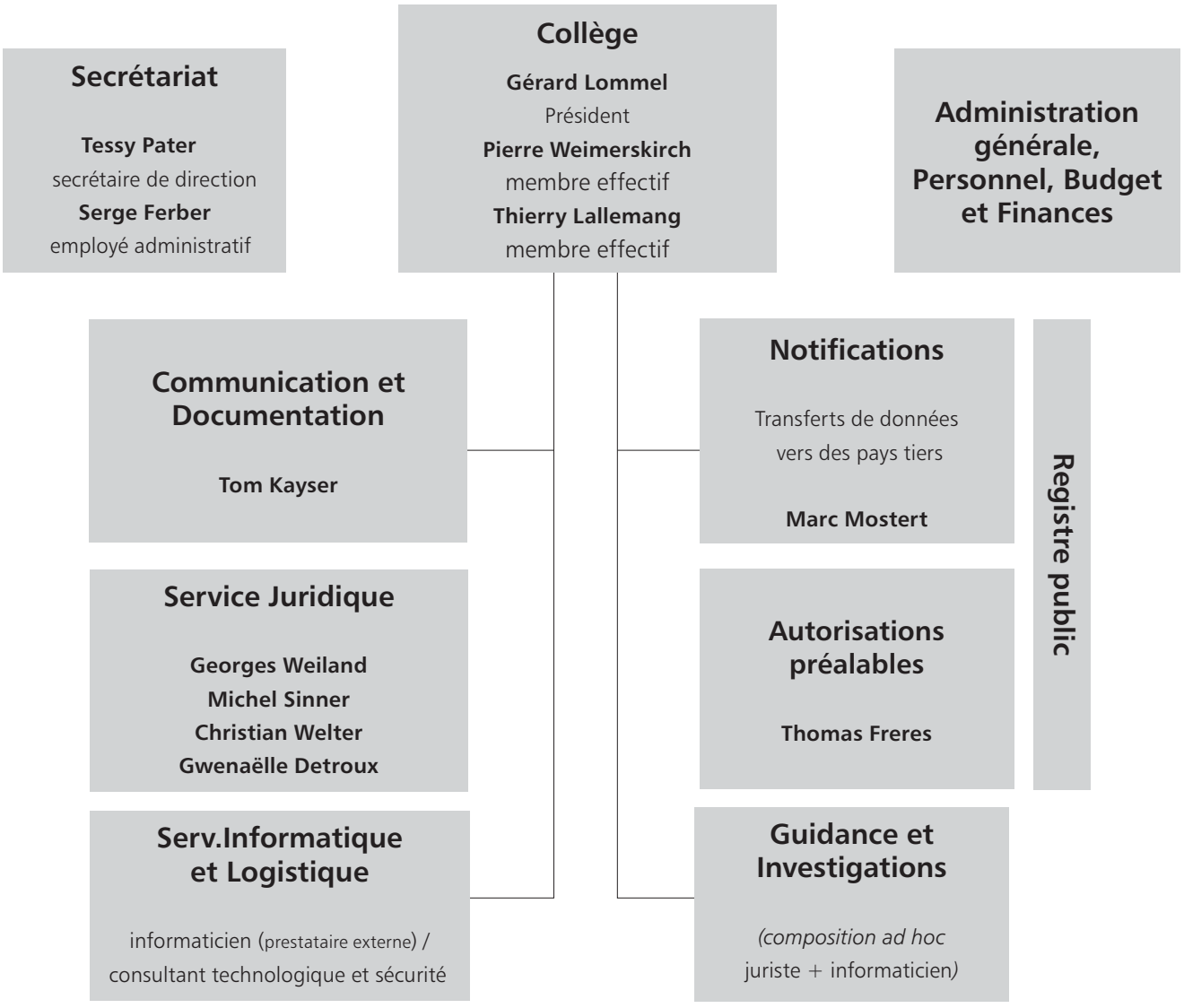
Résultat d'exploitation

Compte tenu de la dotation annuelle de 1.488.000€dont la Commission nationale a bénéficié en 2010 de la part de l'État en application de l'article 37 paragraphe (4) de la loi, le résultat d'exploitation de l'établissement public s'établit à 47.103,03€ au 31 décembre 2010 et sera reporté à nouveau sur l'exercice suivant.

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 Gwenaëlle DETROUX, juriste
Tenue du registre public et prise en charge administrative des notifications et demandes d'autorisations	
	Marc MOSTERT, rédacteur principal Thomas FRERES, rédacteur principal
Service informatique et de la logistique	
	Informaticien (prestataire externe) Consultant technologies et sécurité (prestataire externe)
Secrétariat, administration générale et finances	
	Tessy PATER, secrétaire de direction Serge FERBER, employé administratif
Service communication et documentation	
	Tom KAYSER, attaché de direction stagiaire

5.3 Organigramme de la Commission nationale



6 La Commission nationale en chiffres

Formalités préalables

	2003	2004	2005	2006	2007	2008	2009	2010	
a) Notifications									**TOTAL**
- notifications ordinaires	2.646	850	500	250	760	385	345	295	6.031
- notifications simplifiées	750	900	720	890	537	-	-	-	3.797
- engagements de conformité	-	-	-	-	-	942	227	15	1.184
(Total a)	**3.396**	**1.750**	**1.220**	**1.140**	**1.297**	**1.327**	**572**	**310**	**11.012**
b) Autorisations préalables									
- demandes d'autorisation	765	406	317	295	392	606	542	607	3.930
- engagements de conformité	718	14	17	19	151	220	70	92	1.301
(Total b)	**1.483**	**420**	**334**	**314**	**543**	**826**	**612**	**699**	**5.231**
(Total général a) + b))	**4.879**	**2.170**	**1.554**	**1.454**	**1.840**	**2.153**	**1.184**	**1.009**	**16.243**
Déclarants (responsables ayant accompli des formalités)	2.220	2.500	2.850	3.300	3.754	4.357	4.772	5.110	

Demandes de renseignements

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

Plaintes et investigations

	2003	2004	2005	2006	2007	2008	2009	2010
- plaintes, demandes de vérification de licéité et investigations :	**15**	**38**	**40**	**30**	**34**	**63**	**133**	**145**

Séances de délibération

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

Participations aux groupes de travail sur le plan européen

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

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

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

Séances d'information, conférences, exposés

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

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

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

ANNEXES

Avis et décisions

Avis relatif au projet de loi n°6113 portant modification des articles 5 et 9 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de l'article 67-1 du Code d'instruction criminelle et au projet de règlement grand-ducal déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou de réseaux de communications publics

Délibération n° 85/2010 du 26 avril 2010

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 9 février 2010, Monsieur le Ministre des Communications et des Médias a invité la Commission nationale à se prononcer au sujet du projet de loi n° 6113 portant modification des articles 5 et 9 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de l'article 67-1 du Code d'instruction criminelle (ci-après : le projet de loi) et au sujet du projet de règlement grand-ducal déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou de réseaux de communications publics (ci-après le projet de règlement grand-ducal).

Suivant l'exposé des motifs, le projet de loi et le projet de règlement grand-ducal se placent dans le contexte de la lutte contre le terrorisme et la criminalité grave. Ces textes traitent plus précisément de la rétention des données relatives au trafic et de données de localisation en matière de télécommunications en vue d'assurer leur disponibilité à des fins de recherche, de détection et de poursuite d'infractions graves.

La disponibilité des données de localisation et de trafic aux autorités judiciaires va au-delà de la conservation de données que les opérateurs effectuent en tout état de cause pour leurs propres besoins opérationnels, techniques et administratifs.

Elle concerne les données personnelles de tous les citoyens utilisant des moyens de télécommunication électroniques. Elle porte dès lors atteinte à la sphère privée de l'ensemble de la population qui se trouve en quelque sorte placée sous une suspicion généralisée (« *verdachtsunabhängiger Generalverdacht* »). Certes, la rétention ne porte pas directement sur le contenu des communications, mais uniquement sur les données de trafic et de localisation. Cependant, l'accès à ces données permet de connaître toutes sortes d'informations sur la vie privée et de reconstituer une grande partie des contacts sociaux de tout un chacun. Par ailleurs, il permet de retracer les déplacements de chaque individu utilisant un téléphone mobile. L'accès à ces données révèle des informations concernant non seulement la personne directement ciblée, par exemple un auteur présumé d'une infraction, mais concernant également toutes les personnes ayant communiqué avec elle par téléphone, courriel etc.

A ce sujet, on peut citer la Cour constitutionnelle allemande:

« (a) Die sechs Monate andauernde Möglichkeit des Zugriffs auf sämtliche durch eine Inanspruchnahme von Telekommunikationsdiensten entstandenen Verkehrsdaten bedeutet eine erhebliche Gefährdung des in Art. 10 Abs. 1 GG verankerten Persönlichkeitsschutzes.

Dass ein umfassender Datenbestand ohne konkreten Anlass bevorratet wird, prägt auch das Gewicht der dadurch ermöglichten Verkehrsdatenabrufe. Von der Datenbevorratung ist annähernd jeder Bürger bei jeder Nutzung von Telekommunikationsanlagen betroffen, so dass eine Vielzahl von sensiblen Informationen über praktisch jedermann für staatliche Zugriffe verfügbar ist. Damit besteht für alle am Telekommunikationsverkehr Beteiligten das Risiko, dass im Rahmen konkreter behördlicher Ermittlungen über einen längeren Zeitraum hinweg Verkehrsdaten abgerufen werden. Dieses Risiko konkretisiert sich im einzelnen Abruf, weist jedoch angesichts der flächendeckenden Erfassung des Telekommunikationsverhaltens der Bevölkerung weit über den Einzelfall hinaus und droht, die Unbefangenheit des Kommunikationsaustauschs und das Vertrauen in den Schutz der Unzugänglichkeit der Telekommunikationsanlagen insgesamt zu erschüttern (vgl. zu einzelnen Datenabrufen BVerfGE 107, 299 <320>).

(b) In dem Verkehrsdatenabruf selbst liegt ein schwerwiegender und nicht mehr rückgängig zu machender Eingriff in das Grundrecht aus Art. 10 Abs. 1 GG. Ein solcher Datenabruf ermöglicht es, weitreichende Erkenntnisse über das Kommunikationsverhalten und die sozialen Kontakte des Betroffenen zu erlangen, gegebenenfalls sogar begrenzte Rückschlüsse auf die Gesprächsinhalte zu ziehen. Zudem weist ein Verkehrsdatenabruf eine erhebliche Streubreite auf, da er neben der Zielperson des Auskunftsersuchens notwendigerweise deren Kommunikationspartner erfasst, also vielfach Personen, die in keiner Beziehung zu dem Tatvorwurf stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben (vgl. BVerfGE 107, 299 <318 ff.>).

Weiter werden in vielen Fällen die durch den Verkehrsdatenabruf erlangten Erkenntnisse die Grundlage für weitere Ermittlungsmaßnahmen bilden, die ohne diese Erkenntnisse nicht durchgeführt worden wären. Solche Ermittlungsmaßnahmen, beispielsweise Wohnungsdurchsuchungen oder Überwachungen der Telekommunikation, können ihrerseits den Betroffenen erheblich belasten, ohne dass es darauf ankommt, ob sie den gegen ihn bestehenden Verdacht einer strafbaren Handlung erhärten oder widerlegen. Auch die darin liegenden Nachteile können im Anschluss an die Ermittlungsmaßnahme nicht mehr behoben werden.»[1]

La rétention des données et l'accès à ces données par les autorités chargées de la recherche, de la détection et de la poursuite d'infractions graves constituent une ingérence profonde dans la jouissance des droits fondamentaux prévus par la Constitution et par la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales.

En effet, l'article 28 de la Constitution dispose que *« le secret des lettres est inviolable. - La loi détermine quels sont les agents responsables de la violation du secret des lettres confiées à la poste. La loi réglera la garantie à donner au secret des télégrammes. »*

L'article 11 paragraphe (2) de la Constitution dispose que *« l'Etat garantit la protection de la vie privée, sauf les exceptions fixées par la loi. »*

Enfin, l'article 8 de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales dispose ce qui suit :

« Droit au respect de la vie privée et familiale

1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est 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. »

Il résulte des trois dispositions susmentionnées qu'une exception aux droits y énoncés n'est possible qu'en vertu d'une loi. Il appartient en outre au législateur de faire la balance entre, d'un côté, un droit fondamental et, de l'autre côté, l'intérêt supérieur qui justifie cette exception.

[1] BVerfG, 1 BvR 256/08 vom 11.3.2008, Absatz-Nr. 155-157

Toute exception à un droit fondamental ne peut avoir lieu que dans le respect du principe de proportionnalité. La Cour constitutionnelle allemande a énuméré les devoirs du législateur pour ce qui est de la mise en œuvre de ce principe de proportionnalité en matière de rétention des données :

« Der Grundsatz der Verhältnismäßigkeit verlangt, dass die gesetzliche Ausgestaltung einer solchen Datenspeicherung dem besonderen Gewicht des mit der Speicherung verbundenen Grundrechtseingriffs angemessen Rechnung trägt. Erforderlich sind hinreichend anspruchsvolle und normenklare Regelungen hinsichtlich der Datensicherheit, der Datenverwendung, der Transparenz und des Rechtsschutzes.»[2]

La rétention des données de télécommunications et les possibilités qu'ouvre l'accès à ces données représentent une atteinte sans précédent au droit au respect de la vie privée. Aux yeux de la Commission nationale, une mesure attentatoire au respect de la vie privée ne se justifie que dans le contexte particulier de la lutte contre la criminalité grave et plus particulièrement le terrorisme et la criminalité organisée et que sous des conditions très strictes, en particulier celle d'un contrôle juridictionnel préalable.

I. Le projet de loi n° 6113 portant modification des articles 5 et 9 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de l'article 67-1 du Code d'instruction criminelle

Le projet de loi n° 6113 a pour objet la transposition en droit luxembourgeois de la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.

La directive 2002/58/CE prévoyait déjà la faculté pour les Etats membres de mettre en place une conservation obligatoire relative aux communications électroniques pour les besoins de la recherche, de la détection et de la poursuite d'infractions sans en harmoniser le régime. Au Luxembourg, le législateur a fait usage de cette faculté dans la loi du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques (ci-après désignée « la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques») transposant la prédite directive.

La directive 2006/24/CE a pour but le rapprochement des législations nationales en matière de rétention des données de trafic et de localisation. Elle ne comporte toutefois pas de disposition visant à règlementer l'accès à ces données par les autorités judiciaires. La Cour de justice des Communautés européennes précise en effet ce qui suit:

« À cet égard, il importe de constater que les dispositions de cette directive sont essentiellement limitées aux activités des fournisseurs de services et ne réglementent pas l'accès aux données ni l'exploitation de celles-ci par les autorités policières ou judiciaires des États membres.

Plus précisément, les dispositions de la directive 2006/24 tendent au rapprochement des législations nationales concernant l'obligation de conservation de données (article 3), les catégories de données à conserver (article 5), la durée de conservation des données (article 6), la protection et la sécurité des données (article 7) ainsi que les conditions de stockage de celles-ci (article 8).

En revanche, les mesures prévues par la directive 2006/24 n'impliquent pas, par elles-mêmes, une intervention répressive des autorités des États membres. Ainsi qu'il ressort notamment de l'article 3 de cette directive, il est prévu que les fournisseurs de services doivent conserver les seules données qui sont

[2] Bundesverfassungsgericht, 1 BvR 256/08 vom 2.3.2010, 2e „Leitsatz"

générées ou traitées lors de la fourniture des services de communication concernés. Ces données sont uniquement celles qui sont étroitement liées à l'exercice de l'activité commerciale de ces fournisseurs.

La directive 2006/24 réglemente ainsi des opérations qui sont indépendantes de la mise en œuvre de toute éventuelle action de coopération policière et judiciaire en matière pénale. Elle n'harmonise ni la question de l'accès aux données par les autorités nationales compétentes en matière répressive ni celle relative à l'utilisation et à l'échange de ces données entre ces autorités. Ces questions, qui relèvent, en principe, du domaine couvert par le titre VI du traité UE, ont été exclues des dispositions de cette directive, ainsi qu'il est indiqué notamment au vingt-cinquième considérant et à l'article 4 de celle-ci. »[3]

Comme la règlementation des conditions et modalités d'accès ordonnés par les autorités judiciaires sont de la compétence des Etats membres, les dispositions y relatives du projet de loi ne découlent pas de la directive 2006/24/CE. Le projet de loi sous examen ne fait que reprendre les dispositions actuelles des articles 5 paragraphe (2) et 9 paragraphe (2) de la loi modifiée du 30 mai 2005 et adapter celles de l'article 67-1 du Code d'instruction criminelle. Elles sont analysées sous le point B. du présent avis.

A. <u>L'obligation de conservation des données en vertu de la directive 2006/24/CE</u>

1. La finalité de la conservation

La rétention des données a pour but, selon les termes de la directive 2006/24/CE « *de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne* »

Pour garantir que l'utilisation des données de télécommunication conservées ne dépasse pas la finalité voulue par la directive, une importance particulière revient à la définition des « infractions graves » et à la limitation des accès. Ces questions seront abordées dans la partie B. du présent avis.

2. Les catégories de données concernées

Le projet de loi ne détermine pas les catégories de données faisant l'objet de la rétention, mais prévoit que celles-ci sont fixées par voie de règlement grand-ducal.

La loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques prévoyait déjà la détermination des données faisant l'objet de l'obligation de rétention par un règlement grand-ducal. Or, un tel règlement n'a jamais été adopté ce qui a donné lieu à une situation d'incertitude dans le domaine des droits fondamentaux.

Les catégories de données sont désormais fixées dans le projet de règlement annexé au projet de loi. Ces catégories de données y retenues correspondent a celles fixées par la directive 2006/24/CE.

3. La durée de conservation

La loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques prévoyait initialement une durée de conservation de 12 mois. Cette durée a été ramenée de 12 mois à 6 mois par la loi du 27 juillet 2007 portant modification de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

La Commission nationale approuve que la durée de conservation des données reste limitée à 6 mois, comme c'est le cas en Allemagne, aux Pays-Bas et dans d'autres pays de l'Union européenne.

4. La question de la sous-traitance

L'obligation de conservation pèse sur les fournisseurs de services de communications électroniques accessibles au public et les opérateurs d'un réseau public de communication.

Le projet de loi prévoit que les « *fournisseurs de services ou opérateurs peuvent déléguer l'exécution de ces obligations à une ou plusieurs entités tierces, publiques ou privées, qui agissent au nom et pour le*

[3] Cour de justice des communautés européennes (grande chambre), 10 février 2009, affaire C-301/06, points 80 - 83

compte des fournisseurs de services ou opérateurs». Or, une telle sous-traitance n'est pas prévue par la directive 2006/24/CE. Vu le caractère confidentiel et la quantité des données concernées, la Commission nationale est réservée en ce qui concerne cette possibilité de sous-traitance. Elle s'interroge sur l'opportunité de prévoir la faculté d'externalisation du stockage des données confidentielles concernant des millions de communications.

La loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques contient des dispositions spécifiques en matière de sécurité et de confidentialité pesant sur les fournisseurs de service, dispositions qui devront encore être renforcées dans le cadre de la transposition du second paquet de directives en matière de télécommunications. Les sous-traitants seront-ils toujours en mesure de répondre à ces exigences qui pèsent sur leurs clients, notamment lorsqu'ils presteront leurs services sous forme de « cloud computing » ? Dans l'hypothèse où le législateur maintient le possible recours à un sous-traitant, la Commission nationale estime pour le moins nécessaire de prévoir un encadrement législatif spécifique et rigoureux.

La disposition du projet de loi sous avis relatif à la faculté de la sous-traitance permettrait la mise en place d'un stockage centralisé de données provenant de l'ensemble des opérateurs auprès d'un organisme unique à l'image du « Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) » existant au Pays-Bas.

Un tel système peut avoir certains avantages, comme par exemple celui de garantir des standards de sécurité uniformes ou celui d'une meilleure préservation du secret de l'instruction parce que les accès aux données par les autorités policières et judiciaires se feront à l'insu des opérateurs.

Néanmoins, la Commission nationale n'est pas favorable à l'établissement d'un tel système. Elle est d'avis, en effet, qu'un stockage centralisé augmenterait les risques d'abus et de détournements de finalités et le sentiment des citoyens d'être exposés à une surveillance imperceptible de la part des autorités.

Il semble d'ailleurs qu'aux Pays-Bas, l'accès aux données de télécommunications par les autorités policières et judiciaires soit beaucoup plus fréquent que dans d'autres pays, probablement parce que les données sont stockées par un organisme public proche de ces autorités.

5. La question de la sécurité des données

Le projet de loi ne contient pas de dispositions relatives aux mesures spécifiques de sécurité à appliquer aux données conservées en application de l'obligation de rétention. Néanmoins, l'article 4 (1) du projet de règlement grand-ducal prévoit que *« les données conservées sont soumises aux exigences prévues aux articles 22 (1) et 23 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. »*

La Commission nationale estime cependant que la question de la sécurité devrait être traitée au niveau de la loi, ne serait-ce que pour garder un parallélisme avec la question de la sous-traitance également prévue au niveau de la loi.

Elle relève que le récent arrêt de la Cour constitutionnelle allemande a jugé inconstitutionnelle la législation allemande régissant la rétention des données notamment en raison des garanties de sécurité jugées insuffisantes.[4] Ledit arrêt a estimé que l'hypothèse de la conservation des données de communication électronique nécessite des exigences particulières au niveau de la sécurité dans le texte même de la loi et qu'il ne suffit pas d'y renvoyer aux dispositions de la législation générale.[5]

Il paraît dès lors souhaitable de voir compléter le projet de loi par des dispositions relatives aux obligations spécifiques de sécurité en tenant compte de la nature des données et du risque d'atteinte à la vie privée du citoyen.

---

4 Bundesverfassungsgericht, 1 BvR 256/08 vom 2.3.2010

5 « Absatz » 274
Le §9 BDSG y mentionné et son « Anlage » correspondent aux articles 22 paragraphe (1) et 23 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel

Le récent arrêt de la Cour constitutionnelle allemande cite comme mesures de sécurité envisageables[6] :

- le stockage distinct sur des serveurs physiquement séparés et déconnectés de l'Internet,

- un chiffrement basé sur une encryptage asymétrique avec une sauvegarde séparée des clés d'encryptage,

- le principe des quatre yeux relatif à l'accès aux données lié à des procédés avancés concernant l'authentification relative à l'accès aux clés d'encryptage,

- la journalisation révisable des accès aux données et leur destruction,

- l'application de mécanismes de correction automatique de fautes respectivement d'erreurs et de méthodes de plausibilités.

En ce qui concerne le principe de séparation des systèmes, le Groupe de travail «ARTICLE 29» sur la protection des données a également estimé dans son avis 3/2006 que, « concrètement, les systèmes de stockage de données à des fins d'ordre public devraient logiquement être séparés des systèmes utilisés à des fins commerciales.»[7]

Finalement, la Commission nationale suggère à l'endroit de l'article 4 paragraphe (1) du projet de règlement grand-ducal de ne pas limiter la référence au seul premier paragraphe de l'article 22 de la loi modifiée du 2 août 2002, mais de l'étendre aux deux autres paragraphes du même article dont les dispositions sont également concernées par le projet de loi.

B. <u>L'accès aux données par les autorités judiciaires</u>

Si on peut considérer que la seule conservation des données de trafic et de localisation n'est attentatoire à la vie privée qu'en cas de défaillance des mesures de sécurité, il en est autrement de l'accès à ces données. En effet, c'est à partir du moment où quelqu'un accède aux données concernant un individu qu'il peut retracer où cet individu s'est trouvé à quel moment, à qui il a téléphoné et de qui il a été appelé ou à qui il a envoyé des SMS ou courriels et de qui il en a reçu, quels sites Internet il a consulté etc.

Il est dès lors nécessaire de voir encadré strictement l'accès des autorités policières et judiciaires en vue de limiter au maximum les atteintes à la vie privée des citoyens.

Il s'agit d'une part de limiter les cas d'ouverture en définissant de manière suffisamment restrictive les infractions dont la recherche, la détection et la poursuite pourra donner lieu à un accès aux données (point 1.) et d'autre part, de prévoir des dispositions réglementant la procédure d'accès qui doivent comporter des garanties appropriées visant à exclure toute utilisation allant au-delà de la finalité qui se trouve à la base de la directive et du projet de loi (point 2.).

1. La limitation des infractions pouvant donner lieu à un accès aux données

La rétention des données de communications électroniques telle que prévue par la directive 2006/24/CE vise à garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves. La directive laisse aux Etats membres le soin de déterminer ces infractions graves.

Pour ce faire, deux options se présentent :

- l'établissement d'une énumération d'incriminations auxquelles les faits recherchés doivent correspondre ou

- la définition d'un seuil minimal de peine prévue.

L'établissement par le législateur d'une liste d'infractions apparaît préférable aux yeux de la Commission nationale.

---

6 « Absätze » 223 et 275

7 Groupe de travail «ARTICLE 29» sur la protection des données
Avis 3/2006 sur la directive 2006/24/CE du Parlement européen et du Conseil sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication, et modifiant la directive 2002/58/CE
654/06/FR, WP 119
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp119_fr.pdf

Une énumération limitative permettrait de réserver l'accès aux données aux enquêtes et aux actes de poursuite relatifs à des infractions qui se situent clairement dans le contexte du terrorisme et de la criminalité organisée ou à la poursuite d'infractions dont le degré de gravité permet de les y assimiler. En ce qui concerne la définition des infractions graves, la Cour constitutionnelle allemande s'est exprimée comme suit:

« Für die Strafverfolgung folgt hieraus, dass ein Abruf der Daten zumindest den durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat voraussetzt. Welche Straftatbestände hiervon umfasst sein sollen, hat der Gesetzgeber abschließend mit der Verpflichtung zur Datenspeicherung festzulegen. Ihm kommt hierbei ein Beurteilungsspielraum zu. Er kann dabei entweder auf bestehende Kataloge zurückgreifen oder einen eigenen Katalog schaffen, etwa um Straftaten, für die die Telekommunikationsverkehrsdaten besondere Bedeutung haben, zu erfassen. »[8]

Si néanmoins le législateur retient la voie de la définition d'un seuil de peine - notamment parce que l'exercice de l'élaboration d'un catalogue apparaît excessivement complexe -, le seuil choisi devrait être suffisamment élevé de façon à garantir que l'accès aux données ne soit possible uniquement pour des infractions dont la gravité ne fait aucun doute.

La Commission nationale considère que le seuil de peine envisagé, à savoir celui d'une peine dont le maximum est égal ou supérieur à un an d'emprisonnement, n'est pas assez élevé vu le nombre certainement très important d'infractions concernées. Un seuil de peine de deux ans d'emprisonnement au moins nous semble mieux correspondre aux motifs de la directive. Tel est d'ailleurs le seuil prévu par l'article 88-1 du Code d'instruction criminelle en matière d'écoutes téléphoniques. L'accès aux données faisant l'objet de la rétention et les écoutes téléphoniques affectent en effet le même droit fondamental à savoir celui du secret des communications.

Il est à noter que certains pays ont choisi un seuil de peine de cinq ans.

[8] Bundesverfassungsgericht, 1 BvR 256/08 vom 2.3.2010, Absatz 228

2. L'exigence d'une autorisation judiciaire préalable

Dans son avis du 25 mars 2005, le groupe de l'article 29 estime que les Etats-membres devraient mettre en place dans leurs lois de transposition des garanties spécifiques notamment sur les points suivants[9] :

- la limitation des accès en fonction de la définition de l'infraction grave,

- la limitation des accès aux seuls services répressifs compétents et dans les seuls cas des infractions graves définies,

- l'exclusion d'une exploration à grande échelle des données conservées (sans éléments suffisants en relation avec une telle infraction).

La Commission nationale considère que tel serait le cas si chaque accès aux données était soumis à autorisation judiciaire préalable.

Or, le projet de loi laisse inchangé les articles 5 paragraphe (2) et 9 paragraphe (2) de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques qui permettent l'accès par la police dans l'hypothèse du crime flagrant et du délit flagrant, sans ordonnance d'un juge d'instruction.

La vérification par le juge constituerait une bonne garantie contre d'éventuels abus. La nécessité d'une ordonnance d'un juge d'instruction permettrait d'empêcher le recours aux données de communications conservées pour des recherches systématiques de type „Rasterfahndung". Une telle exigence serait par ailleurs de nature à éviter le sentiment diffus de la population d'être surveillé à son insu, les données de connexion et de localisation de tout un chacun étant librement disponibles pour la police.

[9] Groupe de travail «ARTICLE 29» sur la protection des données
Avis 3/2006 sur la directive 2006/24/CE du Parlement européen et du Conseil sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication, et modifiant la directive 2002/58/CE
654/06/FR, WP 119

La Cour constitutionnelle allemande se prononce à ce sujet comme suit:

« Für die Gewährleistung effektiven Rechtsschutzes ist eine Abfrage oder Übermittlung dieser Daten grundsätzlich unter Richtervorbehalt zu stellen.

Nach der Rechtsprechung des Bundesverfassungsgerichts kann bei Ermittlungsmaßnahmen, die einen schwerwiegenden Grundrechtseingriff bewirken, verfassungsrechtlich eine vorbeugende Kontrolle durch eine unabhängige Instanz geboten sein. Dies gilt insbesondere, wenn der Grundrechtseingriff heimlich erfolgt und für den Betroffenen unmittelbar nicht wahrnehmbar ist (vgl. BVerfGE 120, 274 <331>). Für die Abfrage und Übermittlung von Telekommunikationsverkehrsdaten kann dies der Fall sein. Angesichts des Gewichts des hierin liegenden Eingriffs reduziert sich der Spielraum des Gesetzgebers dahingehend, dass solche Maßnahmen grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen sind. Richter können aufgrund ihrer persönlichen und sachlichen Unabhängigkeit und ihrer ausschließlichen Bindung an das Gesetz die Rechte des Betroffenen im Einzelfall am besten und sichersten wahren ».[10]

La Commission nationale donne également à considérer que si l'accès aux données dans le cadre de l'enquête de flagrant crime ou de flagrant délit est possible sans autorisation du juge en vertu des articles 5 paragraphe (2) et 9 paragraphe (2) de la loi modifiée du 30 mai 2005, cela entraînerait une contradiction avec le régime de l'article 67-1 du Code d'instruction criminelle aux termes duquel le repérage des communications n'est possible que s'il est ordonné par le juge d'instruction.

La question de l'application des dispositions relatives au repérage des communications dans le cadre d'une enquête pour crime flagrant ou délit flagrant a été examinée par la Cour d'appel :

« Cette localisation de la provenance de l'appel téléphonique […] constitue un repérage de données d'appel de moyens de télécommunication à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés, au sens de l'article 67-1 du Code d'instruction criminelle. La compétence pour ordonner un tel repérage appartient en principe au seul juge d'instruction, et ce depuis la loi du 21 novembre 2002 ayant introduit au Code d'instruction criminelle ledit article 67-1. Alors qu'auparavant de telles investigations étaient opérées sur base des articles 65 et 66 du Code d'instruction criminelle, et pouvaient donc également être opérées dans le cadre des crimes et délits flagrants par les officiers de police judiciaire agissant sur base des articles 31 et 33 du Code d'instruction criminelle, le repérage est depuis l'entrée en vigueur de l'article 67-1 réservé à la compétence exclusive du juge d'instruction. Le fait que l'article 67-1 continue à figurer sous la section III « Des transports, perquisitions et saisies » du chapitre Ier du titre III du Livre premier du Code d'instruction criminelle a uniquement pour objet de distinguer le repérage des moyens de surveillance spéciale des télécommunications (articles 88-1 à 88-4 du Code d'instruction criminelle), mais n'autorise pas les officiers de police judiciaire, agissant en vertu des pouvoirs qui leur sont spécialement conférés au titre des crimes et des délits flagrants, à opérer un tel repérage au titre des articles 33 et 31 du Code d'instruction criminelle (perquisition et saisie). L'article 33 du Code d'instruction criminelle est le pendant de l'article 66 du même code, il n'inclut pas les pouvoirs que le juge d'instruction tient de l'article 67-1 dudit code. »[11]

Par ailleurs, contrairement à ce qui est indiqué dans le commentaire des articles du projet de loi sous examen, le repérage prévu par le prédit article 67-1 du Code d'instruction criminelle vise non seulement le recours à des données concernant des communications qui auront lieu après que le juge d'instruction a ordonné leur repérage mais aussi le recours à des données concernant des communications qui ont eu lieu avant que le juge d'instruction n'ait ordonné leur repérage.

En effet, l'article en question dispose notamment qu'il s'applique *« au repérage des données d'appel de moyens de télécommunication à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés »*. Cela ressort d'ailleurs aussi des travaux parlementaires relatifs à la loi du 21 novembre 2002 qui précisent

[10] Bundesverfassungsgericht, 1 BvR 256/08 vom 2.3.2010, „Absätze" 247 et 248

[11] Cour d'appel, cinquième chambre, 26 février 2008, arrêt 106/08 V

ce qui suit : « Il ressort dès lors clairement du libellé de cette disposition que la période sur laquelle porte le repérage peut viser aussi bien les communications passées que les communications futures»[12]. Dès lors, dans les deux cas, le repérage est impossible en enquête de flagrance.

La Commission nationale retient donc que la jurisprudence considère que l'accès par la police pendant l'enquête de flagrance ne peut jamais avoir lieu sans ordonnance du juge d'instruction.

Enfin, on peut relever que « *l'enquête de flagrance a pour fondement l'urgence qu'il y a à recueillir les preuves encore existantes, indispensables à la manifestation de la vérité, d'une infraction dont la commission est récente.*»[13] Or, à la différence de ce qui est le cas par exemple pour les preuves recherchées dans le cadre d'une perquisition au cours d'une enquête de flagrance, il n'existe pas de risque de dépérissement des preuves pour ce qui est des données faisant l'objet de la rétention, puisque leur conservation est assurée pendant le délai de six mois.

La loi ne saurait cependant se borner à déterminer qui a accès aux données et sous quelles conditions. La Commission nationale estime que la protection des droits du citoyen requiert également des sanctions effectives en cas de violation de la loi.

Cette nécessité est déjà mentionnée au niveau de la directive 2006/24/CE:

« Chaque État membre prend, en particulier, les mesures nécessaires pour faire en sorte que l'accès intentionnel aux données conservées conformément à la présente directive ou le transfert de ces données qui ne sont pas autorisés par le droit interne adopté en application de la présente directive soient passibles de sanctions, y compris de sanctions administratives ou pénales, qui sont efficaces, proportionnées et dissuasives.» (article 13)

La Commission nationale estime qu'il ne suffit pas que l'accès aux données et leur utilisation illicites soient assortis de sanctions pénales, mais la loi devrait également prévoir dans ces hypothèses la nullité de la preuve en matière de procédure pénale.

Enfin, la Commission nationale constate que l'article 5 paragraphe (2) de la loi modifiée du 30 mai 2005 mélange d'un côté la rétention des données pour les besoins de la recherche, de la constatation et de la poursuite d'infractions pénales (renvoi au paragraphe (1) et au Code d'instruction criminelle) et de l'autre côté l'utilisation de certaines données de trafic dans le cadre de litiges d'ordre civil ou commercial (renvoi au paragraphes (3) et (4) et mention, dans le deuxième tiret, de « *litiges notamment en matière d'interconnexion ou de facturation* »).

La rédaction de cet article pourrait laisser croire que les données faisant l'objet de la rétention imposée par la directive 2006/24/CE peuvent servir de preuves dans des litiges civils ou commerciaux.

La Commission nationale estime que la conservation des données en vertu de la directive 2006/24/CE, d'une part, et la conservation des données de connexion qui sont nécessaires pour établir les factures des abonnés et les paiements pour interconnexion, d'autre part, devraient faire l'objet de paragraphes distincts.

II. Le projet de règlement grand-ducal déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou de réseaux de communications publics

Le projet de règlement grand-ducal détermine les catégories de données faisant l'objet de la rétention. La Commission nationale n'a pas d'observations particulières à formuler à ce sujet étant donné que ce texte reprend, pour l'essentiel, les dispositions de la directive 2006/24/CE.

En ce qui concerne les mesures de sécurité, il est renvoyé aux observations formulées sous le point A. 5. selon lesquelles la Commission nationale souhaiterait que les mesures de sécurité soient traitées au niveau de la loi.

Elle relève encore que l'article 6 prévoit l'établissement de statistiques sur les accès aux données conservées en application de la directive 2006/24/CE. De telles

[12] Projet de loi n° 488900, commentaire de l'article, p. 4

[13] JurisClasseur, Procédure pénale, fascicule 20, n° 2

statistiques, qui sont publiées déjà dans d'autres pays (en matière d'accès aux données de connexion et de localisation ainsi que dans le domaine des écoutes téléphoniques et interceptions de correspondances), sont susceptibles de contribuer à une plus grande transparence, à la prévention des abus et au contrôle démocratique dans ce domaine.

Ainsi décidé à Luxembourg en date du 26 avril 2010.

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° 6148 portant modification de :

1. la loi modifiée du 22 juin 2000 concernant l'aide financière de l'Etat pour études supérieures;
2. la loi modifiée du 4 décembre 1967 concernant l'impôt sur le revenu;
3. la loi du 21 décembre 2007 concernant le boni pour enfant;
4. la loi du 31 octobre 2007 sur le service volontaire des jeunes;
5. le Code de la sécurité sociale

Délibération n° 186/2010 du 9 juillet 2010

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

C'est dans cette optique et faisant suite à la demande lui adressée par Monsieur le Ministre de l'Enseignement Supérieur et de la Recherche en date du 7 juillet 2010 que la Commission nationale entend présenter ci-après ses commentaires au sujet du projet de loi n° 6148 portant modification de : 1. la loi modifiée du 22 juin 2000 concernant l'aide financière de l'Etat pour études supérieures ; 2. la loi modifiée du 4 décembre 1967 concernant l'impôt sur le revenu ; 3. la loi du 21 décembre 2007 concernant le boni pour enfant ; 4. la loi du 31 octobre 2007 sur le service volontaire des jeunes ; 5. le Code de la sécurité sociale.

L'article III du projet de loi prévoit en particulier de réaménager l'article 7 de la loi du 21 décembre 2007 concernant le « boni enfant » pour l'adapter au nouveau régime de l'aide financière de l'Etat pour études supérieures et des effets sur les allocations familiales et le boni pour enfant pour les élèves et étudiants ayant atteint l'âge de la majorité et les volontaires visés par la loi du 31 octobre 2007 sur le service volontaire des jeunes.

La Commission nationale ne dispose pas du temps nécessaire pour approfondir l'analyse du traitement de données que le projet de loi entend créer, respectivement l'élargir (tant au niveau des catégories de données, des personnes concernées et des responsables distincts dont des fichiers sont appelés à être interconnectés) et se limitera dès lors à présenter quelques observations générales, toutes approches alternatives ne pouvant être envisagées car radicalement incompatibles avec le calendrier prévu d'adoption des modifications.

Comme nous avons eu l'occasion de le noter dans de précédents avis, les libertés individuelles et droits fondamentaux des citoyens, notamment celui à la protection de leur sphère privée, nécessitent que l'Etat s'impose des restrictions au niveau du partage et de l'échange de données même entre administrations et organismes publics dès lors que ceux-ci poursuivent des finalités et sont chargés de missions d'intérêt public distinct.

C'est le principe de finalité inscrit à l'article 8 de la Charte des droits fondamentaux de l'union européenne qui veut que les données personnelles recueillies pour des finalités déterminées ne soient pas ultérieurement utilisées de manière incompatible avec ces finalités. Ce critère de compatibilité avec la finalité pour laquelle les données ont été collectées est aussi d'application en matière d'interconnexion de données (article 16 de la loi).

La condition de compatibilité est interprétée par la doctrine comme étant réunie dès lors que les personnes concernées auraient pu raisonnablement prévoir le traitement ultérieur réservé à leurs données.

Il est admis que le simple fait par le législateur de prévoir un traitement supplémentaire comme une communication par transmission à un autre responsable ou une interconnexion avec des fichiers de celui-ci de données recueillies initialement sans prévoir cette utilisation secondaire rend de facto compatible le nouveau traitement de données.

Toutefois le législateur devrait faire un usage particulièrement parcimonieux de cette faculté et éviter, sinon limiter autant que possible les communications, échanges et partages de données qu'il instaure et devrait en outre prendre égard (par analogie aux exigences de l'article 16 de la loi modifiée du 2 août 2002 sur la protection des données personnelles) aux conditions particulièrement rigoureuses applicables en matière d'interconnexion de fichiers.

Dans le cas qui nous occupe la mise en corrélation de données à caractère personnel figurant dans les fichiers de la Caisse nationale des prestations familiales (CNPF), du Centre commun de la sécurité sociale (CCSS) et dans les fichiers de l'Administration des contributions directes (ACD) est appelée à être étendue à deux acteurs supplémentaires, à savoir le Ministère de l'Enseignement supérieur et de la Recherche (MESR) d'une part pour ce qui concerne les étudiants bénéficiant de l'aide financière de l'Etat pour études supérieures et le Service national de la jeunesse (SNJ) d'autre part pour ce qui est des bénéficiaires de l'aide aux volontaires versée en application de la loi du 31 octobre 2007 sur le service volontaire des jeunes.

L'intention du législateur étant de regrouper aide financière de l'Etat pour études supérieures et boni pour enfant dorénavant directement alloué à l'étudiant ayant atteint l'âge de la majorité, il apparaît que la gestion administrative et le contrôle des conditions liés au bénéfice des allocations familiales, du boni pour enfant et de l'aide financière pour études supérieures ou d'une modération d'impôt (ou même seulement d'un complément différentiel) requièrent que l'échange et le partage de données relatives aux bénéficiaires, allocataires respectivement attributaires entre la Caisse nationale des prestations familiales et l'Administration des Contributions directes instaurés par la loi du 21 décembre 2007 sur le boni pour enfant soient étendus aux acteurs nouvellement impliqués dans le mécanisme.

Comme le CEDIES (département relevant de l'autorité du Ministère de l'Enseignement Supérieur et de la Recherche) est en charge du versement de l'ensemble des « allocations revenant à sa population cible (étudiants majeurs en études supérieures), le boni pour enfant étant dorénavant intégré dans les aides financières de l'Etat pour études supérieures, il est logique que cet organisme doit pouvoir utiliser la banque de données commune instaurée par la loi du 21 décembre 2007.

La Commission nationale s'interroge sur le point de savoir s'il ne suffirait pas de donner accès à la banque de données interconnectée aux agents du CEDIES plutôt que d'indiquer comme utilisateur le Ministère de l'Enseignement Supérieur et de la Recherche dont il relève certes de l'autorité.

Au cas où il est jugé préférable de maintenir la mention du department ministériel sous la responsabilité duquel le traitement des données est instauré et effectué (ce qui est cohérent avec la notion de responsable conjoint du traitement), la recommandation exprimée ci-dessous prévoit de façon explicite une limitation du nombre d'agents des différents organismes publics impliqués autorisés à accéder à la banque de données commune.

Il en va de même pour le Service National de la Jeunesse (le texte ne mentionne d'ailleurs pas le Ministère de la Famille et de l'Intégration dont il relève) qui sera appelé à assurer le versement du boni pour enfant revenant aux volontaires bénéficiant d'une allocation au titre de la loi du 31 octobre 2007 sur le service volontaire des jeunes (dans laquelle il sera intégré).

La Commission nationale ne peut toutefois s'empêcher de renvoyer à ses réflexions exprimées dans son avis du 30 novembre 2007 concernant le projet de loi 5801, devenu la loi du 21 décembre 2007. Elle avait estimé que « *Dans un souci de respect de la protection des données et de la vie privée, le législateur devrait éviter autant que possible d'autoriser la mise en place successive d'interconnexions de fichiers d'administrations dont les missions correspondent à des intérêts publics différents. Le Conseil d'Etat, dans son avis du 30 janvier 2007 relatif au projet de loi n° 5554 portant modification de la loi du 2 août 2002, reste lui aussi « convaincu que l'interconnexion de données constitue une opération délicate devant être entourée d'un maximum de garanties* ».

La délimitation des données auxquelles les protagonistes d'une interconnexion peuvent avoir accès constitue une telle garantie. La Commission nationale estime dès lors que l'accès aux données du fichier commun par les deux intervenants supplémentaires mentionnés plus haut doit être limité aux seules données concernant leurs administrés respectifs, à savoir les bénéficiaires d'une aide financière pour études supérieures, respectivement les bénéficiaires d'une aide aux volontaires. En effet, elle ne voit pas l'intérêt ni la nécessité pour ces deux administrations d'avoir accès aux données personnelles de l'intégralité des personnes figurant dans la base de données commune, contrairement à l'Administration des contributions directes et la Caisse nationale des prestations familiales pour des raisons évidentes. Afin de répondre au souci visant à simplifier la gestion des dossiers et à éviter des cumuls éventuels des différentes prestations et aides entrant en ligne de compte - comme le précisent les auteurs du projet de loi – nous estimons qu'il suffit que le ministère de l'Enseignement supérieure et de la Recherche (CEDIES) ainsi que le Service national de la Jeunesse aient accès aux données des seuls administrés tombant dans leur domaine de compétence respectif. Faut-il rappeler par ailleurs que le fichier commun contient des données à caractère personnel protégées par le secret fiscal ?

L'article du projet de loi sous examen énumère et distingue dans quatre tirets différents les données que doit comprendre le fichier commun en ce qui concerne quatre des cinq intervenants, sans pour autant préciser le rôle du Centre commun de la sécurité sociale ou les données qu'il fournit le cas échéant. Le commentaire de l'article indique simplement que « *les données des différents intervenants seront centralisées dans une banque de données auprès du CCSS* ». Faute d'explications plus précises, la Commission nationale comprend que le CCSS gère la banque de données commune au niveau informatique et fournit éventuellement certaines données dont les autres acteurs ne disposeraient pas dans le cadre de la coordination du boni pour l'enfant. Ceci dit, elle estime que les données du fichier commun ne doivent être communiquées à aucun tiers, de sorte que le CCSS doit garantir qu'aucun autre organisme de la sécurité sociale ne puisse avoir accès à la base de données interconnectées.

Dans son avis du 30 novembre 2007 relatif au projet de loi n° 5801, devenu la loi du 21 décembre 2007, la Commission nationale avait estimé que la gestion partagée du fichier comportait un risque inhérent de dilution des responsabilités des administrations concernées par l'interconnexion et avait, pour cette raison, recommandé de rajouter à l'article 7 un alinéa supplémentaire concernant les mesures de sécurité appropriées dont l'interconnexion devrait être assortie dont la teneur était la suivante : « *L'accès à cette base de données commune est limité à un nombre restreint de personnes autorisées. Le système informatique doit être sécurisé conformément aux articles 22 et 23 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.* ».

Malgré la volonté de la commission parlementaire de rajouter cet alinéa au texte de loi, le Conseil d'Etat, dans son avis complémentaire du 11 décembre 2007[14], avait estimé que cette proposition était superfétatoire, alors qu'elle ne faisait « *que rappeler les principes et des règles de la législation sur la protection des données, qui sont d'ordre public et s'imposent dès lors en tout état de cause* ». Or, la Commission nationale voudrait relever que d'autres textes de loi, contenant des références à la législation sur la protection des données (en particulier aux articles 22 et 23 de la loi modifiée du 2 août 2002), ont été adoptés sans que le Conseil d'Etat ne s'y est opposé. Comme dernier exemple en date on peut citer le projet de loi n° 6113.

La Commission nationale voudrait dès lors réitérer sa proposition de rajouter le susdit alinéa à l'article 7, alors qu'elle estime nécessaire dans le cadre d'une interconnexion autorisée par la voie légale de préciser dans le texte afférent que l'accès au fichier commun doit être limité à un nombre restreint de personnes autorisées. En l'espèce, cette limitation de l'accès aux données revêt une importance particulière en ce qui concerne le Service nationale de la jeunesse, le ministère de l'Enseignement supérieur et de la Recherche ainsi que le Centre commun de la sécurité sociale. En effet, contrairement à la Caisse nationale des prestations familiales et l'Administration des contributions directes, les trois autres acteurs interviennent dans une moindre

[14] doc. Parl. N° 5801/05

mesure, soit pour le traitement des demandes d'aides financières d'un nombre limité d'administrés (SNJ et le CEDIES du MESR), soit pour la gestion informatique de la base de données commune(CCSS). Le nombre de personnes autorisées à accéder aux données devraient dès lors être limité au sein de chacune de ces administrations aux seuls agents et fonctionnaires en charge des demandes d'aides financières ou de la gestion informatique du fichier commun.

L'extension de l'interconnexion de données faisant l'objet maintenant du projet de loi n° 6148 sous revue, démontre que la tendance à regrouper sous prétexte de simplification administrative les données des citoyens dans des fichiers mutualisés dont la responsabilité sera aussi peu clairement identifiée entre les acteurs impliqués qui sont désormais au nombre de cinq, que la nature juridique exacte de l'allocation sui generis dont ils assument conjointement la charge, ne manquera pas d'exposer les citoyens à des risques croissants dans la restriction de leur vie privée et données à caractère personnel.

Ainsi décidé à Luxembourg en date du 9 juillet 2010.

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 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

Délibération n° 238/2010 du 26 juillet 2010

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 ».

Par son courrier du 3 août 2009, Madame la Ministre de l'Éducation nationale et de la Formation professionnelle a soumis à la Commission nationale pour avis 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.

Celui-ci, trouvant son fondement notamment dans l'article 20 de la loi du 6 février 2009 relative à l'obligation scolaire, envisage de couvrir, de manière générale, tout échange de données entre le Ministère de l'Éducation nationale et de la Formation professionnelle (ci-après désigné « le Ministère ») et des tiers, à savoir des personnes, administrations, services publics ou ministères ne faisant pas partie intégrante du ministère en question, effectué en vue de contrôler le respect de l'obligation scolaire et l'assiduité des élèves fréquentant l'enseignement fondamental ou l'enseignement postprimaire ainsi que de vérifier l'accomplissement des missions de l'École en général.

Le texte en projet a vocation à servir de nouvelle base juridique pour l'exploitation, par le Ministère, d'une base de données à caractère personnel relative aux élèves. Il envisage d'englober davantage de données et d'acteurs que ce que ne prétend actuellement le règlement grand-ducal du 20 juin 2001 autorisant la création et l'exploitation d'une banque de données nominatives relative aux élèves, et contient dès lors une disposition abrogeant ledit règlement. De plus, la base de données semble intégrer deux bases de données, « Scolaria élèves » et « Fichier élèves », qui jusqu'à présent ont une existence propre.

La Commission nationale voudrait relever d'emblée qu'elle reconnait l'intérêt d'un tel traitement en vue notamment d'une meilleure planification et évaluation de la qualité de l'enseignement. Toutefois, elle relève que l'accroissement du nombre de données collectées et l'augmentation de transferts de données entre les différents protagonistes soulèvent par nature des interrogations quant à la préservation des libertés et droits fondamentaux, particulièrement la protection de la vie privée et des données à caractère personnel des élèves et de leurs représentants légaux. 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.

Remarques préliminaires

Pour qu'une atteinte au droit au respect de la vie privée et familiale soit légitime, elle doit être conforme à l'article 8 paragraphe (2) de la Convention européenne des droits de l'homme et interprétée à la lumière de la jurisprudence de Strasbourg : d'une part, elle doit être *« prévue par la loi » et, d'autre part, être « nécessaire, dans une société démocratique, 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 »*. À plusieurs reprises, la Cour de Strasbourg a précisé que la loi autorisant l'ingérence devait être accessible

et prévisible[15]. Selon la Cour, une norme est prévisible dans la mesure où elle est rédigée avec une précision telle que toute personne puisse sur sa base régler sa conduite.

Dès lors, afin de contribuer à cette volonté de transparence et de prévisibilité, la Commission nationale est d'avis qu'un règlement grand-ducal devra aller de pair avec l'élaboration d'un projet de loi. Celui-ci devra 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. Quant à l'exploitation et au traitement même des données, cela relève davantage de modalités et pourra faire l'objet d'un règlement grand-ducal.

La Commission nationale note que l'article 2 du texte en projet prend en considération le règlement grand-ducal du 20 juin 2001 autorisant la création et l'exploitation d'une banque de données nominatives relative aux élèves alors que l'article 16 l'abroge explicitement. La Commission nationale recommande de ne pas faire de référence inutile à ce règlement grand-ducal, ce qui serait susceptible de prêter à confusion.

Ci-après, nous passerons en revue les différents éléments touchant à la protection des données à caractère personnel qu'il serait souhaitable de voir précisés dans les futurs textes. Pour ce faire, la Commission nationale appuiera son avis sur les éléments déjà présents dans l'avant-projet de règlement grand-ducal.

1. Les finalités du traitement

Parmi les bases légales[16] sur lesquelles le texte en projet entend se fonder, figure l'article 20 de la loi du 6 février 2009 relative à l'obligation scolaire. Cette disposition prévoit l'échange, entre l'administration de l'éducation nationale, les établissements scolaires et les autorités communales, de différentes données nécessaires pour parvenir aux finalités suivantes :

- le contrôle du respect de l'obligation scolaire ;

- le contrôle de l'assiduité des élèves fréquentant l'enseignement fondamental ou l'enseignement postprimaire ;

- le contrôle de l'accomplissement des missions de l'École en général.

Par ailleurs, d'autres finalités découlent des deux autres bases légales, à savoir l'évaluation des enseignements des lycées et lycées techniques et l'organisation de l'enseignement fondamental, notamment à travers la réalisation d'analyses et de recherches statistiques.

En ce qui concerne les acteurs de ces échanges, la Commission nationale note qu'en ajoutant, en son article 7, des personnes qu'il désigne comme « *tiers* », l'avant-projet de règlement grand-ducal prévoit davantage d'acteurs que les seuls établissements scolaires, administration de l'éducation nationale et autorités communales initialement prévus par la loi.

Par conséquent, la Commission nationale estime que toutes les finalités du traitement ainsi que la participation à la collecte et au traitement des données par des tiers autres que ceux visés à l'article 20 de la loi du 6 février 2009 relative à l'obligation scolaire ainsi que les échanges de données avec ces derniers devront figurer dans la loi. En ce qui concerne plus particulièrement la finalité statistique, nous renvoyons au point 7.

2. Les notions

2.1. L'administrateur

Le texte sous avis traite, à l'article 1er lettre (m) ainsi qu'à l'article 5, du rôle joué par la personne qualifiée d' « administrateur ».

En lui attribuant la prérogative d'accorder aux utilisateurs autorisés l'accès aux données à caractère personnel enregistrées, la Commission nationale reconnait la volonté des rédacteurs de l'avant-projet

[15] Groupe de travail « article 29 » sur la protection des données, document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), 15 février 2007, p. 14.

[16] Article 20 de la loi du 6 février 2009 relative à l'obligation scolaire, Mémorial A n°187 du 3 septembre 2009, p. 2980 ; Article 39 de la loi du 6 février 2009 portant organisation de l'enseignement fondamental, Mémorial A n°187 du 3 septembre 2009, p. 2988 ; Article 11 de la loi du 25 juin 2004 portant organisation des lycées et lycées techniques, Mémorial A n°126 du 16 juillet 2004, p. 1857.

de règlement grand-ducal d'en faire une personne privilégiée, possédant davantage de pouvoirs qu'un utilisateur lambda. Toutefois, elle n'est pas d'avis qu'un administrateur devrait détenir les mêmes pouvoirs que ceux conférés au Ministre, comme le laisse pourtant entendre l'article 5 du texte en projet. Dès lors, elle recommande qu'une délégation de pouvoir soit formalisée au sein d'une décision ministérielle, suffisamment précise pour déterminer le périmètre d'utilisation. L'article 5 du texte pourrait être complété de la manière suivante :

> *« Les données à caractère personnel enregistrées et traitées ne sont accessibles qu'aux utilisateurs autorisés soit par le membre du Gouvernement ayant l'éducation nationale dans ses attributions, appelé par la suite « le ministre », soit par un administrateur tel que défini à l'article 1, agissant dans le cadre de sa délégation de pouvoir. (…) ».*

De plus, la Commission nationale se demande s'il ne serait pas opportun de préciser, dans les commentaires des articles, qu'il ne s'agit pas forcement d'un informaticien. En effet, dans le cas présent, la notion d'administrateur n'est pas celle utilisée dans la terminologie informatique pour viser l'administrateur réseaux. La définition d' « administrateur » pourrait être précisée comme suit :

> *« Une personne physique ayant tous les droits sur la base de données, notamment le droit de gestion et d'attribution des droits d'accès et des ressources systèmes et les droits d'accès en lecture et écriture au contenu de la base ».*

2.2. Les tiers

Au vu des prérogatives qui sont conférées aux « tiers » par les rédacteurs de l'avant-projet de règlement grand-ducal, une définition claire et précise de cette notion s'impose.

Par la loi du 2 août 2002, le législateur a défini la notion de « tiers » en matière de protection des données à caractère personnel. Au regard des implications que possède le traitement dans ce domaine, la Commission nationale propose de reprendre la définition de ladite loi en l'adaptant de la manière suivante :

> *« La personne physique ou morale, l'autorité publique, le service ou tout autre organisme autre que la personne concernée, le ministère et les personnes qui, placés sous l'autorité directe du ministère, sont habilités à traiter les données ».*

2.3. L'échange de données

L'article 1er du projet de règlement grand-ducal propose en ses paragraphes (j) et (n) deux définitions différentes de la notion d' *« échange de données »*. La Commission nationale estime souhaitable de définir cette notion au sein d'une seule et même disposition.

De plus, les rédacteurs du texte en projet semblent vouloir viser ce que la loi du 2 août 2002 entend par *« traitement de données à caractère personnel »*. Dès lors, la Commission nationale recommande d'utiliser les termes et la définition établie à l'article 2 lettre (r) de la loi du 2 août 2002.

3. Les personnes concernées par le traitement

La Commission nationale note que les personnes concernées par le traitement sont les élèves tels que définis à l'article 1er lettre (h) de l'avant-projet de règlement grand-ducal ainsi que les personnes exerçant la responsabilité parentale sur ceux-ci.

4. Les données à caractère personnel

4.1. Remarques préliminaires

Aux termes de l'article 3 du texte en projet, les rédacteurs ont établi des catégories de données nécessaires pour permettre le suivi des parcours scolaires. Il s'agit de *« données relatives à l'inscription, l'admission, la fréquentation, l'identification et l'authentification, la répartition dans les classes, le suivi des effectifs, l'acquisition des compétences des élèves ainsi que le suivi de leur parcours scolaire »*. Afin d'assurer une certaine sécurité juridique, la Commission nationale préconise que ces catégories qui déterminent la nature des données collectées soient inscrites dans une loi.

L'article 4 du texte en projet, quant à lui, énumère concrètement les données enregistrées dans la base de données. Bien que cette liste soit plus importante que celle prévue par le règlement grand-ducal du 20 juin 2001, le législateur, en employant les termes « *au plus* », précise qu'il s'agit là d'une liste exhaustive. Néanmoins, la Commission nationale conseille de déterminer cette liste au sein d'un règlement grand-ducal et ce, dans un souci de flexibilité, pour permettre une évolution ultérieur de cette liste tout en respectant la nature des données telle que définie dans la loi. En vertu de l'article 32 de la loi du 2 août 2002, la Commission nationale sera compétente pour apprécier la conformité de cette liste au prescrit de ladite loi.

4.2. L'origine des données à caractère personnel

Les chapitres III et V de l'avant-projet de règlement grand-ducal concernant tous deux la collecte (l'origine) des données, la Commission nationale suggère de les rassembler en un seul et même chapitre.

Les dispositions de ces chapitres ne sont cependant que succinctes quant à l'origine des données. En particulier, il n'est pas précisé quelles données sont obtenues auprès de quels tiers fournisseurs visés au chapitre V du texte en projet.

En outre, l'avant-projet de règlement grand-ducal ne donne pas d'informations précises quant à l'organisation concrète des transferts informatiques de données alimentant la base de données des élèves. Il ne fait que s'exprimer vaguement sur le sujet à l'article 15 en marquant une préférence pour une interconnexion entre systèmes informatiques ou un transfert par voie électronique. Dès lors, en l'absence de précisions sur la façon dont cette communication ou ce partage de données sera implémenté en pratique ou sur l'architecture informatique choisie, la Commission nationale part de l'hypothèse, dans le présent avis, que la collecte de certaines données aura lieu dans le cadre d'une interconnexion de données.

Les commentaires que la Commission nationale formule ci-après s'avèrent d'ailleurs également justifiés et transposables à l'hypothèse de communications ou de partages de données autres que sous forme d'interconnexion.

Conformément à l'article 16 paragraphe (1) de la loi du 2 août 2002, l'interconnexion peut valablement être autorisée par voie légale. Dans ce cas, il résulte des travaux parlementaires relatifs au projet de loi ayant mené à la loi du 2 août 2002 que « *l'élaboration de textes législatifs ou réglementaires autorisant une interconnexion de données devraient s'inspirer de la ratio des dispositions de l'article 16* »[17].

Or, à la lecture de l'avant-projet de règlement grand-ducal, on constate que ce dernier n'arrête ou ne précise pas les critères de délimitation, les conditions et les restrictions auxquelles l'éventuelle interconnexion doit se conformer. La Commission nationale est cependant d'avis que la future législation devrait prévoir et fixer des critères et conditions au sens de l'article 16 de la loi du 2 août 2002.

Ainsi, la finalité poursuivie par l'interconnexion se doit de respecter les quatre conditions cumulatives établies par le paragraphe (2) de l'article 16, à savoir 1) l'interconnexion doit permettre d'atteindre des objectifs légaux ou statutaires présentant un intérêt légitime pour les responsables du traitement, 2) elle ne peut entraîner de discriminations ou de réduction de droits, libertés et garanties pour les personnes concernées, 3) elle doit être assortie de mesures de sécurité appropriées et 4) elle doit tenir compte du type de données faisant l'objet de l'interconnexion.

De plus, aux termes du paragraphe (3) de l'article 16, un éventuel secret professionnel auquel peut être tenu le responsable du traitement ne peut être mis à mal par l'interconnexion des données.

En vertu de la même disposition, « *l'interconnexion n'est autorisée que dans le respect des finalités identiques ou liées (…)* ». Le législateur a voulu ainsi renvoyer à la notion de compatibilité des finalités des traitements à interconnecter.

Se pose dès lors la question de savoir si les finalités du fichier des élèves sont compatibles avec les finalités pour lesquelles les données ont été initialement collectées par les tiers fournisseurs.

[17] Doc. Parl. n° 4735/13, p.30.

La notion de « compatibilité » n'est pas définie par la loi. Le critère de compatibilité est lié à l'un des principes majeurs de la législation en matière de protection des données à caractère personnel, à savoir la transparence des traitements des données à l'égard des personnes concernées par les données[18].

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

À noter que pour certains tiers fournisseurs de données, une communication ou un transfert de données vers la base de données des élèves peut être prévu dans une autre disposition légale régissant l'organisme fournisseur de données et ses missions. Dans ce cas, la finalité recherchée par le tiers qui fournit les données pourra légitimement découler de ce texte légal.

Enfin, la Commission nationale estime utile qu'une loi vienne préciser auprès de qui sont collectées les données, du moins pour ce qui est des données qui ne sont pas issues des fichiers du Ministère, des établissements scolaires ou du Registre National des Personnes Physiques et Morales du Centre des technologies de l'information de l'État (telles que les informations relatives à la langue habituellement parlée en famille, la date d'arrivée au Grand-Duché de Luxembourg et la catégorie socioprofessionnelle des personnes exerçant la responsabilité parentale). Certaines données sont-elles, le cas échéant, collectées directement auprès des élèves ou de leurs représentants légaux ? Si tel est le cas, la Commission nationale recommande de compléter la disposition comme suit :

> *« Pour le surplus, les données proviendront des questionnaires complétés par les élèves ou leurs représentants légaux ».*

En tout état de cause, la Commission nationale est d'avis que, pour permettre une vérification du caractère légitime, compatible et non excessif par rapport aux finalités du fournisseur et de son fichier dont elles proviennent, il faudrait indiquer plus précisément au sein du règlement grand-ducal quel organisme fournit quelles données. Ceci est d'autant plus important si la collecte des données se fait dans le cadre d'une interconnexion de données.

L'obligation de veiller à l'exactitude des données et, si nécessaire, à leurs mises à jour, pèse sur chaque responsable du traitement[19]. Si, dans son article 13, l'avant-projet de règlement grand-ducal mentionne précisément l'obligation pour les tiers fournisseurs de vérifier l'exactitude des données présentes dans leur fichier, il en est de même pour le Ministère. Comme l'a justement fait remarquer le Groupe de travail « article 29 » sur la protection des données, ceci est d'autant plus important lorsqu'il s'agit de données relatives à un enfant : « L'enfant étant en évolution constante, les responsables du traitement des données devront être particulièrement attentifs à l'obligation de mise à jour des données à caractère personnel »[20].

4.3. La nature des données à caractère personnel

La Commission nationale note avec satisfaction que le texte contient, à l'article 4, une énumération exhaustive des données contenues dans le fichier des élèves

En ce qui concerne les informations relatives à la catégorie socioprofessionnelle des personnes exerçant la responsabilité parentale, la Commission nationale se demande si cette notion n'est pas trop large et imprécise.

En effet, les rédacteurs du texte en projet n'ont pas défini cette notion qui pourtant peut inclure plusieurs éléments :

- niveau de revenu des représentants légaux ;
- niveau de formation des représentants légaux ;

[18] De Terwangne, C., la nouvelle loi belge de protection des données à caractère personnel, in La protection de la vie privée dans la société de l'information, coll. Cahier des Sciences morales et politiques, pp. 91-109.

[19] Article 4 paragraphe (1) lettre (c) de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, Mémorial A n°91 du 13 août 2002, p. 1837.18

[20] Groupe de travail « article 29 » sur la protection des données, document de travail 1/2008 sur la protection des données à caractère personnel de l'enfant (principes généraux et cas particulier des écoles), 18 février 2008, p. 8.

- activités professionnelles exercées par les représentants légaux ;
- l'état d'inactivité des représentants légaux pour raison de chômage, d'incapacité de travail, d'invalidité ;
- etc.

L'intention d'englober les informations relatives à la catégorie socioprofessionnelle renferme le danger que celles-ci soient trop détaillées pour figurer dans une base de données conservée durant une longue période et accessible à un nombre important de personnes. L'enregistrement de telles informations détaillées et qui plus est possédant une connotation sociale importante, n'est pas nécessaire et serait à considérer comme disproportionnée par rapport aux finalités assignées à la base de données.

Toutefois, elle comprend parfaitement le souci légitime et l'utilité de disposer d'informations plus détaillées pour réaliser des études en conformité avec les finalités du traitement. Il serait dès lors préférable de collecter ponctuellement, dans le cadre d'études statistiques, des informations détaillées sur la catégorie socioprofessionnelle des personnes exerçant la responsabilité parentale, le cas échéant rendues anonymes et accessibles à un nombre restreint de personnes plutôt que d'enregistrer ces informations dans un fichier ayant une durée de conservation très longue.

À noter qu'en ce qui concerne les données d'identification et familiales, le législateur français a pris position dans le cadre de l'application informatique appelée « Base élèves ». L'objectif poursuivi par cette application est de permettre la gestion tant administrative que pédagogique des élèves fréquentant une école maternelle ou primaire. Suite à de nombreuses plaintes de parents d'élèves, le Ministère de l'Éducation Nationale français a retiré du périmètre des données collectées, les champs concernant la catégorie socioprofessionnelle des parents, l'origine, la nationalité et la situation familiale de l'élève ainsi que la langue parlée chez lui, et ce, notamment afin d'éviter que ces renseignements ne soient détournés de leurs finalités initiales en vue d'aider à repérer les familles sans-papiers. Ainsi, l'arrêté du 20 octobre 2008[21] mettant en place la « Base élèves » pour les élèves du premier degré prévoit une liste plus restreinte de données récoltées que celle initialement prévue.

Au stade actuel, il est difficile d'apprécier, conformément à l'article 4 paragraphe (1) lettre (b) de la loi du 2 août 2002, le caractère adéquat, pertinent et non excessif de certaines données envisagées dans l'avant-projet.

En effet, plusieurs questions restent ouvertes, comme par exemple :

- à quelle fréquence la photo doit-elle être récoltée?
- ces photos seront-elles archivées ou effacées chaque année ?
- quelle différence doit-on faire entre la notion de « pays de naissance » et celle de « pays d'origine » ? Quelle est la nécessité d'en disposer ?

5. L'accès aux données à caractère personnel

Le nombre important de données en jeu et le caractère sensible de certaines rendent la réglementation de leur accès nécessaire. La Commission nationale n'émet aucun doute quant à l'intérêt légitime des utilisateurs autorisés d'accéder aux données mais se demande si cet accès n'est pas trop large et donc susceptible de faciliter des abus. Dès lors, elle est d'avis que cela ne peut faire l'objet d'un accès global à l'ensemble des données contenues dans la base de données.

Ainsi, en vertu des principes de proportionnalité et de nécessité établis à l'article 4 de la loi modifiée du 2 août 2002, l'accès ne pourra être autorisé que pour les seules données nécessaires à l'exécution des missions dédiées aux utilisateurs autorisés.

La Commission nationale recommande donc d'énumérer pour chaque groupe d'utilisateurs, les données auxquelles ils pourront avoir accès. En exécution de l'article 32 de la loi du 2 août 2002, cette liste pourra

[21] Arrêté du 20 octobre 2008 portant création d'un traitement automatisé de données à caractère personnel relatif au pilotage et à la gestion des élèves de l'enseignement du premier degré, J.O. n° 256 du 1 novembre 2008 - texte n° 19.

faire l'objet d'une appréciation du respect des principes de nécessité et de proportionnalité par la Commission nationale.

Toutefois, la Commission nationale est rassurée que, dans le souci de contrer d'éventuels abus, tout accès est répertorié par un administrateur en spécifiant pour chaque utilisateur le type d'accès aux données.

L'article 11 du texte en projet est appelé à restreindre le cercle des personnes ayant accès aux données. La Commission nationale préconise toutefois d'ajouter la précision suivante :

> « *Seuls les agents du ministère désignés nommément par arrêté ministériel sont autorisés à communiquer ou à transférer les données, dans la limite des prévisions des articles 9 et 10* ».

6. La communication de données à caractère personnel à des tiers

L'avant-projet de règlement grand-ducal ne donne également aucune précision quant à l'organisation concrète des transferts informatiques à partir de la base de données. Tout comme la collecte des données, la communication à des tiers de données à caractère personnel issues de la base de données peut avoir lieu ou non sous la forme d'une interconnexion. Dès lors, les réflexions décrites au point 4.2. trouvent à s'appliquer. L'article 15 de l'avant-projet de règlement grand-ducal ne précisant pas s'il concerne la collecte des données ou leurs communications à des tiers, la Commission nationale part de nouveau de l'hypothèse que ce transfert ultérieur se fait dans le cadre d'une interconnexion.

Comme le préconise le Conseil d'État, l'interconnexion de données étant considérée comme une opération délicate, celle-ci doit être entourée d'un maximum de garanties[22]. En conséquence, la Commission nationale suggère, d'une part, d'établir 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 propose qu'au sein d'un règlement grand-ducal, pour une question de flexibilité, soient énumérées les données qui feront l'objet d'une communication ou d'un partage ainsi que leurs destinataires respectifs, et ce, en vue de pouvoir apprécier la compatibilité des finalités de la base de données avec celles du traitement opéré par après par les destinataires. Ainsi, les rédacteurs pourront s'inspirer du prescrit de l'article 138 de la loi du 29 août 2008 portant sur la libre circulation des personnes et immigration et de son règlement grand-ducal d'exécution, 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.

7. Le traitement de données à caractère personnel à des fins de recherches statistiques ou scientifiques

7.1. Le traitement ultérieur de données à des fins de recherches statistiques ou scientifiques par des tiers

Conformément aux textes européens[23], l'article 10 du texte en projet exige que les données soient rendues anonymes.

La Commission nationale recommande de spécifier clairement les destinataires de l'article 9 de l'avant-projet de règlement grand-ducal auxquels l'article 10 dudit texte s'applique, tels que l'Inspection Générale des Finances, le CEPS, le STATEC ou l'Université du Luxembourg. En effet, la Commission nationale propose que ces destinataires ne figurent plus à l'article 9, qui parle de « *données à caractère personnel* », c'est-à-dire des données concernant une personne identifiée ou identifiable selon l'article 2 lettre (e) de la loi du 2

[22] Avis du Conseil d'État du 30 janvier 2007 relatif au projet de loi n° 5554, p. 11.

[23] Article 8.1. de la Recommandation n° R(97)18 du Conseil de l'Europe concernant la protection des données à caractère personnel collectées et traitées à des fins statistiques.

août 2002, alors que ces destinataires ont vocation à recevoir uniquement des données anonymisées en vertu de l'article 10.

À noter que l'article 10 ne préjudicie en rien la possibilité pour d'autres tiers de recevoir des données anonymes s'ils souhaitent effectuer des statistiques conformément à l'article 4 paragraphe (2) de la loi du 2 août 2002.

7.2. Le traitement de données à des fins de recherches statistiques ou scientifiques par le Ministère lui-même

Dans la mesure du possible, lorsque le Ministère souhaite effectuer lui-même une recherche statistique ou scientifique à partir de données issues de la base de données des élèves, il ne devrait le faire qu'à l'aide de données préalablement anonymisées.

Néanmoins, si le recours à des données anonymes ne permet pas d'atteindre les finalités 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. Pour ce faire, un fichier indépendant, contenant ces données, pourra être créé à côté de la base de données des élèves.

Par ailleurs, la Commission nationale souhaite attirer l'attention sur le fait qu'il existe des procédés d'anonymisation, tel que la technique du hachage avec clé secrète, permettant de suivre des personnes sur un certain laps de temps sans avoir à connaître leur identité véritable.

8 Les droits des personnes concernées

L'avant-projet de règlement grand-ducal, en son article 8, rappelle l'article 26 de la loi du 2 août 2002, à savoir le droit pour toute personne d'être informée notamment des finalités pour lesquelles ses données sont utilisées. Il nous paraît qu'outre une information précise sur les finalités, il serait indiqué de faire référence également à l'identité du responsable du traitement, aux destinataires respectivement groupes de destinataires auxquelles les données sont communiquées ainsi qu'au droit d'accès et de rectification et au droit d'opposition.

9. Les mesures de sécurité

Le droit de la protection des données s'appuie sur l'idée fondamentale que le responsable du traitement doit s'assurer que les données à caractère personnel qu'il détient sont traitées 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.

La Commission nationale se réjouit de voir intégré au sein du règlement grand-ducal un chapitre particulier traitant du sujet mais souhaite toutefois formuler quelques remarques.

Tout d'abord, elle est d'avis que le chapitre VI devrait subir une refonte dans un souci de clarté, en modifiant d'une part son intitulé de la manière suivante : « Confidentialité et sécurité des données » et, d'autre part, en distinguant bien les flux, c'est-à-dire les situations dans lesquelles les données sont fournies de celles où elles sont appelées à être communiquées à certains tiers.

Ensuite, dans l'optique d'une modification de la notion d' « *échange de données* » en « traitement de données à caractère personnel », la Commission nationale suggère de modifier l'article 14 de la manière suivante, en faisant également référence au principe de finalité :

> « *Les personnes qui sont en droit d'accéder aux données à caractère personnel traitent seulement les données qui sont indispensables à la réalisation de la finalité à laquelle il participe. Elles sont tenues à la confidentialité des données traitées* ».

Quant à l'article 15, la Commission nationale lui propose la tournure suivante :

> « *Les données sont échangées dans la mesure du possible directement par interconnexion entre systèmes informatiques ou par voie électronique.*

Le responsable du traitement prend toutes les mesures pour assurer la confidentialité, l'intégrité, la disponibilité et la traçabilité des données, conformément aux articles 21 à 23 de la loi du 2 août 2002 ».

Afin de garantir le traitement en cause, la Commission nationale suggère également de préciser les mesures techniques d'accessibilité telles que le journalisme, la traçabilité ou le recours à un login, ainsi que de spécifier les mesures organisationnelles. Ainsi, à l'instar d'autres lois[24], il pourrait être ajouté l'alinéa suivant :

« *Le système informatique par lequel l'accès direct est opéré doit être aménagé de sorte que les informations relatives à la personne bénéficiant de la communication, les informations communiquées, la date, l'heure ainsi que le motif précis de la communication puissent être retracés* ».

10. La durée de conservation

L'article 4 paragraphe (1) de la loi 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* ».

Le texte en projet entend autoriser la conservation des données en question durant une période de cent ans. La Commission nationale considère cette durée comme difficilement justifiable au vu des finalités exposées, à savoir le suivi de la scolarité des élèves. De plus, une saine limitation de la durée de conservation est une garantie supplémentaire des libertés et droits des personnes concernées.

C'est pourquoi la Commission nationale estime qu'une période de conservation de dix ans après la fin du cursus scolaire devrait être suffisante. Au-delà, les données devront être anonymisées de façon irréversible.

En limitant la conservation des données à dix ans après le cursus scolaire, la Commission nationale considère que les finalités du fichier pourront être atteintes pour les personnes qui, le cas échéant, auraient repris leurs études après les avoir interrompues.

Il est à noter d'ailleurs que dans un avis récent[25], le Conseil d'Etat français a eu à se prononcer sur une question similaire. La Haute Juridiction a jugé excessif une durée de conservation totale de 35 ans (à partir de l'inscription en maternelle) prévue dans un projet de texte.

Une fois la durée de conservation maximale prémentionnée révolue, les données devront donc faire l'objet d'une anonymisation totale et irréversible de nature à rendre impossible l'identification des personnes concernées. Les données anonymisées de façon irréversible qui ne sont plus liées à une personne physique identifiée ou identifiable et, qui dès lors ne sont plus considérées comme des données à caractère personnel tombant sous le couvert de la loi du 2 août 2002[26], pourront être conservées aussi longtemps que souhaité.

À noter que le présent avis ne préjudicie en rien l'existence d'un archivage des informations relatives aux diplômes qui poursuit une finalité autre que celles attribuées à la base de données, à savoir une finalité de certification.

Ainsi décidé à Luxembourg en date du 26 juillet 2010.

La Commission nationale pour la protection des données

Gérard Lommel	Président
Pierre Weimerskirch	Membre effectif
Thierry Lallemang	Membre effectif

[24] Loi du 29 août 2008 portant sur la libre circulation des personnes et l'immigration, Mémorial A n°138 du 10 septembre 2008, pp.

[25] Conseil d'État français, 19 juillet 2010, no 334014, M. F… et Mme C…2023-2052.

[26] Cf. article 2 lettre (e) de la loi du 2 août 2002.

Avis relatif au projet de loi n°6172 portant réforme du mariage et de l'adoption et modifiant certaines dispositions légales

Délibération n°269/2010 du 24 septembre 2010

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 31 juillet 2010, Monsieur le Ministre de la Justice a invité la Commission nationale à se prononcer au sujet du projet de loi n° 6172 portant réforme du mariage et de l'adoption et modifiant : a) le Code civil, b) le Nouveau Code de procédure civile, c) le Code d'instruction criminelle, d) la loi modifiée du 16 avril 1979 fixant le statut général des fonctionnaires d'Etat, e) la loi modifiée du 24 décembre 1985 fixant le statut général des fonctionnaires communaux, f) la loi modifiée du 14 mars 1988 portant création d'un congé d'accueil pour les salariés du secteur privé, g) la loi du 23 octobre 2008 sur la nationalité luxembourgeoise (ci-après : le projet de loi).

Suivant l'exposé des motifs, la loi projetée permettra d'appliquer de manière équivalente tant aux mariages des couples de sexe différent qu'aux couples de même sexe, l'ensemble des droits et obligations issus du mariage, les règles applicables en matière de dissolution du mariage ou encore les dispositions en matière de donations ou de successions.

Dans une deuxième partie, le projet de loi propose pour l'essentiel d'ouvrir les portes de l'adoption simple, que ce soit par une procédure nationale ou internationale, aux couples de même sexe, qu'ils vivent sous le régime du mariage ou celui du partenariat enregistré.

Par ailleurs, le projet de loi introduit une nouvelle disposition qui soumet la recevabilité de toutes les demandes d'adoption internationale auprès des tribunaux luxembourgeois au traitement préalable du service de l'adoption du Ministère de la Famille. Cette nouvelle disposition entraîne nécessairement la tenue d'un fichier afférent auprès du Ministère de la Famille.

Sauf exceptions, le traitement de données relatives à la santé ou à la vie sexuelle des personnes concernées n'est pas permis. La Commission nationale est donc à s'interroger si le traitement effectué par le Ministère de la Famille ne soulève pas de problèmes au regard de l'article 6 de la loi modifiée du 2 août 2002 alors que ce traitement concernera tant les couples de sexe différent que les couples du même sexe.

Après l'entrée en vigueur de la loi sous examen, cette question se posera de façon plus générale alors que les fichiers (publics ou privés) reprenant l'état civil d'un couple contiendront nécessairement des données à caractère personnel susceptibles de révéler l'orientation sexuelle des personnes concernées.

Or, la Commission nationale considère qu'en ouvrant l'institution du mariage aux couples de même sexe, il devient inévitable que cette information figurera dans de nombreux fichiers publics ou privés.

Pour le surplus, la Commission nationale n'a pas d'observation à formuler au regard en particulier de la protection des données à caractère personnel.

Ainsi décidé à Luxembourg en date du 24 septembre 2010.

La Commission nationale pour la protection des données

Gérard Lommel	Président
Pierre Weimerskirch	Membre effectif
Thierry Lallemang	Membre effectif

Interdiction à la société GOOGLE INC. de collecter des données personnelles et notamment de capter des images d'habitations à moins de prendre l'engagement de se conformer aux conditions posées

Délibération n°329/2010 du 5 novembre 2010

Considérant que la presse se fait l'écho de déclarations d'une porte-parole du département Presse de Google Benelux suivant lesquelles Google entendrait ne pas prendre en considération d'éventuelles oppositions à la publication d'images de leur habitation lui adressées préalablement à la mise en service en ligne de la fonction « Streetview » pour le Grand-Duché sur Google Maps.

Google invite les résidents luxembourgeois à se servir exclusivement de la fonctionnalité électronique mise à disposition pour s'opposer ou signaler en ligne des images problématiques lors de la navigation sur Internet.

Vu les articles 4, 5, 30 et 33 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

L'article 4, paragraphe 1er dispose que « *le responsable du traitement doit s'assurer que les données qu'il traite le sont loyalement et licitement, et notamment que ces données sont :*

> *(a) collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités* »

La condition de légitimité invoquée par Google Inc. est celle mentionnée à l'article 5, premier paragraphe, lettre (d) qui prévoit que « *le traitement des données ne peut être effectué que 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 et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er* ».

Dans sa correspondance avec Google, notamment la lettre adressée le 3 septembre 2010 à Google Inc., ayant son siège à Mountain View, CA/USA, à son représentant à Luxembourg Maître Gary Cywie, désigné en application de l'article 3, paragraphe 2, dernier alinéa, et à Google Netherlands BV, la Commission nationale a précisé les conditions qui doivent être réunies pour que le traitement réponde aux exigences légales.

Considérant que la loi prévoit que la Commission nationale peut prononcer des sanctions administratives à l'égard des responsables de traitement : l'article 33 paragraphe (1) lettre (c) de la loi prévoit ainsi qu'elle peut « *interdire temporairement ou définitivement un traitement contraire aux dispositions de (…) la loi ou de ses règlements d'exécution* ».

A défaut d'assurances sur le respect des oppositions préalables, la poursuite de la collecte de données et notamment du captage d'images d'habitations porte atteinte aux libertés et droits fondamentaux des personnes concernées.

Dès lors, la Commission nationale estime nécessaire de prononcer une sanction administrative en application de l'article 33 paragraphe (1) lettre (c) de la loi.

***

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

- interdit à la société Google Inc., représentée au Grand-Duché de Luxembourg par Maître Gary Cywie, de poursuivre le traitement faisant l'objet de la notification (T6850 Google Inc.) du 10.2.2009, aussi longtemps qu'elle ne respecte pas les oppositions exprimées préalablement à la mise en ligne des images par des personnes concernées par son service Streetview pour le Luxembourg.

Ainsi décidé à Luxembourg en date du 5 novembre 2010.

La Commission nationale pour la protection des données

Gérard Lommel	Président
Pierre Weimerskirch	Membre effectif
Thierry Lallemang	Membre effectif

Indication des voies de recours

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

Avis relatif au projet de loi n° 6243 portant modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

Délibération n°330/2010 du 10 novembre 2010

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 14 septembre 2010, Monsieur le Ministre des Communications et des Médias a invité la Commission nationale à se prononcer au sujet du projet de loi portant modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

L'objet central de ce dernier consiste dans la transposition en droit luxembourgeois de la directive 2009/136/CE qui fait partie du nouveau « paquet télécom » par lequel le droit communautaire a été adapté à l'évolution technologique rapide du secteur qui s'est encore accélérée depuis l'adoption de la précédente directive de 2002. En outre, la directive a voulu consolider l'indépendance des autorités nationales de régulation du secteur des télécommunications et le principe d'un Internet ouvert et neutre tout en renforçant la protection des consommateurs par des garanties nouvelles portant entre autres sur le respect de leur vie privée.

La principale innovation que le projet de loi se propose d'introduire par un ajout à l'article 3 de la loi modifiée du 30 mai 2005 porte sur l'obligation pesant dorénavant sur les fournisseurs de services de communications électroniques accessibles au public d'avertir immédiatement la Commission nationale pour la protection des données 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 au niveau de la protection de leur vie privée et des données les concernant.

L'idée d'une telle notification publique obligatoire est reprise de la législation de certains Etats des Etats-Unis d'Amérique et s'est avérée constituer une mesure efficace dont l'intérêt dépasse celui de l'avertissement des personnes exposées en vue de leur permettre de prévenir ou d'atténuer les effets risquant de découler de la rupture de la confidentialité et sécurité de leurs données.

De telles dispositions promettent en effet d'induire une vigilance accrue de la part des responsables des traitements de données, de promouvoir l'amélioration continue des procédures internes et de favoriser l'investissement dans des ressources techniques visant à assurer la sécurité des données à caractère personnel et à prévenir des accès non autorisés et pannes susceptibles de ternir l'image de marque de l'entreprise ou de l'organisation en question et de lui faire perdre la confiance de ses utilisateurs et clients.

A ce titre, il est remarquable que les débats au Parlement européen ont abouti à l'insertion dans le libellé final du considérant N° 59 de la directive d'une déclaration d'intention de voir étendre à l'avenir à d'autres secteurs économiques l'exigence explicite de notification des incidents de sécurité ayant conduit à la violation de données à caractère personnel.

Le texte dudit considérant charge la Commission européenne d'examiner la législation communautaire et de prendre les mesures appropriées pour promouvoir l'application dans les autres secteurs de telles règles favorisant une attention accrue des responsables des traitements à leur obligation de mettre en œuvre toutes les mesures nécessaires sur le plan technique et organisationnel pour prévenir des pertes, des vols, des

divulgations ou des utilisations abusives de données personnelles.

L'introduction dans la loi modifiée du 30 mai 2005 de cette obligation de signalement des violations de sécurité/confidentialité des données à caractère personnel constitue donc une avancée majeure sur le plan de la protection de la vie privée dans le secteur des communications électroniques.

Le texte actuel de l'article 3 de la loi est complété par les dispositions afférentes reprises de la directive 2009/136/CE. Un rôle important reviendra dorénavant à notre Commission nationale dans la mise en œuvre des nouvelles règles. Rappelant qu'aux termes des articles 21 à 23 et 32 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel elle assume déjà parmi ses missions générales la charge de vérifier l'application de mesures appropriées visant à assurer la confidentialité et la sécurité des données personnelles soumises à traitement par les acteurs de tous les secteurs de la vie socio-économique.

Dans le secteur des communications électroniques un suivi rigoureux sera désormais garanti par la nouvelle procédure de notification obligatoire.

Notons que la directive prend soin de préciser en son article 3, point 4, lettre b) in fine que « les autorités nationales compétentes sont habilitées à vérifier les mesures prises par les fournisseurs des services de communications électroniques accessibles au public, ainsi qu'à émettre des recommandations sur les meilleures pratiques concernant le degré de sécurité que ces mesures devraient atteindre ».

Dans ce domaine notre Commission nationale s'efforcera d'allier de façon non bureaucratique mais pragmatique et ouverte au dialogue constructif avec les acteurs concernés, guidance, contrôle et promotion d'une approche vigilante et anticipatrice (« Privacy by Design »).

Les ressources de la Commission nationale, en particulier au niveau de collaborateurs à compétence informatique et technologique, devront elles aussi évoluer de façon à lui permettre d'assumer convenablement ces nouvelles responsabilités.

Le projet de loi examiné présente encore deux innovations importantes. L'une d'entre elles découle directement de la transposition de la directive et a trait aux témoins de connexions sur Internet (généralement appelés « cookies ») et renforce les garanties de transparence et d'usage loyal de ces techniques qui se sont quasi généralisées avec l'évolution d'Internet. Les offres de services en ligne (souvent non payants) se servent de cette méthode pour personnaliser autant que possible la navigation de l'internaute et l'interaction avec lui (y compris le placement de publicités tenant compte de ses intérêts). L'exigence de loyauté et de transparence et la possibilité qui doit lui être offerte d'accepter ou de refuser le recours aux « cookies » s'étend aussi bien au placement sur le terminal de l'usager (stockage d'informations de connexion) qu'à l'accès ultérieur à ces témoins (informations stockées) par le site web d'origine et/ou par d'autres sites partenaires ou similaires.

Le projet de loi reprend fidèlement dans la loi luxembourgeoise le texte exact de l'article de la directive et du considérant afférent.

Cette démarche apparaît judicieuse et fondée parce qu'elle reprend à son compte l'adage raisonnable de bonne légistique « Toute la directive, rien que la directive », mais aussi parce que des négociations sont actuellement en cours sur le plan communautaire avec les principales entreprises multinationales du secteur sur les pratiques recommandables et les moyens techniques les plus conviviaux et efficaces pour atteindre les objectifs d'information appropriée et de choix laissé au consommateur/usager formulés par la directive.

Il s'est avéré que les notices compliquées sur les principes suivis en matière de « privacy » par les opérateurs de sites web et services sur Internet sont souvent trop longues, incompréhensibles et mal accessibles pour contribuer utilement à l'éclairage du choix de l'internaute et que ce dernier réagit souvent par impulsion.

Peut-être que la liberté de l'internaute de contrôler la collecte et l'usage des informations le concernant devra trouver des façons de s'exprimer plus modernes, simples, intuitives, qui tiennent compte des situations

où le visiteur d'un site web et l'usager de ces services a implicitement mais sans ambiguïté accepté la finalité du traitement de ses données (par opposition à celles où une information plus explicite est nécessaire pour un consentement éclairé).

Le législateur luxembourgeois est donc bien inspiré de reprendre mot par mot, comme le prévoit le projet de loi, le texte issu de la directive et de ne pas gêner la flexibilité évolutive par des dispositions spécifiques originales pour laisser les bonnes pratiques se dégager à travers les initiatives en cours de la Commission européenne et du groupe de l'article 29 de protection des données (cf. appel au secteur privé - réseaux publicitaires en ligne et concepteurs de navigateurs web - de développer des modalités pratiques appropriées[27]) en vue d'amener les principaux représentants du secteur en question à s'adapter aux exigences du droit européen.

Finalement, le projet de loi vient insérer un certain nombre de modifications et d'ajouts aux articles 4, 5 et 7 de la loi modifiée du 30 mai 2005 pour assurer l'accès de la Police et des Centres d'appels d'urgence aux données d'identification et de localisation des appelants et se propose d'abroger l'article 41 de la loi modifiée du 2 août 2002 qui n'a jamais donné lieu à une application effective en raison des difficultés techniques rencontrées par l'ILR dans sa mise en œuvre pratique.

Il s'est avéré entre-temps que le modèle, qui avait inspiré le législateur de 2002, n'est pratiqué à grande échelle que dans un seul Etat membre de l'Union européenne. Aussi les rédacteurs du projet de loi ont-ils opté pour remplacer ce système de stockage centralisé des données d'identification et de localisation des abonnés pour les besoins du recours en cas d'urgence par la Police grand-ducale et les services de secours par un système de transmission décentralisé au cas par cas aux opérateurs des numéros d'urgence (112, 113, etc.) des données d'identification et de localisation concernant les appelants. Les dispositions proposées reflètent les systèmes similaires pratiqués dans la plupart des autres pays européens.

Commentaire des articles du projet de loi :

Articles 1 (champ d'application) et 2 (définitions)

Les modifications proposées visent à aligner le texte de la loi sur celui résultant des adaptations opérées par la directive 2009/136/CE modifiant la directive 2002/58/CE relative aux dispositions spécifiques de protection des personnes à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques. Il s'agit d'une transposition littérale qui n'appelle pas d'observations.

Article 3 : Sécurité « du traitement »

L'ajout d'un troisième paragraphe qui reprend littéralement les paragraphes ajoutés à l'article correspondant de la directive (article 4 point 3) correspond à une transposition fidèle.

Le paragraphe 1 bis inséré sub b) au même article 4 de la directive relatif aux mesures de sécurité n'est toutefois pas énuméré dans les ajouts opérés par le projet de loi. Le commentaire des articles énonce qu'il s'agit d'une redite des principes généraux figurant déjà aux articles 22 et 23 de la loi générale sur la protection des données (loi modifiée du 2 août 2002) et justifie cette omission par la constatation qu'il ne s'agirait pas de dispositions ayant valeur normative.

Si on peut suivre les auteurs du projet de loi sur ce point, force est de constater que les auteurs de la directive ont vu une utilité suffisante pour les insérer dans la directive par souci de sécurité juridique et de précision quant aux prérogatives de l'autorité de contrôle dans l'application pratique.

Par ailleurs, le projet de loi omet également de transposer le point 4 premier alinéa ajouté par la directive à l'article 4 de la directive 2002/48. Notre Commission nationale estime qu'il serait préférable que la loi précise en transposition fidèle de la directive de 2009 que la CNPD a le pouvoir de prescrire des formats et d'édicter des instructions relatifs aux modalités pratiques de la notification des violations de données et à la procédure de transmission.

[27] WP 171/2010 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_fr.pdf

Le même paragraphe de la directive impose en outre aux Etats membres de mettre les autorités nationales compétentes en mesure de contrôler si les fournisseurs ont satisfait aux obligations de notification et d'infliger des sanctions appropriées si ces derniers ne s'y sont pas conformés.

La Commission nationale suggère dès lors de la doter à cet effet de la faculté de prononcer des amendes administratives et propose d'inscrire ce pouvoir de sanction pécuniaire à l'article 12 de la loi modifiée, article auquel il convient à son avis d'ajouter les deux alinéas prémentionnés formant le point 4 nouveau de l'article 4 de la directive modifiée que le texte actuel du projet de loi omet de transposer. Aucune des sanctions administratives prévues à l'article 33 de la loi modifiée du 2 août 2002 ne satisfait en effet aux exigences de la directive à l'exception de l'avertissement qui n'apparaît pas approprié en cas de non respect répété.

Le deuxième alinéa précise l'obligation pour chaque opérateur de réseau et fournisseur de services de communications électroniques, accessibles au public, de tenir un inventaire des violations de données à caractère personnel constatées et des mesures prises pour y remédier. Cette disposition constitue bien à notre avis une disposition substantielle nécessitant transposition.

Il est donc proposé d'ajouter ces deux points aux dispositions modificatives du projet de loi.

Article 4 : « Confidentialité des communications »

A l'article en question, après l'ajout de deux précisions mineures sub b) et d) visant à aligner le libellé avec la directive, le projet de loi prévoit l'insertion sub e) des deux paragraphes opérant transposition du paragraphe 3 de l'article 5 de la directive.

Le texte proposé reprend intégralement celui de la directive y compris deux phrases essentielles du considérant 66 afférent qui résultent du compromis textuel tel qu'entériné à l'occasion de l'adoption de la directive. S'il est vrai que malgré cette transposition littérale proposée, toute ambiguïté n'est pas écartée, quant aux modalités d'application pratiques, la Commission nationale approuve cependant la voie choisie par les rédacteurs du projet de loi qui se sont sagement abstenus de procéder à des adaptations nationales originales. Les modalités de bonne pratique à observer concrètement par les acteurs du secteur des communications sur Internet devront résulter du dialogue constructif avec les acteurs et des recommandations édictées par des instances régulatrices internationales et nationales, sinon des efforts d'harmonisation déployés par la Commission européenne, auxquelles le législateur luxembourgeois est bien inspiré de ne pas préjuger à travers sa transposition nationale.

Article 7 : Identification de la ligne appelante et de la ligne connectée

(et abrogation de l'article 41 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel)

Le projet de loi se propose d'insérer au paragraphe 5 de l'article 7 de la loi des dispositions assurant que tout fournisseur ou opérateur de téléphonie fixe ou mobile transmet d'office pour chaque appel à destination d'un des numéros d'urgence déterminés par l'ILR les données d'identification et de localisation disponibles.

Ces nouvelles dispositions remplacent aussi bien la dernière phrase de l'article 9 paragraphe (1) dont la suppression par la loi du 24 juillet 2010 avait donné lieu à un regrettable vide juridique et l'article 41 actuel de la loi modifiée du 2 août 2002 qui poursuivaient le même objectif, à savoir garantir en cas d'appel d'un numéro d'urgence de la Police grand-ducale ou des services de secours (112, opéré par la Protection civile et le service d'incendie et de sauvetage de la Ville de Luxembourg) l'accès de plein droit des autorités policières respectivement des services de secours d'urgence à toutes les données d'identification et de localisation disponibles des personnes à l'origine de l'appel (de détresse ou de signalement).

Elles sont parfaitement adaptées aux yeux de la Commission nationale pour résoudre la difficulté soulevée à juste titre par le Ministre de l'Intérieur et de la Grande Région et répondre à son souhait de voir rétablir le fondement légal de l'accès aux données permettant à la Police grand-ducale, au Central des Secours d'Urgence et au Central du service d'incendie

et d'ambulance de la Ville de Luxembourg d'identifier et de localiser les personnes dont émane l'appel.

Notre Commission ne partage en revanche pas l'avis exprimé par Monsieur le Directeur général de la Police grand-ducale que le système prévu aux termes de l'article 41 de la loi modifiée du 2 août 2002 sur la protection des données et dont la mise en œuvre n'a jamais abouti pour des raisons techniques au Luxembourg. serait nécessaire ou préférable à celui prévu par le projet de loi.

Le législateur de 2002 avait retenu à l'article 41 une solution centralisée dont il s'est avéré par la suite que seul un Etat membre, à savoir les Pays-Bas, l'a choisie et effectivement mise en service. Les conditions de sécurité nécessaires pour protéger une banque de données centralisée ont constitué, semble-t-il, un obstacle empêchant sa réalisation opérationnelle par l'ILR. Dans tous les autres pays de l'Union Européenne l'accès des autorités policières et judiciaires à ces données s'effectue de façon décentralisée directement auprès des opérateurs de réseaux de téléphonie fixe ou mobile.

Dans son avis du 26 avril 2010 (Délibération n° 85/2010) relatif au projet de loi n° 6113 relatif à la conservation des données relatives aux communications électroniques, notre Commission nationale s'était exprimée clairement en défaveur de la mise en place d'un stockage centralisé des données de trafic provenant de l'ensemble des opérateurs de réseaux et fournisseurs de services de communications électroniques (comme le CIOT aux Pays-Bas) pour l'accès des autorités judiciaires agissant au titre de l'article 67-1 du Code d'Instruction criminelle et de celles compétentes en vertu des articles 88-1 à 88-4 pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique et pour la prévention, la recherche et la constatation et la poursuite des infractions pénales emportant une prise minimale prévue par la loi du 24 juillet 2010. Elle avait été suivie sur ce point par le législateur.

La modification de l'article 41 (extension aux données de localisation) envisagée dans le courrier prémentionné du Directeur général de la Police grand-ducale conduirait à une confusion non souhaitable entre les dispositions légales ayant pour objet la transposition de la directive 2006/24/CE du 15 mars 2006 sur la conservation des données générées et traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public et celles répondant au besoin spécifiquement visé dans le courrier de Monsieur le Ministre de l'Intérieur et de la Grande Région. Les nouvelles dispositions prévues au projet de loi répondent à ce besoin.

Notre Commission nationale y marque donc son accord et approuve l'abrogation proposée de l'article 41 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Article 11 : Communications non sollicitées

Les modifications à cet article de la loi dérivent directement de la directive à transposer et n'appellent pas de commentaire.

Ainsi décidé à Luxembourg en date du 10 novembre 2010.

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° 6196 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

Délibération n° 345/2010 du 24 novembre 2010

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 sécurité sociale en date du 12 novembre 2010, la Commission nationale expose ci-après ses réflexions et commentaires au sujet du projet de loi n°6196 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 (ci-après : le projet de loi).

Au vu des contraintes de délai, elle entend limiter son analyse aux aspects relatifs au dossier de soins partagé.

Avant-propos

La Commission nationale a été consultée à plusieurs reprises par le Ministère de la Santé au cours de l'élaboration du programme eSanté. C'est dans le cadre de ces travaux qu'elle faisait valoir que la création et la mise en place d'un dossier médical électronique partagé devaient être inscrites dans la loi. Elle note avec satisfaction que les auteurs du projet de loi ont suivi cette recommandation.

Si l'instauration d'un dossier médical partagé recueillant les principales informations sur le parcours de santé de chaque patient peut incontestablement présenter des avantages non négligeables, elle entraîne aussi des risques. Ainsi, un dossier médical électronique peut contribuer à améliorer la qualité des soins et la sécurité des patients. En effet, le regroupement des renseignements donne aux professionnels de santé une meilleure connaissance de l'anamnèse du patient et des interventions effectuées précédemment par d'autres confrères, ce qui facilite le choix d'un traitement approprié.

Mais, avec la mise en place d'un dossier médical virtuel partagé à travers une plateforme d'échange, la relation classique qu'entretient le patient avec son médecin « en binôme » peut s'en trouver affectée. Les informations sont recueillies, conservées et utilisées avec le consentement du malade par le médecin qu'il a librement choisi et qui est tenu d'en sauvegarder le secret en vertu des règles de déontologie médicale.

L'introduction du dossier électronique partagé vise à élargir dorénavant l'accessibilité des renseignements qu'il contient et à permettre une vue d'ensemble des résultats de tous les examens, des traitements et soins prodigués[28].

Par ailleurs, se pose la question de comment prévenir de façon suffisante les risques d'interception et les utilisations abusives du dossier de soins partagé, compte tenu de l'ampleur inédite du traitement des données de santé et de la multiplication des destinataires. Il a été retenu que « *certains éléments des dossiers médicaux, lorsqu'ils sont utilisés hors de la relation médecin-malade, peuvent nuire au patient. Les données médicales font partie de la sphère la plus intime des personnes. La divulgation non autorisée des données médicales à caractère personnel peut donc être à l'origine de différentes sortes de discrimination, et même de la violation de droits fondamentaux* »[29]

[28] page 3 du document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques adopté le 15 février 2007 par le Groupe de travail « Article 29 » sur la protection des données (WP 131), ci-après le « document de travail WP131 »

[29] Exposé des motifs relatif à la recommandation Rec(97)5 du Conseil de l'Europe relative à la protection des données médicales, point n°9

C'est pour conserver cette relation de confiance que le législateur doit prévoir des garanties particulières.

La Commission nationale relève que le projet de loi définit avec précision les finalités du dossier de soins partagé. L'article 1er point 32° qui introduit un article 60quater au Code de la sécurité sociale précise que le dossier de soins partagé a pour finalités la sécurité, la continuité des soins, la coordination des soins et une utilisation efficiente des services de santé. Ces finalités s'inscrivent dans les finalités retenues par le groupe de travail « Article 29 » dans son avis[30].

1. Le critère de légitimation

Les dossiers de soins partagés contiendront des données de santé qualifiées de données sensibles au sens de l'article 8 paragraphe 1 de la directive 95/46/CE[31] du Parlement Européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après : la directive 95/46/CE).

Cette disposition[32], reprise de l'article 6 de la Convention 108 du Conseil de l'Europe[33] pose le principe de l'interdiction de tout traitement des données relatives à la santé.

Cette interdiction générale est toutefois assortie à l'article 8 paragraphes 2 à 5 de la dite directive, de dérogations qui sont « *limitées, exhaustives et (qui) doivent être interprétées strictement* »[34].

La création et la mise en place d'un dossier de soins partagé peut se justifier par l'article 8 paragraphe 4 de la directive 95/46/CE qui pose comme conditions que :

1. cette dérogation soit inscrite dans une disposition légale ou une décision de l'autorité de contrôle,

2. le traitement soit justifié par un motif d'intérêt public important et

3. des garanties spécifiques et appropriées soient prévues afin de protéger les droits fondamentaux et la vie privée des personnes.

La Commission nationale estime que l'introduction d'un système généralisé de dossiers électroniques partagés répond au critère posé à l'article 8 paragraphe 4 de la directive 95/46/CE dès lors que le projet de loi apporte les garanties appropriées suffisantes en matière de protection de la vie privée et des données personnelles.

2. 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[35], dont le respect doit être assuré par le ou les responsables du traitement

Le groupe de travail « *Article 29* » *retient que* « *tout système de DME [dossier médical électronique] doit (…) garantir que le risque d'atteintes à la vie privée dû au stockage de données médicales et à la fourniture de ces données soit adéquatement contrebalancé par la responsabilité pour le préjudice causé, par exemple par l'utilisation incorrecte ou non autorisée de données des DME*[36]».

Il résulte de l'économie générale du projet de loi que la responsabilité est exercée de manière conjointe.

A défaut d'indications précises dans le texte, la Commission nationale estime pouvoir reconstituer une répartition des responsabilités entre les différents acteurs en fonction de leur rôle attribué par les dispositions proposées.

Ainsi, tout médecin qui consulte le dossier de soins partagé est tenu de traiter les données de manière

30 page 1 du document de travail de travail WP 131

31 « *Les Etats membres interdisent (…) le traitement des données relatives à la santé et à la vie sexuelle* »

32 Cette disposition a été transposée à l'article 6 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard des traitement des données à caractère personnel

33 Convention pour la protection des personnes à l'égard du traitement informatisé des données à caractère personnel du 28 janvier 1981

34 page 9 du document de travail WP 131

35 Qui transpose l'article 6 de la directive 95/46/CE

36 Document de travail WP 131, page 23 point 10 paragraphe 1er

loyale et licite et dans le respect des finalités légales du traitement.

Ces obligations sont prévues à l'article 4 de la loi modifiée du 2 août 2002 qui dispose que « *le responsable du traitement doit s'assurer que les données qu'il traite le sont loyalement et licitement, et notamment que ces données sont : (a) collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités (…)* ».

Ensuite, le médecin qui inscrit des informations dans un dossier de soins partagé est tenu de vérifier l'exactitude de ses informations et il doit s'astreindre, conformément aux exigences du projet de loi sous examen, à intégrer les données « *utiles et pertinentes*[37] »

L'article 4, paragraphe (1), lettres (b) et (c) de la loi du 2 août 2002 précise que le responsable du traitement doit s'assurer que les données qu'il traite sont « *adéquates, pertinentes et non excessives au regard des finalités (…) (et) exactes et, si nécessaire, mises à jour (…)* ».

Le nouvel article 60quater du Code de la sécurité sociale tel que proposé dans le projet de loi prend d'ailleurs soin de réserver à tout professionnel de la santé la possibilité d'accéder ultérieurement aux données qu'il a inscrit dans un dossier de soins partagé.

Pour sa part, le médecin référent se voit attribuer un rôle plus important dans le fonctionnement du dossier de soins partagé. Ses missions sont plus nombreuses que celles qui incombent aux différents intervenants isolés. L'article 1er point 8° du projet de loi, qui crée l'article 19bis du Code de la sécurité sociale précise que le médecin référent a notamment pour mission de « *3) suivre régulièrement le contenu du dossier de soins partagé de l'assuré (…)* ». Cette disposition, même si elle ne confère pas la maîtrise totale du dossier, attribue au médecin référent des prérogatives significatives dans le traitement de données.

Le groupe de travail « Article 29 » suggère d'ailleurs qu'une seule personne soit responsable envers les patients de l'usage correct des demandes d'accès.

> « *Les systèmes de DME (dossier médical électronique) sont toutefois des systèmes de mise en commun d'informations qui comptent de nombreux responsables du traitement des données. Dans ces conditions, une seule institution spéciale doit être responsable envers les personnes concernées du traitement correct des demandes d'accès. Vu la complexité prévisible d'un DME pleinement opérationnel et la nécessité de faire en sorte que les patients aient confiance dans le système, il semble essentiel que les patients dont les données sont traitées dans un DME sachent comment contacter un partenaire responsable avec lequel ils peuvent discuter des éventuelles lacunes du système. Des dispositions spéciales à cet effet devront être incluses dans tout règlement sur les systèmes de DME.* »[38]

Enfin, l'Agence nationale des informations partagés dans le domaine de la santé (ci-après : l'Agence), instituée par l'article 60ter du Code de la sécurité sociale est notamment chargée d'une mission technique et administrative pour mettre en place l'architecture technique et organisationnelle du dossier de soins partagé. Cette agence a une mission stratégique active qui incombe, en vertu de l'article 17 de la directive 95/46/CE au responsable du traitement[39]. Il est vrai que le projet de loi sous examen prévoit que les mesures de sécurité seront déterminées par règlement grand-ducal. Il n'en reste pas moins que l'Agence a une responsabilité particulière en matière de sécurité du système.

La Commission nationale note par ailleurs que les différents intervenants doivent en tout état de cause, chacun pour ce qui le concerne, assumer les obligations prévues aux articles 21 à 23 de la loi du 2 août 2002 en matière de sécurité du traitement.

Tout responsable du traitement est tenu de respecter l'obligation d'information vis-à-vis des personnes

[37] article 60quater paragraphe (2) du Code de la Sécurité sociale tel que proposé dans le projet de loi

[38] Pages 23 et 24 du document de travail WP 131

[39] « (…) le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau ainsi que contre toute autre forme de traitement illicite. »

concernées[40]. La Commission nationale pense qu'une information appropriée sur le fonctionnement du système doit être assurée avant l'ouverture d'un dossier de soins partagé. Il conviendra dans les mesures à préciser ultérieurement dans les dispositions réglementaires comment se passera cette information.

En définitive, la Commission nationale constate que les différentes obligations qui incombent au responsable du traitement sont, dans le projet de loi, éclatées entre différents intervenants au dossier de soins partagé. Or, en cas de non-respect des différentes obligations légales, le texte sous examen ne règle pas la question de la responsabilité. Notons que la loi du 2 août 2002 prévoit des sanctions pénales à l'égard du responsable du traitement[41].

3. Le rôle du patient dans la tenue du dossier

Dans son avis précité, le groupe de travail « Article 29 » se penche sur des garanties particulières qui « semblent particulièrement nécessaires dans les systèmes de DME afin de garantir les droits des patients à la protection des données »[42]. La première de ces garanties est, selon lui, le respect de l'autodétermination du patient.

Il précise que « même si un système de DME n'a pas que le consentement pour base juridique (article 8 paragraphe 2 de la directive 95/46/CE), la détermination par le patient lui-même de quand et comment ses données sont utilisées devrait constituer une garantie majeure »[43].

L'autodétermination du patient peut se concevoir au niveau de trois stades successifs :

- lors de la création du dossier,
- lors de l'inscription des données dans le dossier et
- lors de la consultation du dossier par les professionnels de santé.

La Commission nationale examine ci-après dans quelle mesure le projet de loi tient compte du principe de l'autodétermination du patient lors de ces trois différents stades.

Lors de la création du dossier

En France, le législateur a prévu que chaque bénéficiaire de l'assurance maladie dispose, avec son consentement, d'un dossier électronique[44].

Le projet de loi sous examen prévoit, à l'inverse de la solution française, qu'un dossier est ouvert d'office pour chaque patient.

Toutefois, il ressort du texte sous examen que le patient peut tout de même avoir un rôle actif lors de la création du dossier. En choisissant un médecin référent, il prend indirectement la décision que son dossier sera régulièrement suivi dans le cadre de la continuation de soins[45]. En ne désignant pas de médecin référent, son dossier de soins partagé ne sera pas passé en revue régulièrement. Quoi qu'il en soit, le patient peut désigner d'autres médecins qui peuvent consulter son dossier.

Lors de l'inscription des données dans le dossier de soins partagé

Le projet de loi sous examen n'a pas prévu de droit de regard lors de l'inscription des données dans le dossier de soins partagé.

La Commission nationale se demande si pour des données susceptibles d'un usage plus préjudiciable, il ne serait pas souhaitable que le patient puisse décider de leur intégration dans son dossier de soins partagé. Le groupe de travail « Article 29 » cite à titre d'exemple, les données psychiatriques et les avortements et on pourrait songer en outre aux données relatives à des maladies sexuellement transmissibles. Le patient pourrait craindre qu'à travers le dossier de soins partagé des professionnels de santé autres que ceux qu'il a consulté n'obtiennent connaissance d'informations ultrasensibles qu'il a tenu jusqu'alors secret. Or, un

40 Article 26 de la loi du 2 août 2002 transposant l'article 10 de la directive 95/46/CE

41 Par exemple, article 4 paragraphe (3) ou article 25 ou encore l'article 26 paragraphe (3).

44 Articles L.1111-8 et L.1111-14 et suivants du Code de la santé publique

45 Article 19bis du Code de la sécurité sociale tel que prévu à l'article 1er point 8° du projet de loi

droit d'opposition à l'inscription de ces données risque d'aller au détriment du caractère exhaustif du dossier. Une solution intermédiaire pourrait consister dans le recours de techniques particulières telles que des « enveloppes scellées » qui ne peuvent être ouvertes sans la coopération du patient.

Ainsi, le patient pourrait se voir attribuer la faculté de ne pas porter à la connaissance de certains praticiens certains groupes d'informations qui le concernent. A cet effet, la Commission nationale suggère de compléter le libellé du paragraphe (6) sub 3) du nouvel article 60quater du Code de la sécurité sociale tel que proposé dans le projet de loi en bout de phrase *« … en tenant compte des attributions des différentes catégories de prestataires et des différentes catégories de données ; »*.

Lors de la consultation du dossier

L'autodétermination du patient pourrait se traduire par la faculté lui attribuée d'empêcher l'accès de certains professionnels de santé à certaines des données de son dossier de soins partagé.

Le nouvel article 60quater paragraphe (4) du Code de la sécurité sociale tel que proposé dans le projet de loi donne certes la possibilité au patient de s'opposer au partage d'informations qui le concernent. Le patient a ainsi la possibilité de verrouiller le partage entre professionnels de la santé de toutes les informations le concernant. Or, on peut se demander si le patient ne devrait pas avoir la faculté d'attribuer un accès modulaire des informations qui le concernent selon les médecins appelés à consulter son dossier et selon la nature des informations enregistrées. L'ajout proposé par la Commission nationale au point précédent devrait être de nature à régler cette question dans le contexte du règlement grand-ducal d'exécution à prendre.

La Commission nationale estime que ce droit d'opposition (ou opt-out) est une garantie appropriée acceptable[46] au sens de la directive 95/46/CE.

L'Asbl « Patiente Vertriedung » se prononce en revanche pour une maîtrise totale du patient sur l'accès à son dossier. Si une information préalable ponctuelle paraît difficilement réalisable en pratique, une plus grande transparence à l'égard du patient peut être obtenue dans les systèmes où l'accès au dossier est conditionné par la présentation d'une carte électronique.

A titre d'exemple, le système français prévoit que pour accéder à un dossier médical électronique, le praticien doit insérer sa carte de soins professionnelle ainsi que la carte électronique du patient (la « carte Vitale ») : en lui remettant sa carte électronique, le patient donne indirectement son accord à ce que le médecin consulte son dossier.

Il convient de noter que les systèmes étrangers qui ont opté pour une telle solution prévoient que l'exigence de double carte peut être écartée en cas d'urgence médicale[47].

4. l'accès aux dossiers par les professionnels de santé

- Le respect du secret médical

La concentration de façon quasi exhaustive des informations relatives au parcours de santé d'un patient dans un dossier électronique, accessible à travers une plateforme d'échange nationale, pourrait susciter l'intérêt de tiers tels que par exemple employeur, industrie pharmaceutique, compagnies d'assurances, autorités répressives etc.

Pourtant, toute relation entre un patient et son médecin doit être scellée par le principe de confidentialité et le respect du secret médical pour éviter d'éventuels abus.

La Commission nationale suggère dès lors de rajouter au début du paragraphe (3) du nouvel article 60quater du Code de la sécurité sociale tel que proposé dans le projet de loi le début de phrase suivant : *« Dans le respect du secret médical et des finalités visées au présent article, l'accès au dossier de soins partagé est réservé : … »*.

[46] « L'accord en tant que garanties ne doit pas nécessairement être donné sous la forme d'un consentement préalable : la possibilité d'autodétermination pourrait également, en fonction de la situation, être conférée sous la forme d'un droit de refus », page 25 du document de travail WP 131[41]
Par exemple, article 4 paragraphe (3) ou article 25 ou encore l'article 26 paragraphe (3).

[47] En France, ce procédé est appelé le « bris de glace ». Il est toujours possible sauf dans l'hypothèse où le patient a précisé dans son dossier qu'il interdisait cette pratique même en cas d'urgence.

- La limitation des personnes pouvant consulter le dossier de soins partagé

L'amendement 8° adopté le 12 novembre 2010 a restreint les catégories de personnes qui sont autorisées à accéder aux dossiers de soins partagés.

C'est dans le souci du respect des finalités pour lesquelles le dossier de soins partagé est institué que la Commission nationale estime que la liste des destinataires ne devrait pas être élargie à l'avenir à d'autres catégories de personnes.

Dans ce contexte, la Commission nationale renvoie à l'article L 1111-18 du Code de la santé publique français qui dispose ce qui suit :

> *« L'accès au dossier médical personnel ne peut être exigé en dehors des cas prévus aux articles L. 1111-15 et L. 1111-16, même avec l'accord de la personne concernée.*
>
> *L'accès au dossier médical personnel est notamment interdit lors de la conclusion d'un contrat relatif à une protection complémentaire en matière de couverture des frais de santé et à l'occasion de la conclusion de tout autre contrat exigeant l'évaluation de l'état de santé d'une des parties. L'accès à ce dossier ne peut également être exigé ni préalablement à la conclusion d'un contrat, ni à aucun moment ou à aucune occasion de son application.*
>
> *Le dossier médical personnel n'est pas accessible dans le cadre de la médecine du travail.*
>
> *Tout manquement aux présentes dispositions donne lieu à l'application des peines prévues à l'article 226-13 du code pénal. »*

- L'exigence de l'exactitude des informations contenues dans le dossier de soins partagé

Le texte sous examen donne la possibilité aux professionnels de santé de pouvoir modifier les informations qu'ils ont intégrées dans le dossier de soins partagé[48]. Cette prérogative répond au principe de l'exactitude des données, principe majeur en matière de protection des données. Le dossier de soins partagé doit être régulièrement mis à jour. Il ne doit en effet contenir que des données justes et nécessaires, en vertu de l'article 6 paragraphe 1er lettre d) de la directive 95/46/CE[49], pour que les professionnels de santé puissent continuer les soins au patient dans les conditions les plus favorables.

- La pseudonymisation des données pour les échanges à des fins statistiques et épidémiologiques

L'Agence nationale est appelée également à échanger des informations dans le domaine de la santé avec d'autres organismes à des fins statistiques et épidémiologiques. L'article 60quater paragraphe (5) du Code de la sécurité sociale tel que le prévoit le projet de loi précise que les informations doivent préalablement avoir été anonymisées.

Le paragraphe (3) du même article 60quater en projet ne mentionne pas l'Agence nationale dans l'énumération des personnes pouvant accéder aux dossiers. La Commission nationale est donc amenée à conclure que l'Agence ne peut pas accéder aux données contenues dans un dossier de soins partagés.

Il ressort aussi des documents communiqués par le Ministère de la Santé dans le cadre du programme eSanté que les données d'identification du patient et les données médicales seront séparées. Un tiers de confiance (appelé « Trusted third party » TTP) serait chargé de fournir à la plateforme uniquement des données pseudonymisées. Ce tiers gérerait exclusivement les données d'identification.

La Commission nationale estime que ces intentions sont satisfaisantes en termes de protection des données. Afin d'éviter tout problème d'interprétation, il serait préférable que la mise en place d'un tiers de confiance chargé de la pseudonymisation des données soit inscrite dans la loi.

[48] Article 60quater paragraphe 4 alinéa 2° du Code de la sécurité sociale sous l'article 1er point 32 du projet de loi

[49] « Les données à caractère personnel doivent être exactes et, si nécessaire, mises à jour ; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées »

5. Le contenu du dossier de soins partagé

Le contenu du dossier de soins partagé fait l'objet du paragraphe (2) de l'article 60quater du Code la sécurité sociale tel que proposé dans le projet de loi. Ces dispositions pourront être précisées davantage par des mesures réglementaires.

6. Les mesures de sécurité

L'exigence de confidentialité et la sécurité du système d'information médicale est primordiale.

La Commission nationale estime que les patients accepteront plus facilement le nouveau système de dossiers de soins partagés s'ils sont convaincus que les mesures de sécurité assurent la confidentialité, le respect du secret médical et préviennent les détournements de finalité.

L'article 1er point 32° paragraphe (6) (l'article nouveau 62quater du Code de la sécurité sociale) du projet de loi prévoit qu'un règlement grand-ducal, pris après avis de la Commission nationale déterminera les modalités et les conditions de mise en place du dossier de soins partagé.

La Commission nationale salue le fait que les auteurs du projet de loi l'associent à cette tâche. Elle précise que ces mesures devront présenter des garanties suffisantes pour protéger la nature sensibles des données médicales.

L'exigence d'un niveau de sécurité particulièrement élevé de la plateforme électronique nationale d'échange et de partage des données de santé devrait, aux yeux de la Commission nationale, être inscrite dans le texte même de la loi. Les modalités et conditions détaillées peuvent toutefois faire l'objet d'un règlement grand-ducal.

Elle suggère dès lors de rajouter un point à la liste des modalités et des conditions contenue à l'article 60quater paragraphe (6) du Code de la sécurité sociale avec le libellé suivant :

« les mesures nécessaires pour assurer un niveau de sécurité particulièrement élevé de la plateforme électronique nationale d'échange et de partage des données de santé. »

Lors de l'examen des dispositions de ce règlement grand-ducal, la Commission nationale sera attentive à ce que l'authentification des personnes qui accèdent aux dossiers de soins partagés – tant les patients que les professionnels de santé - soit forte. Elle se félicite de ce que le projet de loi retient d'ores et déjà le principe de la traçabilité des accès. Cette mesure technique est un outil précieux pour que le patient exerce pleinement son droit d'accès mais aussi pour vérifier a posteriori toute consultation du dossier en dehors des hypothèses pour lesquelles il a été institué. Il permet encore d'assurer les praticiens de l'exactitude des informations.

Ainsi décidé à Luxembourg en date du 24 novembre 2010.

La Commission nationale pour la protection des données

Gérard Lommel	Président
Pierre Weimerskirch	Membre effectif
Thierry Lallemang	Membre effectif

Notification unique pour les traitements de données à caractère personnel mis en œuvre par les communes du Grand-Duché de Luxembourg

Délibération n°2/2010 du 15 janvier 2010

La Commission nationale pour la protection des données (ci-après dénommée « Commission nationale ») ;

vu les articles 99, 101, 102, 107 et 108 de la Constitution ;

les articles 34 à 57, 63 à 70, 75 à 80, 84 à 85 et 102 à 111 du Code civil ;

le Code du Travail ;

l'article 165 de la loi générale des impôts ;

le décret du 4 thermidor an XIII (23 juillet 1805) relatif aux autorisations des officiers de l'état civil sur les inhumations ;

le Décret du 20 juillet 1807 concernant les tables alphabétiques des actes de l'état civil ;

l'arrêté du Gouverneur général du 20 août 1814 concernant la police des inhumations ;

l'arrêté royal du 8 juin 1823 concernant des dispositions à l'égard des officiers de l'état civil ;

l'arrêté royal du 31 juillet 1828 qui prescrit aux officiers de l'état civil de donner de tous décès avis par écrit aux juges de paix ;

l'arrêté royal grand-ducal du 6 mai 1874 portant délégation des juges de paix pour la vérification des registres de l'état civil ;

la loi modifiée du 19 mai 1885 sur la chasse ;

la loi modifiée du 22 décembre 1886 concernant les recensements de la population à faire en exécution de la loi électorale ;

la loi modifiée du 19 mai 1885 sur la chasse ;

la loi modifiée du 19 juillet 1904 sur les impositions communales ;

la loi modifiée du 20 juillet 1925 sur l'amodiation de la chasse et l'indemnisation des dégâts causés par le gibier ;

la loi modifiée du 1er décembre 1936 sur l'impôt foncier ;

l'arrêté grand-ducal du 30 août 1939 portant introduction de la carte d'identité obligatoire ;

l'article 5 paragraphe 3 de la loi modifiée du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies publiques ;

la loi du 1er avril 1968 relative aux mentions marginales des actes de l'Etat civil ;

la loi du 1er août 1972 portant réglementation de l'inhumation et de l'incinération des dépouilles mortelles ;

le règlement grand-ducal du 21 juin 1978 relatif à la dispersion des cendres ;

la loi modifiée du 24 décembre 1985 fixant le statut général des fonctionnaires communaux ;

le règlement grand-ducal du 11 janvier 1988 déterminant les pièces contenues dans le dossier personnel des fonctionnaires communaux ;

le règlement grand-ducal du 15 novembre 2001 concernant le régime des employés communaux ;

la loi modifiée du 16 juillet 1987 concernant le colportage, la vente ambulante, l'étalage de marchandises et la sollicitation de commandes ;

la loi communale modifiée du 13 décembre 1988 et notamment ses articles 29, 60, 70, 99, 105, 106, 114, 135, 140, 148 et 160 ;

l'article 1er de la loi du 19 juillet 1991 portant création d'un Service de la formation des adultes et donnant un statut légal au Centre de langues Luxembourg ;

le règlement grand-ducal du 31 mars 2000 ayant pour objet 1) de fixer les modalités des contrats conventionnant des cours pour adulte et les conditions d'obtention d'un label de qualité et d'une subvention ; 2) de créer une Commission Consultative à l'Education des Adultes ;

l'article 17 de la loi modifiée du 17 juin 1994 relative à la prévention et à la gestion des déchets ;

la loi du 8 septembre 1998 réglant les relations entre l'Etat et les organismes oeuvrant dans les domaines social, familial et thérapeutique ;

la loi modifiée du 29 avril 1999 portant création d'un droit à un revenu minimum garanti ;

les articles 4, 5, 12 et 13 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci après « la loi du 2 août 2002 ») et notamment le paragraphe (4) de l'article 13 ;

la loi électorale modifiée du 18 février 2003 ;

la loi du 9 juillet 2004 relative aux effets légaux de certains partenariats ;

l'article 37 de la loi modifiée du 19 juillet 2004 concernant l'aménagement communal et le développement urbain ;

le règlement grand-ducal du 8 août 2007 portant introduction d'une carte d'identité pour les personnes de nationalité luxembourgeoise âgées de moins de quinze ans ;

la loi du 29 août 2008 sur la libre circulation des personnes et l'immigration ;

la loi du 9 mai 2008 relative aux chiens ;

le règlement grand-ducal du 9 mai 2008 concernant l'identification et la déclaration des chiens ;

le règlement grand-ducal du 9 mai 2008 relatif aux cours de formation des détenteurs de chiens et aux cours de dressage des chiens ;

le règlement grand-ducal du 9 mai 2008 énumérant les éléments de reconnaissance des types de chiens susceptibles d'être dangereux ;

la loi du 29 août 2008 1) portant sur la libre circulation des personnes et l'immigration; 2) modifiant - la loi modifiée du 5 mai 2006 relative au droit d'asile et à des formes complémentaires de protection, - la loi modifiée du 29 avril 1999 portant création d'un droit à un revenu minimum garanti, - le Code du travail, - le Code pénal; 3) abrogeant - la loi modifiée du 28 mars 1972 concernant 1. l'entrée et le séjour des étrangers; 2. le contrôle médical des étrangers; 3. l'emploi de la main-d'oeuvre étrangère, - la loi du 26 juin 1953 portant fixation des taxes à percevoir en matière de cartes d'identité pour étrangers, - la loi du 28 octobre 1920 destinée à endiguer l'affluence exagérée d'étrangers sur le territoire du Grand-Duché ; le règlement grand-ducal du 5 septembre 2008 définissant les critères de ressources et de logement prévus par la loi du 29 août 2008 sur la libre circulation des personnes et l'immigration ;

le règlement grand-ducal du 5 septembre 2008 portant sur l'attestation de prise en charge en faveur d'un étranger prévue à l'article 4 de la loi du 29 août 2008 sur la libre circulation des personnes et l'immigration ;

le règlement grand-ducal 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 ;

la loi du 19 décembre 2008 relative à l'eau ;

le règlement grand-ducal du 13 février 2009 instituant le « chèque-service accueil » ;

la loi du 6 février 2009 portant organisation de l'enseignement fondamental ;

la loi du 6 février 2009 concernant le personnel de l'enseignement fondamental ;

la loi du 6 février 2009 relative à l'obligation scolaire ;

le règlement grand-ducal du 28 mai 2009 ayant pour objet de déterminer : - les modalités d'élection des représentants des parents d'élèves à l'école et à la commission scolaire communale ; - les modalités d'élection des représentants du personnel des écoles et à la commission scolaire communale ; - l'organisation et le fonctionnement de la commission scolaire communale ;

la loi du 18 décembre 2009 organisant l'aide sociale,

considérant que les communes assurent de nombreuses missions d'intérêt public,

qu'elles constituent, tiennent à jour et utilisent à cette fin des fichiers et effectuent des traitements de données à caractère personnel tombant dans le champ d'application de la loi du 2 août 2002,

que les textes légaux susvisés chargent les communes de nombreuses missions d'intérêt public,

que, par ailleurs, l'article 28 de la loi communale modifiée dispose que « le conseil communal règle tout ce qui est d'intérêt communal»,

qu'ainsi, un nombre toujours croissant de services de plus en plus diversifiés sont offerts par les communes aux citoyens, comme par exemple les activités de loisir, les services de téléalarme ou de repas sur roues ou les antennes collectives gérées par des communes pour ne citer que quelques uns,

que le fait d'offrir ces services implique la mise en œuvre par les communes de traitements de données à caractère personnel tombant dans le champ d'applications de la loi du 2 août 2002,

que pour remplir certaines de leurs missions, les communes se sont regroupées en syndicats de communes,

que les dispositions légales ainsi que les pratiques établies font en sorte que les modalités des traitements de données mis en œuvre par les différentes communes sont identiques pour une mission ou un service donné,

que, par ailleurs, pour une mission ou un service donné, les traitements de données poursuivent des finalités identiques,

qu'en vertu de l'article 12 paragraphe (1) lettre (a) de la loi 2 août 2002, les traitements de données à caractère personnel à l'exception de ceux prévus aux articles 8, 14 et 17 de la loi font l'objet d'une notification préalable par le responsable du traitement auprès de la Commission nationale, à moins que ce dernier n'en soit exempté en vertu de l'article 12 paragraphes (2) et (3) de la loi et notamment en vertu de la lettre (j) dudit paragraphe (3),

que cette exemption vise uniquement les traitements de données à caractère personnel effectués par des autorités administratives soumis à des règlementations particulières adoptées par ou en vertu de la loi et réglementant l'accès aux données traitées ainsi que leur utilisation et leur obtention, qu'à ce jour, la majorité des traitements mis en œuvre par les communes ne sont pas exemptés en vertu de ladite disposition, faute de réglementation spécifique de l'accès au données traitées ainsi que de leur utilisation et de leur obtention,

qu'il appert que la Commission nationale peut décider que des traitements font l'objet d'une notification unique conformément à l'article 13 paragraphe (4) qui précise les conditions à respecter et mesures, notamment de sécurité, à appliquer dans la mise en œuvre du traitement, conformément à l'article 13 paragraphe (4) de la loi du 2 août 2002,

décide que les traitements décrits ci-dessous opérés par les communes, soit en nom propre, soit sous la forme de syndicats intercommunaux, dans le cadre de l'exécution de leurs missions leur conférées, peuvent faire l'objet d'une déclaration par notification unique.

Il appartiendra par la suite aux communes désireuses de se conformer à la loi du 2 août 2002 et de notifier ledit traitement de données en bonne et due forme à la Commission nationale sous la forme d'un simple engagement formel de conformité (prévu à l'article 13 paragraphe (4) de la loi du 2 août 2002) à la description figurant dans la présente décision qui énumère par ailleurs les conditions à respecter lors la mise en œuvre du traitement.

Les communes spécifieront dans l'engagement formel visé ci-dessus les traitements mis en œuvre parmi ceux décrits dans la présente décision.

I. Conditions et modalités des traitements

TRAITEMENTS MIS EN ŒUVRE PAR LE COLLÈGE DES BOURGMESTRE ET ÉCHEVINS

Sont à considérer comme responsables des traitements les collèges des bourgmestre et échevins des communes mettant en œuvre les traitements de données à caractère personnel décrits sous les points 1 à 25 en relation avec les missions qui leur sont conférées.

1. Administration de la population luxembourgeoise

1.1 Description du traitement

Le traitement consiste en la tenue d'un fichier permettant d'administrer la population de la commune/ville ainsi que l'établissement de documents d'identité pour ces derniers. Le traitement permet en outre d'envoyer aux résidents de la commune/ville des courriers d'information personnalisés sur les activités et services offerts par la commune/ville, à l'exclusion de toute fin commerciale ou politique.

1.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, les deux conditions de légitimité suivantes, énumérées à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous les lettres a) et b) sont réunies dans le chef des responsables des traitements :

- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis et/ou
- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant d'une autorité publique, dont est investi le responsable du traitement.

Le traitement est mis en œuvre conformément aux bases légales suivantes :

- articles 102 à 111 du Code civil ;
- loi modifiée du 22 décembre 1886 concernant les recensements de population à faire en exécution de la loi électorale ;
- arrêté grand-ducal du 30 août 1939 portant introduction de la carte d'identité obligatoire ;
- règlement grand-ducal du 8 août 2007 portant introduction d'une carte d'identité pour les personnes de nationalité luxembourgeoise âgées de moins de quinze ans.

1.3. Finalité(s) du traitement

Administration des résidents ayant déclaré leur domicile dans la commune. Administration de la population ainsi que l'établissement de documents d'identité pour les résidents de la commune. Gestion des ménages.

1.4. Description des catégories de données

Les données relatives aux résidents et ex-résidents de la commune, notamment données d'identification, adresse, historique des adresses, civilité, sexe, date et lieu de naissance, nationalité(s), composition du ménage et rôle dans le ménage, profession et emploi, matricule, date de décès, descendance, ascendance, conjoint(s), date d'arrivée/de départ dans la commune, indigénat, numéro de la carte d'identité, validité, suivi, observations.

1.5. Description des catégories de personnes concernées

Personnes physiques de nationalité(s) luxembourgeoise et/ou étrangère ayant déclaré leur résidence ou ayant résidé dans la commune ainsi que les ascendants et descendants de ces personnes.

1.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal

qui, dans le cadre de leurs fonctions, assurent l'administration de la population.

2. Administration de la population étrangère

2.1. Description du traitement

Le traitement consiste en la tenue d'un fichier des étrangers résidant dans la commune. Il permet en outre l'établissement de déclarations d'arrivée, attestations d'enregistrement, cartes de séjour, titres de séjour, titre de voyage ainsi que d'autres documents spécifiques pour étrangers.

2.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, les deux conditions de légitimité suivantes, énumérées à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous les lettres a) et b) sont réunies dans le chef des responsables des traitements :

- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis et/ou
- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant d'une autorité publique, dont est investi le responsable du traitement.

Le traitement est mis en œuvre conformément aux bases légales suivantes :

- Règlement grand-ducal du 5 septembre 2008 définissant les critères de ressources et de logement prévus par la loi du 29 août 2008 sur la libre circulation des personnes et l'immigration ;
- Règlement grand-ducal du 5 septembre 2008 portant sur l'attestation de prise en charge en faveur d'un étranger prévue à l'article 4 de la loi du 29 août 2008 sur la libre circulation des personnes et l'immigration ;
- Règlement grand-ducal 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 ;
- Loi du 29 août 2008 sur la libre circulation des personnes et l'immigration ;
- Loi du 23 octobre 2008 sur la nationalité luxembourgeoise.

2.3. Finalité(s) du traitement

Administration des personnes de nationalité étrangère ayant déclaré leur domicile ou ayant résidé dans la commune. Etablissement des documents visés sous le point 2.1. ci-dessus.

2.4. Description des catégories de données

Les données relatives aux étrangers résidant ou ayant résidé dans la commune, notamment données d'identification, adresse, historique des adresses, civilité, sexe, date et lieu de naissance, nationalité(s), composition du ménage et rôle dans le ménage, profession et emploi, date de décès, descendance, ascendance, conjoint(s), date d'arrivée/départ, numéro de la carte d'identité, validité, suivi, observation, numéro du dossier auprès du Ministère des Affaires Etrangères, validité de l'autorisation de séjour, date d'arrivée Schengen/Luxembourg.

2.5. Description des catégories de personnes concernées

Personnes physiques de nationalité étrangère ayant déclaré leur résidence ou ayant résidé dans la commune ainsi que les ascendants et descendants de ces personnes.

2.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent l'administration de la population.

3. Recensements

3.1. Description du traitement

Le traitement consiste en la tenue des fichiers relatifs au recensement fiscal annuel. Il permet l'établissement, la modification et l'impression des cartes d'impôt des contribuables, l'organisation des recensements fiscal annuel, agricole et décennal et des chiens.

3.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, les deux conditions de légitimité suivantes, énumérées à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous les lettres a) et b) sont réunies dans le chef des responsables des traitements :

- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis et/ou
- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant d'une autorité publique, dont est investi le responsable du traitement.

Le traitement est mis en œuvre conformément aux bases légales suivantes :

- Article 107 de la Constitution ;
- Article 165 de la loi générale des impôts ;
- Loi du 9 mai 2008 relative aux chiens ;
- Règlement grand-ducal du 9 mai 2008 concernant l'identification et la déclaration des chiens ;
- Article 183 de la loi électorale modifiée du 18 février 2003.

3.3. Finalité(s) du traitement

Mise en ouvre de recensements conformément aux bases légales applicables.

3.4. Description des catégories de données

Les données relatives aux personnes résidant ou ayant résidé dans la commune, notamment données d'identification, adresse, historique des adresses, civilité, sexe, date et lieu de naissance, nationalité(s), composition du ménage et rôle dans le ménage, profession et emploi, date de décès, descendance, ascendance, conjoint(s), indication si fonctionnaire européen ou non, allocation de famille, catégorie d'impôt, observations quant à une éventuelle 2e carte d'impôt ou carte de pension, historique des duplicatas émis, équipement ménager, données en relation avec le recensement agricole et le relevé des chiens.

3.5. Description des catégories de personnes concernées

Personnes physiques ayant déclaré leur résidence ou ayant résidé dans la commune.

3.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent l'administration de la population, notamment ceux à qui incombe l'organisation des recensements.

4. Gestion des listes électorales

4.1. Description du traitement

Le traitement permet la tenue et mise à jour des listes électorales (répertoire des électeurs), l'organisation des élections communales, léglislatives et européennes sur la base des fichiers de la population de la commune. Edition des documents nécessaires à l'exécution des opérations prescrites par la loi électorale.

4.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, les deux conditions de légitimité suivantes, énumérées à l'article 5 paragraphe

(1) de la loi modifiée du 2 août 2002, sous les lettres a) et b) sont réunies dans le chef des responsables des traitements :

- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis et/ou
- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant d'une autorité publique, dont est investi le responsable du traitement.

Le traitement est mis en œuvre conformément aux bases légales suivantes :

- Loi modifiée du 22 décembre 1886 concernant les recensements de la population à faire en exécution de la loi électorale ;
- Loi électorale modifiée du 18 février 2003.

4.3. Finalité(s) du traitement

Administration de la population en vue de l'organisation des élections communales, législatives et européennes. Tenue et mise à jour des listes électorales.

4.4. Description des catégories de données

Les données relatives aux personnes résidant ou ayant résidé dans la commune, notamment données d'identification, adresse, historique des adresses, civilité, sexe, date et lieu de naissance, nationalité(s), composition du ménage et rôle dans le ménage, profession et emploi, date de décès, descendance, ascendance, conjoint(s), indications sur le transfert de vote, perte du droit de vote avec motif, indications sur les demandes de participation des étrangers aux élections communales et européennes, bureau de vote, adresse d'envoi si vote par correspondance.

4.5. Description des catégories de personnes concernées

Personnes physiques majeures ayant déclaré leur résidence ou ayant résidé dans la commune et susceptibles de figurer sur les listes électorales de la commune.

4.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent l'administration de la population, notamment ceux à qui incombe la gestion des listes électorales.

5. Organisation (para-/péri-)scolaire

5.1. Description du traitement

Le traitement permet le contrôle de l'obligation scolaire des personnes concernées, la gestion des inscriptions scolaires ainsi que l'organisation de l'enseignement fondamental dans la commune. Par ailleurs, il permet la gestion de l'allocation des subsides aux élèves.

5.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, les deux conditions de légitimité suivantes, énumérées à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous les lettres a) et b) sont réunies dans le chef des responsables des traitements :

- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis et/ou
- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant d'une autorité publique, dont est investi le responsable du traitement.

Le traitement est mis en œuvre conformément aux bases légales suivantes :

- Loi du 6 février 2009 portant organisation de l'enseignement fondamental et ses règlements d'exécution ;

- Loi du 6 février 2009 relative à l'obligation scolaire ;

- Loi du 6 février 2009 concernant le personnel de l'enseignement fondamental.

5.3. Finalité(s) du traitement

Administration des élèves et des classes. Assistance aux élèves. Gestion et suivi de l'octroi de subsides.

5.4. Description des catégories de données

Les données relatives aux enseignants de la commune, notamment données d'identification, adresse, école, classe(s).

Les données relatives aux élèves, notamment données d'identification, matricule, adresse, date et lieu de naissance, parents, données de contact du tuteut ou responsable de l'enfant, caisse de maladie, titulaire et salle de classe, niveau d'études, catégorie d'élève (p.ex. membre du Lasep, élève utilisant le bus scolaire, éducation morale et laïque ou religieuse), échéances des visites médicales scolaires, notes (p.ex. accident dans la cour).

5.5. Description des catégories de personnes concernées

Les enfants (élèves) en âge d'obligation scolaire et leurs parents ou les personnes exerçant le droit de garde sur eux. Le personnel enseignant.

5.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres de la commission scolaire, au comité d'école ainsi qu'aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent l'organisation scolaire, ainsi qu'aux collaborateurs du service d'assistance sociale.

6. Gestion des services publics

6.1. Description du traitement

Le traitement consiste en la tenue et mise à jour des listes des ménages abonnés aux différents services publics, notamment poubelles, canalisation et eau. Il permet d'établir des factures et titres de recette pour lesdits services, l'établissement des pièces comptables y relatives ainsi que la gestion des propriétaires d'immeubles.

Le traitement permet en outre l'organisation des services publics, d'assurer le dépannage et l'assistance technique aux abonnés.

6.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, les deux conditions de légitimité suivantes, énumérées à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous les lettres a) et b) sont réunies dans le chef des responsables des traitements :

- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis et/ou

- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant d'une autorité publique, dont est investi le responsable du traitement.

Le traitement est mis en œuvre conformément aux bases légales suivantes :

- Article 17 de la loi modifiée du 17 juin 1994 relative à la prévention et à la gestion des déchets ;

- Loi du 19 décembre 2008 relative à l'eau.

6.3. Finalité(s) du traitement

Organisation, gestion et suivi des services publics offerts par la commune. Facturation. Assurer le dépannage et l'assistance technique aux abonnés des services publics.

6.4. Description des catégories de données

Les données relatives aux abonnés aux abonnés de la commune bénéficiant de services publics, notamment données d'identification, adresse de facturation, point de facturation, indications sur les services publics sollicités, notamment la lecture des compteurs, indications bancaires, montants à payer.

6.5. Description des catégories de personnes concernées

Les abonnés et clients des services publics (résidents ou non).

6.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent la gestion et la facturation des différents services publics respectifs ainsi qu'aux agents de la recette communale.

7. Gestion des cimetières et des inhumations

7.1. Description du traitement

Le traitement consiste en la tenue d'un fichier de données des personnes décédées sur la base des bulletins d'enterrement émis par l'Etat civil, en vue d'organiser et exécuter les enterrements sur le(s) cimetière(s) de la commune. Le traitement permet également la gestion des concessions des tombes ainsi que la tenue d'un fichier contenant les entreprises de pompes funèbres.

7.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, les deux conditions de légitimité suivantes, énumérées à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous les lettres b) et d) sont réunies dans le chef des responsables des traitements :

- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant d'une autorité publique, dont est investi le responsable du traitement ;
- le traitement 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 et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er.

Le traitement est mis en œuvre conformément aux bases légales suivantes :

- Décret du 4 thermidor an XIII (23 juillet 1805) relatif aux autorisations des officiers de l'état civil sur les inhumations ;
- Arrêté du Gouverneur général du 20 août 1814 concernant la police des inhumations ;
- Loi du 1er août 1972 portant réglementation de l'inhumation et de l'incinération des dépouilles mortelles ;
- Règlement grand-ducal du 21 juin 1978 relatif à la dispersion des cendres.

7.3. Finalité(s) du traitement

Organisation d'enterrements. Gestion des tombes et colombaires et des concessions. Gestion des pompes funèbres.

7.4. Description des catégories de données

Les données relatives aux personnes inhumées dans la commune, notamment données d'identification, lieu et date de naissance, date de décès, conjoint, données bancaires et financières, indications sur la concession de la tombe.

Les données d'identification des entreprises de pompes funèbres et des personnes assurant le service de permanence.

7.5. Description des catégories de personnes concernées

Les personnes inhumées dans la commune ainsi que leur conjoint éventuel ou d'autres membres de la famille. Entreprises de pompes funèbres.

7.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent l'organisation des inhumations.

8. Gestion des biens communaux

8.1. Description du traitement

Le traitement consiste en la tenue d'un fichier permettant la gestion des locations de logements ou de surfaces commerciales dans des immeubles appartenant à la commune.

8.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, les deux conditions de légitimité suivantes, énumérées à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous les lettres c) et d) sont réunies dans le chef des responsables des traitements :

- le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
- le traitement 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 et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er.

8.3. Finalité(s) du traitement

Gestion des locations de logements ou de surfaces commerciales dans des immeubles appartenant à la commune.

8.4. Description des catégories de données

Les données relatives aux personnes locataires d'un logement ou d'une surface commerciale appartenant à la commune, notamment données d'identification, données bancaires et financières, caractéristiques personnelles, composition du ménage, indications concernant le bien loué.

8.5. Description des catégories de personnes concernées

Les personnes ayant loué un logement ou une surface commerciale appartenant à la commune.

8.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent la gestion des biens communaux.

9. Organisation de la chasse et pêche

9.1. Description du traitement

Le traitement permet la gestion des syndicats de chasse sur le territoire de la commune. Il consiste en la tenue d'un fichier reprenant les propriétaires de territoires de chasse. En outre, le traitement permet d'établir le rôle de chasse, le calcul et le virement des indemnités dues aux propriétaires ainsi que la gestion des permis de pêche.

9.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, les deux conditions de légitimité suivantes, énumérées à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous les lettres a) et b) sont réunies dans le chef des responsables des traitements :

- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis et/ou
- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant d'une autorité publique, dont est investi le responsable du traitement.

Le traitement est mis en œuvre conformément aux bases légales suivantes :

- Loi modifiée du 18 mai 1885 sur la chasse ;
- Loi modifiée du 20 juillet 1925 sur l'amodiation de la chasse t l'indemnisation des dégâts causés par le gibier ;
- Loi modifiée du 28 juin 1976 portant réglementation de la pêche dans les eaux intérieures.

9.3. Finalité(s) du traitement

Gestion des syndicats de chasse. Etablissement du rôle de chasse. Indemnisation des propriétaires de territoires de chasse.

9.4. Description des catégories de données

Les données relatives aux propriétaires de fonds de chasse, notamment données d'identification, données bancaires et financières, lieu et surface du fonds de chasse.

9.5. Description des catégories de personnes concernées

Les propriétaires de fonds non bâtis sur lequel peut s'exercer le droit de chasse sur le territoire de la commune.

9.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent la gestion des syndicats de chasse.

10. Suivi administratif et gestion des chiens

10.1. Description du traitement

Le traitement consiste en la tenue d'un fichier reprenant les détenteurs de chiens résidant ou ayant résidé sur le territoire de la commune (ou représentants de personnes morales détenant des chiens). Il permet la gestion et le suivi administratif des chiens et de leurs détenteurs ainsi que la facturation de l'impôt dû.

10.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, la condition de légitimité énumérée à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous la lettre a) est remplie dans le chef des responsables des traitements :

- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis et/ou

Le traitement est mis en œuvre conformément aux bases légales suivantes :

- Loi du 9 mai 2008 relative aux chiens ;
- Règlement grand-ducal du 9 mai 2008 concernant l'identification et la déclaration des chiens ;

Règlement grand-ducal du 9 mai 2008 relatif aux cours de formation des détenteurs de chiens et aux cours de dressage des chiens ;

- Règlement grand-ducal du 9 mai 2008 énumérant les éléments de reconnaissance des types de chiens susceptibles d'être dangereux.

10.3. Finalité(s) du traitement

Tenue et gestion du fichier des chiens et de leurs détenteurs. Perception de l'impôt pour chiens.

10.4. Description des catégories de données

Les données relatives aux chiens ainsi qu'à leurs détenteurs, notamment les données d'identification, données bancaires et financières, données concernant les formations suivies, données concernant l'identification et le suivi du chien, à savoir le nom, la race, la robe, classement parmi les chiens susceptibles d'être dangereux, date naissance, suivi médical, cours de dressage suivis, réclamations reçues, historique ainsi que le montant des taxes dues.

10.5. Description des catégories de personnes concernées

Les personnes résidant ou ayant résidé dans la commune ou les sociétés avec siège social dans la commune et détenant des chiens ou ayant présenté une réclamation relative à un chien.

10.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent l'enregistrement et le suivi administratif des chiens et de leurs détenteurs.

11. Circulation : gestion des zones piétonnes

11.1. Description du traitement

Le traitement consiste en la tenue d'un fichier de personnes ayant le droit de circuler dans la/les zone(s) piétonne(s) de la commune.

11.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, les deux conditions de légitimité suivantes, énumérées à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous les lettres a) et b) sont réunies dans le chef des responsables des traitements :

- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis et/ou

- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant d'une autorité publique, dont est investi le responsable du traitement.

Le traitement est mis en œuvre conformément à la base légale suivante :

- Article 5 paragraphe 3 de la loi modifiée du 14 février 1955 concernant la règlementation de la circulation sur les voies publiques

11.3. Finalité(s) du traitement

Gestion des autorisations spéciales de circuler dans la/les zone(s) piétonne(s) de la commune.

11.4. Description des catégories de données

Données d'identification telles que nom, prénom et adresse, indications concernant le véhicule autorisé ainsi que l'objet et la durée de validité de l'autorisation.

11.5 Description des catégories de personnes concernées

Les personnes habitant en zone piétonne, celles qui y ont un magasin ou celles disposant d'autorisations spéciales de circuler en zone piétonne.

11.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent la gestion et le suivi des autorisations spéciales en matière de circulation routière.

12. Circulation : gestion du stationnement résidentiel

12.1. Description du traitement

Le traitement consiste en la tenue d'un fichier de personnes physiques et morales ayant des vignettes de stationnement résidentiel.

12.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, les deux conditions de légitimité suivantes, énumérées à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous les lettres a) et b) sont réunies dans le chef des responsables des traitements :

- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis et/ou
- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant d'une autorité publique, dont est investi le responsable du traitement.

Le traitement est mis en œuvre conformément à la base légale suivante :

- Article 5 paragraphe 3 de la loi modifiée du 14 février 1955 concernant la règlementation de la circulation sur les voies publiques

12.3. Finalité(s) du traitement

Gestion des vignettes de stationnement résidentiel et de leurs titulaires.

12.4. Description des catégories de données

Données d'identification telles que nom, prénom et adresse, données bancaires et financières, composition du ménage ainsi que des indications concernant le(s) véhicule(s) utilisé(s) et l'objet et la validité de la vignette.

12.5 Description des catégories de personnes concernées

Les personnes physiques et morales résidentes et non-résidentes bénéficiant de vignettes de stationnement résidentiel.

12.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent la gestion et le suivi des autorisations spéciales en matière de circulation routière.

13. Circulation : gestion des chantiers

13.1. Description du traitement

Le traitement consiste en la tenue d'un fichier permettant la gestion des chantiers occupant la voie publique.

13.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, la condition de légitimité suivante, énumérée à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous la lettre b) est remplie dans le chef des responsables des traitements :

- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant d'une autorité publique, dont est investi le responsable du traitement.

13.3. Finalité(s) du traitement

Gestion des autorisations d'occuper la voie publique par un chantier.

13.4. Description des catégories de données

Données d'identification telles que dénomination, nom, prénom et adresse, indications concernant le chantier ainsi que la période et la durée du chantier.

13.5. Description des catégories de personnes concernées

Les sociétés ou personnes désirant occuper la voie publique lors d'un chantier (bennes, bétonnières etc.).

13.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent la gestion et le suivi des autorisations spéciales en matière de circulation routière.

14. Circulation : gestion des autorisations spéciales

14.1. Description du traitement

Le traitement consiste en la tenue d'un fichier permettant le traitement des demandes d'autorisation d'exploitation de terrasses et d'étalages ainsi que la gestion et le suivi y relatif.

14.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, les deux conditions de légitimité suivantes, énumérées à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous les lettres a) et b) sont réunies dans le chef des responsables des traitements :

- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis et/ou
- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant d'une autorité publique, dont est investi le responsable du traitement.

Le traitement est mis en œuvre conformément aux bases légales suivantes :

- Article 5 paragraphe 3 de la loi modifiée du 14 février 1955 concernant la règlementation de la circulation sur les voies publiques
- Loi modifiée du 16 juillet 1987 concernant le colportage, la vente ambulante, l'étalage de marchandises et la sollicitation de commandes.

14.3. Finalité(s) du traitement

Traitement de demandes d'autorisation et d'exploiter des terrasses et d'étalages. Gestion et suivi des autorisations.

14.4. Description des catégories de données

Données d'identification telles que nom, prénom et adresse, indications concernant l'autorisation, la durée et la période de l'autorisation.

14.5 Description des catégories de personnes concernées

Toute personne désirant occuper la voie publique par une terrasse ou par une étalage à des fins commerciales.

14.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent la gestion et le suivi des autorisations spéciales en matière de circulation routière.

15. Gestion des activités de loisir, foyers/ crèches, maisons-relais et chèques-services accueil

15.1. Description du traitement

Le traitement consiste en la tenue d'un fichier permettant la gestion et la planification des activités de loisir organisées dans la commune, la gestion des maisons-relais, foyers, crèches ainsi que les chèques-services accueil. Il englobe les inscriptions et permet la facturation.

15.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, les deux conditions de légitimité suivantes, énumérées à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous les lettres b) et d) sont réunies dans le chef des responsables des traitements :

- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant d'une autorité publique, dont est investi le responsable du traitement.
- le traitement 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 et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er.

Le traitement est mis en œuvre conformément aux bases légales suivantes :

- Loi du 8 septembre 1998 réglant les relations entre l'Etat et les organismes oeuvrant dans les domaines social, familial et thérapeutique ;
- Règlement grand-ducal du 13 dévrier 2009 instituant le « chèque-service accueil ».

15.3 Finalité(s) du traitement

Organisation d'activités de loisir par la commune. Gestion des maisons-relais, foyers, crèches et chèques-services accueil. Planification, suivi et facturation.

15.4. Description des catégories de données

Données d'identification telles que nom, prénom, adresse, loisirs et intérêts, affiliations et situation de membres, indications concernant l'activité de loisir, maison-relais, foyer ou infrastructures utilisées.

15.5. Description des catégories de personnes concernées

Les personnes participant aux activités de loisir organisées par la commune et recourant aux services offerts par les maisons-relais et foyers ainsi que leurs tuteurs.

15.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent l'organisation, la gestion et le suivi d'activités de loisir.

16. Gestion et suivi du courrier

16.1. Description du traitement

Le traitement consiste en la tenue d'un fichier contenant des indications sur chaque courrier entrée à l'administration communale. Il permet la diffusion du

courrier dans les différents services ainsi que le suivi y relatif.

16.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, la condition de légitimité suivante, énumérée à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous la lettre d) est remplie dans le chef des responsables des traitements :

- le traitement 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 et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er.

16.3. Finalité(s) du traitement

Gestion et diffusion du courrier entrant et sortant. Suivi du courrier.

16.4. Description des catégories de données

Données d'identification, date d'entrée/sortie, objet du courrier, données relatives au suivi administratif.

16.5. Description des catégories de personnes concernées

Toute personne ayant introduit une demande d'autorisation, de renseignement ou tout autre type de courrier auprès de la commune.

16.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions et suivant l'objet du courrier, assurent le traitement et le suivi de celui-ci.

17. Gestion des activités des agents municipaux

17.1. Description du traitement

Le traitement consiste en la tenue d'un fichier permettant la gestion et le recouvrement des avertissements taxés de stationnement non réglementaire infligés aux contrevenants par les agents municipaux

17.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, les trois conditions de légitimité suivantes, énumérées à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous les lettres a), b) et d) sont réunies dans le chef des responsables des traitements :

- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis et/ou

- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant d'une autorité publique, dont est investi le responsable du traitement.

- le traitement 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 et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er.

Le traitement est mis en œuvre conformément à la base légale suivante :

- Article 99 de la loi communale modifiée du 13 décembre 1988.

17.3. Finalité(s) du traitement

Gestion des avertissements taxés et recouvrement de ceux-ci.

17.4. Description des catégories de données

Plaque d'immatriculation, marque et type du véhicule, lieu, date, heure, type de l'infraction et montant de l'avertissement taxé.

17.5. Description des catégories de personnes concernées

Toute personne ayant obtenu un avertissement taxé pour cause de stationnement no réglementaire par un agent municipal de la commune.

17.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, gèrent le recouvrement des avertissements taxés ainsi qu'aux agents de la recette communale.

18. Gestion du contentieux

18.1. Description du traitement

Le traitement permet la gestion du contentieux ainsi que le recouvrement des créances.

18.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, la condition de légitimité suivante, énumérée à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous la lettre d) est remplie dans le chef des responsables des traitements :

- le traitement 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 et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er.

18.3. Finalité(s) du traitement

Gestion du contentieux.

18.4. Description des catégories de données

Données d'identification, données bancaires et financières.

18.5. Description des catégories de personnes concernées

Les personnes étant impliquées dans des procédures de recouvrement (contentieuses) auprès de la commune.

18.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, gèrent le recouvrement des créances ainsi qu'aux agents de la recette communale.

19. Administration du personnel et gestion des ressources humaines

19.1. Description du traitement

Le traitement permet l'administration du personnel en ce qui concene le calcul des rémunérations, des charges déductibles ainsi que la gestion des congés, conformément aux dispositions législatives et réglementaires en vigueur et aux dispositions statutaires ou contractuelles régissant les membres du personnel.

Par ailleurs, le traitement permet la gestion des ressources humaines ainsi que le recrutement du personnel sur la base des curriculi vitae envoyés à la commune par des demandeurs d'emploi.

19.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, les deux conditions de légitimité suivantes, énumérées à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous les lettres

a) et c) sont réunies dans le chef des responsables des traitements :

- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
- le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci.

Le traitement est mis en œuvre conformément aux bases légales suivantes :

- Loi modifiée du 24 décembre 1985 fixant le statut général des fonctionnaires communaux ;
- Règlement grand-ducal du 11 janvier 1988 déterminant les pièces contenues dans le dossier personnel des fonctionnaires communaux ;
- Règlement grand-ducal du 15 novembre 2001 concernant le régime des employés communaux ;
- Code du Travail.

19.3. Finalité(s) du traitement

Administration du personnel et gestion des ressources humaines.

19.4. Description des catégories de données

Données d'identification, données bancaires et financières, caractéristiques personnelles, composition du ménage, profession et emploi, fonction, salaire, évaluations professionnelles, formation, photos.

19.5. Description des catégories de personnes concernées

Les fonctionnaires, employés communaux, employés privés, ouvriers et stagiaires ainsi que les collaborateurs externes travaillant auprès de la commune. Les demandeurs d'emploi stipulant à un poste au sein de la commune.

19.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent l'administration du personnel existant, la gestion des ressources humaines ainsi que celles qui opèrent le recrutement.

20. Relations publiques

20.1. Description du traitement

Le traitement consiste en la tenue d'un fichier d'adresses permettant d'envoyer des informations ou invitations à certaines personnes.

20.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, la condition de légitimité suivante, énumérée à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous la lettre d) est remplie dans le chef des responsables des traitements :

- le traitement 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 et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er.

20.3. Finalité(s) du traitement

Gestion des contacts, adresses et invitations.

20.4. Description des catégories de données

Données d'identification, fonction et titre, centres d'intérêt.

20.5. Description des catégories de personnes concernées

Personnes ayant demandé des informations, membres du Gouvernement, députés, conseillers communaux, fonctionnaiers ou autres personnes invitées à des manifestations.

20.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent la gestion des relations publiques.

21. Gestion des fournisseurs

21.1. Description du traitement

Le traitement consiste en la tenue d'un fichier comprenant les fournisseurs de la commune. Il permet la gestion des commandes ainsi que le paiement des factures y relatives.

21.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, les deux conditions de légitimité suivantes, énumérées à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous les lettres c) et d) sont réunies dans le chef des responsables des traitements :

- le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
- le traitement 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 et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er.

21.3. Finalité(s) du traitement

Gestion des fournisseurs. Comptabilité.

21.4. Description des catégories de données

Données d'identification, données bancaires et financières, profession et emploi, produits ou services fournis.

21.5. Description des catégories de personnes concernées

Les fournisseurs livrant ou ayant livré des biens à la commune ainsi que les prestataires de services de la commune.

21.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent la réception de produits, marchandises et de services, ainsi que les agents chargés du paiement de factures et de la comptabilité

22. Organisation des cours de formation

22.1. Description du traitement

Le traitement permet l'organisation et la facturation de divers cours de formation (p.ex. cours de langue, d'informatique etc).

22.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, les trois conditions de légitimité suivantes, énumérées à l'article 5 paragraphe

(1) de la loi modifiée du 2 août 2002, sous les lettres a) b) et d) sont réunies dans le chef des responsables des traitements :

- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant d'une autorité publique, dont est investi le responsable du traitement ;
- le traitement 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 et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er.

Le traitement est mis en œuvre conformément aux bases légales suivantes :

- Article 1er de la loi du 19 juillet 1991 portant création d'un Service de la formation des adultes et donnant un statut légal au Centre de langues Luxembourg ;
- Règlement grand-ducal du 31 mars 2000 ayant pour objet 1) de fixer les modalités des contrats conventionnant des cours pour adulte et les conditions d'obtention d'un label de qualité et d'une subvention ; 2) de créer une Commission Consultative à l'Education des Adultes.

22.3. Finalité(s) du traitement

Organisation, gestion, facturation et suivi de cours de formation.

22.4. Description des catégories de données

Données d'identification, données bancaires et financières, caractéristiques personnelles, loisirs et intérêts, éducation, formation et qualification, indications sur le cours suivi.

22.5. Description des catégories de personnes concernées

Les personnes participant à des cours de formation organisés par la commune.

22.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent l'organisation, la gestion et le suivi de cours de formation.

23. Subsides et subventions accordés par la commune

23.1. Description du traitement

Le traitement consiste en la tenue d'un fichier permettant le traitement des demandes de subsides et de subventions accordés par la commune ainsi que la gestion et le suivi y relatif.

23.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, les deux conditions de légitimité suivantes, énumérées à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous les lettres a) et b) sont réunies dans le chef des responsables des traitements :

- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis et/ous
- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant d'une autorité publique, dont est investi le responsable du traitement.

Le traitement est mis en œuvre conformément aux bases légales suivantes :

- Article 107 de la Constitution;

- Loi communale modifiée du 13 décembre 1988;
- Règlements de subsides communaux dûment approuvés et publiés.

23.3. Finalité(s) du traitement

Traitement de demandes de subsides et de subventions. Contrôle des conditions d'octroi et versement des montants accordés.

23.4. Description des catégories de données

Données d'identification telles que nom, prénom et adresse, numéro de téléphone ou adresse courriel, indications concernant le subside visé, la date d'entrée de la demande, des données bancaires pour le versement du subside

23.5. Description des catégories de personnes concernées

Toute personne désirant avoir un subside ou une subvention de la commune dans le cadre d'un règlement de subside ou de subvention existant.

23.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent la gestion et le suivi des demandes de subside et de subventions.

24. Liste des associations

24.1. Description du traitement

Le traitement consiste en la tenue d'un fichier permettant le traitement et la gestion des données et demandes des associations de la commune.

24.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, les deux conditions de légitimité suivantes, énumérées à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous les lettres a) et b) sont réunies dans le chef des responsables des traitements :

- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant d'une autorité publique, dont est investi le responsable du traitement.

Le traitement est mis en œuvre conformément aux bases légales suivantes :

- Loi communale modifiée du 13 décembre 1988;
- Règlements communaux réglant les demandes de subside des associations, la gestion de l'accès des associations aux infrastructures publiques et leur intégration dans la vie communale.

24.3. Finalité(s) du traitement

Traitement de demandes de subsides, envoi d'invitations, gestion de l'accès aux infrastructures publiques.

24.4. Description des catégories de données

Données d'identification telles que nom de l'association, nom, prénom, adresse, numéro de téléphone ou adresse courriel des responsables, des données bancaires pour le versement de subside, l'adresse du siège de l'association.

24.5 Description des catégories de personnes concernées

Les responsables des associations déclarées à la commune.

24.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent la gestion des relations avec les associations.

25. Gestion des réunions et des jetons de présence resp. indemnités pour les commissions communales et le conseil communal

25.1. Description du traitement

Le traitement consiste en la tenue d'un fichier permettant le traitement de l'organisation des réunions des commissions communaux et des conseils communaux respectivement du calcul et du versement des jetons de présence, des indemnités.

25.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, les deux conditions de légitimité suivantes, énumérées à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous les lettres a) et b) sont réunies dans le chef des responsables des traitements :

- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis et/ou
- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant d'une autorité publique, dont est investi le responsable du traitement.

Le traitement est mis en œuvre conformément aux bases légales suivantes :

- Articles 15 et 27 de la loi communale modifiée du 13 décembre 1988;
- Règlements communaux d'ordre interne réglant l'organisation des réunions du conseil communal et des commissions communaux ;
- Règlement grand-ducal du 13 février 2009 arrêtant les maxima des indemnités des bourgmestre et des échevins ;
- Règlements communaux fixant le montant des jetons de présence et des indemnités.

25.3. Finalité(s) du traitement

Traitement des données des membres du conseil communal et des commissions communaux.

25.4. Description des catégories de données

Données d'identification telles que nom, prénom, adresse, numéro de téléphone ou adresse courriel, des données bancaires pour le versement des jetons ou indemnités, relevé des présences.

25.5 Description des catégories de personnes concernées

Les membres du conseil communal et des commissions communaux

25.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent la gestion du conseil communal et des commissions communaux.

TRAITEMENT MIS EN ŒUVRE PAR LE BOURGMESTRE

Est à considérer comme responsable du traitement le bourgmestre mettant en œuvre le traitement de données à caractère personnel décrit sous le point 26 en relation avec les missions qui lui sont conférées.

26 Gestion des autorisations de bâtir

26.1. Description du traitement

Le traitement consiste en l'établissement et la gestion des autorisations de bâtir et permet aussi le suivi de celles-ci.

26.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, les deux conditions de légitimité suivantes, énumérées à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous les lettres a) et b) sont réunies dans le chef des responsables des traitements :

- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis et/ou
- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant d'une autorité publique, dont est investi le responsable du traitement.

Le traitement est mis en œuvre conformément aux bases légales suivantes :

- Article 37 de la loi modifiée du 19 juillet 2004 concernant l'aménagement communal et le développement urbain.

26.3. Finalité(s) du traitement

Traitement des demandes d'autorisation de bâtir. Gestion et suivi des autorisations de bâtir.

26.4. Description des catégories de données

Les données relatives aux personnes demandant une autorisation de bâtir, notamment, données d'identification, indications concernant le bâtiment et la construction autorisée, données de suivi.

26.5. Description des catégories de personnes concernées

Les demandeurs d'autorisations de bâtir sur le territoire de la commune.

26.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement au bourgmestre, aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent la gestion des autorisations de bâtir.

TRAITEMENT MIS EN ŒUVRE PAR L'OFFICIER DE L'ETAT CIVIL

Est à considérer comme responsable du traitements l'Officier de l'Etat Civil mettant en œuvre le traitement de données à caractère personnel décrit sous le point 27 de la présente en relation avec les missions qui lui sont conférées.

27. Etat civil

27.1. Description du traitement

Le traitement permet la constitution et la tenue et mise à jour des registres de l'état civil. Il permet en outre l'établissement des actes de l'état civil et l'édition d'extraits des actes de celui-ci.

27.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, les deux conditions de légitimité suivantes, énumérées à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous les lettres a) et b) sont réunies dans le chef des responsables des traitements :

- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis et/ou
- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant d'une autorité publique, dont est investi le responsable du traitement.

Le traitement est mis en œuvre conformément aux bases légales suivantes :

- Article 108 de la Consitution ;

- Articles 34 à 57, 63 à 70, 75 à 80 et 84 à 85 du Code civil ;
- Articles 69 et 70 de la loi communale modifiée du 13 décembre 1988 ;
- Décret du 20 juillet 1807 concernant les tables alphabétiques des actes de l'état civil ;
- Arrêté royal du 8 juin 1823 concernant des dispositions à l'égard des officiers de l'état civil ;
- Arrêté royal du 31 juillet 1828 qui prescrit aux officiers de l'état civil de donner de tous décès avis par écrit aux juges de paix ;
- Arrêté royal grand-ducal du 6 mai 1874 portant délégation des juges de paix pour la vérification des registres de l'état civil ;
- Loi du 1er avril 1968 relative aux mentions marginales des actes de l'état civil ;
- Loi du 9 juillet 2004 relative aux effets légaux de certains partenariats ;
- Loi du 23 décembre 2005 relative au nom des enfants.

27.3. Finalité(s) du traitement

Administration de la population. Tenue et mise à jour des actes de l'Etat civil.

27.4. Description des catégories de données

Les données de contact relatives aux officiers de l'Etat civil, médecins, tribunaux, consulats et maternités.

Les données relatives aux personnes résidant dans la commune nées, mariées ainsi qu'aux celles décédées dans la commune, notamment les données d'identification, date et lieu de naissance et de décès, adresse, profession, nationalité(s), employeur, date d'arrivée dans la commune, lieux de résidence précédents, signalétique de l'époux, de l'épouse, partenaire, des parents de ces derniers, du partenaire de l'ascendance et descendance, numéro de l'acte, données relatives au mariage, mentions marginales.

27.5. Description des catégories de personnes concernées

Les personnes physiques ayant déclaré leur résidence dans la commune ainsi que celles qui sont néées, mariées ou décédées dans la commune.

27.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement à l'Officier de l'Etat civil ainsi qu'aux membres du personnel communal qui, dans le cadre de leurs fonctions, assument des tâches en matière d'Etat civil.

TRAITEMENT MIS EN ŒUVRE PAR LE RECEVEUR COMMUNAL

Est à considérer comme responsable du traitement le receveur communal mettant en œuvre le traitement de données à caractère personnel décrit sous le point 28 de la présente en relation avec les missions qui lui sont conférées.

28. Perception d'impôts et de taxes

28.1. Description du traitement

Le traitement consiste en la tenue d'un fichier permettant la perception des taxes et impôts dus à la commune.

28.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, la condition de légitimité énumérée à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous la lettre a) est remplie dans le chef des responsables des traitements :

- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis et/ou

Le traitement est mis en œuvre conformément aux bases légales suivantes :

- Articles 99, 101, 102 et 107 paragraphe 3 de la Constitution ;
- Loi modifiée du 19 juillet 1904 sur les impositions communales ;
- Loi modifiée du 1er décembre 1936 sur l'impôt foncier ;
- Articles 29, 105, 106, 114, 135, 140 et 148 à 160 de la loi communale modifiée du 13 décembre 1988.

28.3. Finalité(s) du traitement

Perception d'impôts et de taxes.

28.4. Description des catégories de données

Les données relatives aux débiteurs de la commune et passibles d'impôts et de taxes, notamment données d'identification, données bancaires et financières, biens et services fournis et reçus, type de l'impôt ou de la taxe à payer.

28.5. Description des catégories de personnes concernées

Les personnes débitrices et contribuables de l'impôt foncier ainsi, les personnes redevables d'impôts et de taxes.

28.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent la perception des impôts et taxes communales.

TRAITEMENT MIS EN ŒUVRE PAR L'OFFICE SOCIAL

Est à considérer comme responsable du traitements l'office social mettant en œuvre le traitement de données à caractère personnel décrit sous le point 29 de la présente en relation avec les missions qui lui sont conférées.

29. Office social : gestion de l'aide sociale

29.1. Description du traitement

Le traitement permet le suivi et l'assistance sociale aux personnes qui sont dans un état nécessiteux ainsi que l'octroi de l'allocation de vie chère.

29.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, les deux conditions de légitimité suivantes, énumérées à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous les lettres a) et b) sont réunies dans le chef des responsables des traitements :

- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis et/ou
- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant d'une autorité publique, dont est investi le responsable du traitement.

Le traitement est mis en œuvre conformément aux bases légales suivantes :

- Loi modifiée du 29 avril 1999 portant création d'un droit à un revenu minimum garanti ;
- Loi du 18 décembre 2009 organisant l'aide sociale.

29.3. Finalité(s) du traitement

Assistance sociales aux personnes étant dans un état nécessiteux.

29.4. Description des catégories de données

Les données relatives aux personnes résidant dans la commune qui se trouvent dans un état nécessiteux, notamment nom, prénom, adresse, , civilité, date et lieu de naissance, nationalité(s), composition du ménage, enfants, profession et emploi, salaire, données bancaires et financières.

29.5. Description des catégories de personnes concernées

Personnes résidant dans la commune qui se trouvent dans un état nécessiteux.

29.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux assistantes et assistants sociaux ainsi qu'aux collaborateurs de l'office social ayant en charge la gestion de l'aide sociale.

TRAITEMENTS MIS EN ŒUVRE PAR UN RESPONSABLE DU TRAITEMENT À DÉFINIR DANS L'ENGAGEMENT FORMEL DE CONFORMITÉ

Il appartient aux communes de préciser dans l'engagement formel de conformité le(s) responsable(s) du traitement pour chacun des traitements décrits sous les points 30 à 33 (p.ex. syndicat de communes).

30. Gestion des abonnés à l'antenne collective

30.1. Description du traitement

Le traitement consiste en la tenue d'un fichier permettant la gestion des abonnés aux services de l'antenne collective de la commune ainsi que la facturation y relative.

30.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, les deux conditions de légitimité suivantes, énumérées à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous les lettres c) et d) sont réunies dans le chef des responsables des traitements :

- le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
- le traitement 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 et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er.

30.3. Finalité(s) du traitement

Gestion des abonnés à l'antenne collective. Facturation.

30.4. Description des catégories de données

Les données relatives aux abonnés au service de l'antenne collective telles que données d'identification, données bancaires et financières, composition du ménage, services abonnés.

30.5. Description des catégories de personnes concernées

Les abonnés au service de l'antenne collective.

30.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent la gestion et la facturation des services de l'antenne collective.

31. Organisation du service « Téléalarme »

31.1. Description du traitement

Le traitement consiste en la tenue d'un fichier permettant la gestion des personnes connectées au service « Téléalarme ».

31.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, les deux conditions de légitimité suivantes, énumérées à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous les lettres b), c) et e) sont réunies dans le chef des responsables des traitements :

- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant d'une autorité publique, dont est investi le responsable du traitement ;
- le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
- le traitement est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée.

31.3. Finalité(s) du traitement

Gestion et organisation du service public « Téléalarme ».

31.4. Description des catégories de données

Les données relatives aux personnes connectées au service « Téléalarme », notamment données d'identification, données bancaires et financières, caractéristiques personnelles, composition du ménage et indication des personnes de contact en cas d'urgence.

31.5. Description des catégories de personnes concernées

Les abonnés au service « Téléalarm » ainsi que les personnes à contacter en cas d'urgence.

31.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent la gestion du service « Téléalarme », ainsi qu'aux collaborateurs des services d'urgence sollicités.

32. Organisation du service « Repas sur roues »

32.1. Description du traitement

Le traitement consiste en la tenue d'un fichier reprenant les personnes bénéficiant du service « repas sur roues » et permet d'organiser les commandes et la livraison des repas.

32.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, la condition de légitimité suivante, énumérée à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous la lettres b) est remplie dans le chef des responsables des traitements :

- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant d'une autorité publique, dont est investi le responsable du traitement.

32.3. Finalité(s) du traitement

Gestion et organisation du service public « repas sur roues ».

32.4. Description des catégories de données

Les données relatives aux personnes bénéficiant du service « Repas sur roues », notamment données d'identification, données bancaires et financières, caractéristiques personnelles, composition du ménage et indications sur les repas à livrer.

32.5. Description des catégories de personnes concernées

Les personnes bénéficiant du service « Repas sur roues » de la commune.

32.6 Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent la gestion et le suivi du service « Repas sur roues » .

33. Organisation des transports en commun

33.1 Description du traitement

Le traitement permet l'organisation et la planification des lignes de transports en commun (autobus, « Flexibus », « NovaBus », « NightRider », etc.) de la commune ainsi que la gestion des abonnés et usagers de ceux-ci.

33.2. Condition de légitimité

Concernant les traitements opérés par les responsables des traitements en la matière, la condition de légitimité énumérée à l'article 5 paragraphe (1) de la loi modifiée du 2 août 2002, sous la lettre b) est remplie dans le chef des responsables des traitements :

- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant d'une autorité publique, dont est investi le responsable du traitement.

33.3. Finalité(s) du traitement

Organisation et planification de transports en commun.

33.4. Description des catégories de données

Les données d'identification des abonnés et usagers de transports en commun organisés par la commune, données bancaires et financières, données concernant les lignes d'autobus/transports en commun, horaire.

33.5. Description des catégories de personnes concernées

Les abonnés et usagers des transports communs organisés par la commune.

33.6. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Aucune communication, avec ou sans le consentement de la personne concernée respectivement de leurs représentants légaux (enfants mineurs, majeurs sous tutelle) de données à des tiers ne peut avoir lieu, sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

L'accès interne aux données doit être accordé exclusivement aux membres du personnel communal qui, dans le cadre de leurs fonctions, assurent l'organisation et la gestion des transports en commun.

II. Dispositions supplémentaires concernant tous les traitements

1. Qualité des données

Les données collectées et traitées doivent être adéquates, pertinentes et non excessives au regard de la finalité que poursuit leur traitement.

Les traitements doivent :

- ne porter que sur des données objectives aisément contrôlables par les intéressés grâce à l'exercice du droit individuel d'accès ;
- ne pas donner lieu à des interconnexions autres que celles expressément prévues par un texte légal ;
- ne pas donner lieu à des rapprochements autres que ceux nécessaires à l'accomplissement des

devoirs compris dans les finalités énoncées au points 1 à 31 ci-dessus ;

2. Droits des personnes concernées

Les responsables du traitement visés aux points I., II., III. et IV. doivent veiller au respect des droits des personnes concernées faisant l'objet du chapitre VI. de la loi modifiée du 2 août 2002. En particulier, ils sont tenus de fournir aux personnes concernées les informations prévues à l'article 26 de la loi pour les traitements de données décrits ci-dessus.

3. Durée de conservation

Conformément à l'article 4 paragraphe (1) lettre (d) de la loi du 2 août 2002, les données traitées ne peuvent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées.

Cette durée peut varier en fonction des traitements en tenant compte de la nature et de la finalité des traitements ainsi que des textes légaux sur base desquels les traitements sont mis en œuvre.

4. Pays tiers vers lesquels des transferts de données sont envisagés

Les données à caractère personnel faisant l'objet de traitements par les responsables du traitement définis dans la présente ne doivent pas être transférées à destination de pays tiers (hors Union européenne), sauf si le consentement de la personne concernée visé à l'article 19 paragraphe (1) lettre (a) de la loi a été obtenu ou si une autre dérogation visée aux lettres (b) à (f) du même article est remplie.

5. Subordination

Les responsables du traitement mettant en œuvre les traitements visés par la présente ont la faculté de choisir un sous-traitant agissant au nom et pour compte des responsables, à condition que ce sous-traitant apporte des garanties suffisantes au regard des mesures de sécurité technique d'organisation relatives aux traitements à effectuer. Il incombe au responsable du traitement ainsi qu'au sous-traitant de veiller au respect de ces mesures.

Conformément à l'article 21 de la loi, toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, ainsi que le sous-traitant lui-même, et qui accède à des données ne peut les traiter que sur instruction du responsable du traitement, sauf en vertu d'obligations légales.

Par ailleurs, le responsable du traitement doit s'assurer que les personnes autorisées ne peuvent accéder qu'aux données relevant de leur compétence (contrôle d'accès) et au regard des finalités du traitement en question. Il incombe dès lors au responsable du traitement d'établir et de tenir à jour une liste des personnes précisant les modalités de leurs accès aux données.

6. Mesures de sécurité prévues aux articles 22 et 23

Pour l'essentiel les procédures opérées par les communes font l'objet d'un traitement informatique. Les dossiers, documents, listes et données appréhendés sous forme automatisées doivent faire l'objet de mesures de sécurité organisationnelles et techniques suffisantes conformément aux articles 19 à 24 de la loi du 2 août 2002.

L'ensemble des mesures prises pour assurer la sécurité du traitement en application des articles 22 et 23 de la loi du 2 août 2002 doit conférer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger, le tout en fonction du risque d'atteinte à la vie privée, ainsi que de l'état de l'art et des coûts liés à la mise en œuvre dudit traitement.

Ainsi décidé à Luxembourg en date du 15 janvier 2010.

La Commission nationale pour la protection des données

Gérard Lommel	Président
Pierre Weimerskirch	Membre effectif
Thierry Lallemang	Membre effectif

Participations aux travaux européens

Documents adoptés par le groupe de travail en 2010

Document	Date d'adoption	Référence
Avis 8/2010 sur la loi applicable	16.12.2010	WP 179
Avis 7/2010 sur la communication de la Commission européenne relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers	12.11.2010	WP 178
Avis 6/2010 sur le niveau de protection des données à caractère personnel dans la République orientale de l'Uruguay	12.10.2010	WP 177
Liste des questions les plus fréquentes soulevées par l'entrée en vigueur de la décision 2010/87/UE de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil	12.07.2010	WP 176
Avis 5/2010 sur la proposition 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)	13.07.2010	WP 175
Avis 4/2010 sur le code de conduite européen de la FEDMA relatif à l'exploitation de données à caractère personnel dans le cadre d'opérations de marketing direct	13.07.2010	WP 174
Avis 3/2010 sur le principe de la responsabilité	13.07.2010	WP 173
Rapport 01/2010 sur la deuxième action commune de contrôle de l'application de la législation UE: Respect au niveau national par les fournisseurs de télécommunications et les fournisseurs de services Internet (FSI) des obligations découlant de la législation nationale sur la conservation des données relatives au trafic, sur la base juridique des articles 6 et 9 de la directive 2002/58/CE «vie privée et communications électroniques» et de la directive 2006/24/CE sur la conservation des données la modifiant	13.07.2010	WP 172
Avis 2/2010 sur la publicité comportementale en ligne	22.06.2010	WP 171
Programme de travail 2010-2011	15.02.2010	WP 170
Avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant»	16.02.2010	WP 169

Article 29 Working Party – « Programme de travail 2010-2011 »

Adopté le 15 février 2010

Mission

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

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

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

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

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

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

Activités en 2010-2011

Pour la période 2010-2011, le groupe de travail s'est fixé pour objectif non seulement d'assurer une mise en oeuvre cohérente et correcte du cadre juridique actuel, mais également de préparer l'avenir. Il sera nécessaire de relever des défis tels que les nouvelles avancées technologiques, les difficultés liées à la mondialisation et les changements institutionnels engendrés par le traité de Lisbonne.

Le groupe de travail entend préciser et renforcer le rôle de tous les acteurs dans le domaine de la protection des données: personnes concernées, responsables du traitement des données et autorités chargées de la protection des données. Il veut également assurer la prise en compte du respect de la vie privée dès la conception dans tous les domaines, ce qui peut donner lieu à l'implication de nouveaux acteurs.

Le groupe de travail examinera aussi sa propre efficacité et poursuivra l'amélioration de ses méthodes de travail, en étroite collaboration avec le secrétariat. Il intensifiera en outre les échanges avec d'autres institutions et organisations.

Compte tenu des défis exposés ci-dessus, le groupe de travail entend se concentrer sur quatre thèmes stratégiques principaux et quelques questions d'actualité qu'il juge les plus pertinents et urgents pour le développement de la protection des données:

I. Mettre en oeuvre la directive et préparer un futur cadre juridique global

II. Faire face à la mondialisation

III. Répondre aux défis technologiques

IV. Accroître l'efficacité du groupe de travail «article 29» et des autorités chargées de la protection des données

V. Questions d'actualité

Par ailleurs, le groupe de travail reste disponible pour traiter les demandes d'avis de la Commission, ainsi que toutes autres questions imprévues. Il est en particulier prêt à conseiller la Commission dans les domaines qui touchent à l'avenir de la protection de la vie privée, par exemple en développant certaines questions liées à la prise en compte du respect de la vie privée dès la conception, à l'obligation de rendre compte ou au renforcement du rôle des personnes concernées.

Ces questions peuvent être étroitement liées à plusieurs niveaux, et le groupe de travail choisira donc le meilleur moyen de les traiter. Il examinera la mise en oeuvre de ce programme de travail à intervalles réguliers et se réserve le droit, le cas échéant, de le préciser davantage ou de le mettre à jour.

Méthodologie

Parmi les quatre thèmes stratégiques principaux qui ont été choisis (de I à IV), des choix stratégiques spécifiques ont été faits (tels que règles d'entreprise contraignantes, informatique dématérialisée, application des règles). Outre les priorités choisies, le programme de travail mentionne les travaux en cours qui correspondent aux quatre thèmes stratégiques et qu'il est nécessaire de poursuivre (notamment niveau de protection adéquat, moteurs de recherche, aspects financiers). Ces choix sont le résultat des priorités évoquées par les membres du groupe de travail.

I. Assurer la mise en oeuvre correcte du cadre juridique actuel et préparer l'avenir

- Interpréter les dispositions clés de la directive 95/46/CE (responsable du traitement des données/sous-traitant, droit applicable, limitation des finalités et raisons du traitement)
- Mettre en oeuvre la directive «Vie privée et communication électronique» telle que modifiée
- Évaluer les conséquences du traité de Lisbonne

Ce thème comprend des travaux sur le suivi des questions relatives à l'avenir du respect de la vie privée.

II. Faire face à la mondialisation

- Développer des règles d'entreprise contraignantes
- Participer aux travaux sur la normalisation (par exemple ISO)
- S'aligner sur les normes internationales (déclaration de Madrid)
- Participer à l'examen des lignes directrices de l'OCDE

Ce thème comprend des travaux sur :

- la sphère de sécurité
- le niveau de protection adéquat des pays tiers

III. Défis technologiques

- Informatique dématérialisée
- Profilage (y compris la publicité comportementale)

Ce thème comprend des travaux sur:

- les moteurs de recherche et le droit à l'oubli
- les sites de socialisation
- l'évaluation de l'impact de l'identification par radiofréquence (RFID) sur la protection de la vie privée

IV. Accroître l'efficacité des autorités chargées de la protection des données et du groupe de travail «article 29»

- Réfléchir sur le rôle du groupe «article 29»
- Renforcer l'application des règles (développement et amélioration des méthodes d'enquête, harmonisation des pouvoirs des autorités chargées de la protection des données et promotion de la coopération internationale entre les autorités chargées de la protection de la vie privée)

V. Questions sectorielles:

- Aspects financiers
- Données relatives aux voyageurs
- Mise à jour du document de travail sur la biométrie (WP80)
- Éventuellement: mise à jour du document de travail sur l'administration électronique et la gestion des identifiants (WP73) [à décider en vue d'un développement ultérieur]

Fait à Bruxelles, le 15 février 2010

Pour le groupe de travail
Le président
Jacob KOHNSTAMM

Working Party 29 – « Avis 2/2010 sur la publicité comportementale en ligne »

Adopté le 22 juin 2010

Table des matières

Résumé

La publicité comportementale consiste à suivre les utilisateurs lorsqu'ils surfent sur l'internet et à constituer des profils à travers le temps, qui serviront ultérieurement à leur proposer des publicités correspondant à leurs centres d'intérêt. Bien que le groupe de travail ne remette pas en cause les avantages économiques que les parties prenantes peuvent tirer de la publicité comportementale, il est fermement convaincu que cette pratique ne saurait exister aux dépens du droit des personnes à la protection de leurs données et de leur vie privée. Le cadre réglementaire de l'UE en matière de protection des données, qui établit des garanties spécifiques, doit être respecté. Afin d'en favoriser et d'en promouvoir le respect, le présent avis précise le cadre juridique applicable aux acteurs de la publicité comportementale.

Le groupe de travail souligne en particulier que les fournisseurs de réseaux publicitaires sont soumis à l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques», selon lequel le placement de cookies ou de dispositifs similaires dans l'équipement terminal d'un utilisateur ou l'accès à des informations par l'intermédiaire de ces dispositifs n'est autorisé qu'avec le consentement informé de l'utilisateur. Or le groupe constate que le paramétrage des navigateurs actuellement disponibles et les mécanismes d'«opt-out» n'assurent la manifestation d'un consentement que dans des cas très restreints. Il demande donc aux fournisseurs de réseaux publicitaires de mettre en place des mécanismes d'«opt-in» préalable qui nécessitent une action positive des personnes concernées indiquant leur acceptation que des cookies ou des dispositifs similaires soient placés sur leur équipement et que leur comportement sur l'internet soit suivi aux fins de l'envoi de publicités personnalisées. Le groupe de travail considère qu'une acceptation unique par les utilisateurs de recevoir un cookie peut également emporter leur acceptation de lectures ultérieures du cookie et, partant, du suivi de leur navigation sur l'internet. Par conséquent, pour répondre aux exigences énoncées à l'article 5, paragraphe 3, il ne serait pas nécessaire de demander un consentement pour chaque lecture du cookie. Or, pour que les personnes concernées n'oublient pas qu'elles font l'objet de ce suivi, les fournisseurs de réseaux publicitaires devraient: i) limiter la portée du consentement dans le temps; ii) offrir la possibilité de révoquer aisément le consentement et iii) créer des outils visibles qui s'affichent lorsque le suivi a lieu. On éviterait ainsi d'importuner les utilisateurs avec des avis multiples tout en veillant à ce que l'envoi des cookies et le suivi ultérieur du comportement de navigation sur l'internet à des fins de publicités personnalisées ne puissent avoir lieu qu'avec le consentement informé des personnes concernées.

Comme la publicité comportementale repose sur l'utilisation d'identifiants permettant la création de profils d'utilisateurs extrêmement détaillés qui, la plupart du temps, seront considérés comme des données à caractère personnel, la directive 95/46/CE s'applique également. Le groupe de travail explique comment les fournisseurs de réseaux de publicité en ligne doivent se conformer aux obligations qu'impose cette directive, notamment en matière de droits d'accès, de rectification, d'effacement, de conservation, etc. Les diffuseurs étant susceptibles d'assumer une certaine responsabilité dans le traitement des données effectué à des fins de publicité comportementale, le groupe de travail appelle les diffuseurs à partager avec les fournisseurs de réseaux de publicité en ligne la responsabilité d'informer les particuliers et il encourage la créativité et l'innovation dans ce domaine. En raison de la nature de la publicité comportementale, des exigences de transparence sont une condition essentielle pour que les particuliers soient en mesure de donner leur consentement à la collecte et au traitement de leurs données à caractère personnel et d'exercer un véritable choix. L'avis décrit les obligations d'information imposées aux diffuseurs/fournisseurs de réseaux publicitaires à l'égard des personnes concernées, en faisant plus particulièrement référence à la directive «vie privée et communications électroniques», qui exige que les utilisateurs reçoivent des «informations précises et complètes».

L'avis analyse et précise les obligations prévues par le cadre juridique applicable. Il ne prescrit toutefois pas la manière dont, sur le plan technologique, ces obligations doivent être satisfaites. En revanche, en différents domaines, le groupe de travail invite les professionnels concernés à engager un dialogue avec lui afin de proposer des solutions techniques et

d'autres moyens de se conformer dans les meilleurs délais au cadre décrit dans l'avis. À cet effet, le groupe de travail contactera les parties prenantes afin de leur demander leur contribution. Les entités qui ne seront pas expressément consultées sont invitées à envoyer leurs contributions au secrétariat du groupe de travail «Article 29».

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

établi par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995[50],

vu l'article 29, l'article 30, paragraphe 1, point a), et l'article 30, paragraphe 3, de ladite directive, et l'article 15, paragraphe 3, de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002,

vu l'article 255 du traité CE et le règlement (CE) n° 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission,

vu son règlement intérieur,

A ADOPTÉ LE PRÉSENT AVIS:

1. Introduction

La publicité en ligne est une source essentielle de revenus pour un large éventail de services en ligne et elle est un facteur clé de la croissance et de l'expansion de l'économique numérique. Cependant, la pratique même de la publicité comportementale suscite de sérieuses inquiétudes en termes de protection des données et de la vie privée. La technologie de base de l'internet permet en effet aux fournisseurs de réseaux publicitaires de tracer des personnes concernées sur différents sites et à travers le temps. Les informations réunies sur le comportement de navigation de ces personnes sont ensuite analysées afin de constituer des profils détaillés sur leurs centres d'intérêt. Ces profils peuvent alors servir à leur envoyer des publicités personnalisées.

Étant donné l'essor que connaît la publicité comportementale fondée sur l'utilisation de cookies traceurs et de dispositifs similaires, et son intrusion considérable dans la vie privée des internautes, le groupe de travail a décidé de consacrer le présent avis à la publicité comportementale en ligne pratiquée

sur plusieurs sites web, sans préjudice d'avis futurs qui pourraient se pencher sur d'autres techniques publicitaires.

Par cet avis, le groupe de travail entend préciser le cadre juridique applicable aux acteurs de la publicité comportementale. Il invite également les professionnels concernés à proposer des mesures techniques et d'autre nature pour se conformer à ce cadre dans les meilleurs délais et à engager avec lui un dialogue sur ces mesures. Enfin, le groupe de travail évaluera la situation et prendra les mesures appropriées qui s'imposent pour assurer le respect du cadre juridique décrit dans le présent avis.

2. La publicité comportementale en ligne

La publicité par média interactif recouvre diverses méthodes destinées à créer des publicités plus ciblées. Ces méthodes peuvent être classées en plusieurs catégories, dont la publicité contextuelle, la publicité segmentée et la publicité comportementale.

La *publicité comportementale* est une forme de publicité qui repose sur l'observation du comportement des individus au fil du temps. Elle vise à étudier les caractéristiques de ce comportement à travers leurs actions (visites successives de sites, interactions, mots clés, production de contenu en ligne, etc.) pour établir un profil spécifique et proposer aux personnes concernées des publicités adaptées à leurs centres d'intérêt ainsi déduits.

Alors que la publicité contextuelle[51] et la publicité segmentée[52] recourent à des «instantanés» de ce que

[50] Journal officiel L 281 du 23.11.1995, p. 31.

[51] La publicité contextuelle est une publicité choisie en fonction du contenu que la personne concernée est en train de consulter. Dans le cas d'un moteur de recherche, le contenu peut être déduit des mots clés saisis pour la recherche, de la recherche précédente ou de l'adresse IP de l'utilisateur, si elle indique sa localisation géographique probable.

[52] Publicité choisie en fonction des caractéristiques connues de la personne concernée (âge, sexe, localisation, etc.) qu'elle a elle-même indiquées en s'inscrivant sur un site.

les personnes concernées regardent ou font sur un site web particulier, ou aux caractéristiques connues des utilisateurs, la publicité comportementale est susceptible de fournir aux annonceurs une image très détaillée de la vie en ligne d'une personne concernée, en indiquant un grand nombre des sites web et des pages spécifiques consultés, combien de temps certains articles ou éléments ont été regardés, dans quel ordre, etc.

2.1. Modes de diffusion de la publicité comportementale

La publicité comportementale s'appuie sur les acteurs suivants: *(a) les fournisseurs de réseaux publicitaires*, qui sont les principaux diffuseurs de publicité comportementale puisqu'ils mettent en relation les diffuseurs et les annonceurs; *(b) les annonceurs* qui veulent promouvoir un produit ou un service auprès d'un public spécifique et *(c) les diffuseurs,* qui sont les propriétaires des sites web et cherchent à tirer des revenus de la vente d'espaces publicitaires sur leur(s) site(s)[53].

L'affichage de publicités par les fournisseurs de réseaux publicitaires fonctionne comme suit: le diffuseur réserve un espace visuel sur son site pour afficher une annonce et abandonne la suite du processus à un ou plusieurs fournisseurs de réseaux publicitaires. Ces derniers sont chargés de distribuer les annonces aux diffuseurs en obtenant l'effet optimal. Les fournisseurs de réseaux publicitaires contrôlent la technologie de ciblage et les bases de données correspondantes.

Plus le fournisseur de réseau publicitaire est important, plus il possède de ressources pour suivre les utilisateurs et «tracer» leur comportement[54]. Généralement,

l'annonceur négocie avec un ou plusieurs fournisseurs de réseaux publicitaires et il n'aura pas nécessairement connaissance de l'identité de tous les diffuseurs (le cas échéant) qui vont distribuer sa publicité. Parallèlement, un diffuseur peut avoir conclu plusieurs contrats avec différents fournisseurs de réseaux publicitaires, par exemple en réservant plusieurs emplacements sur son site web pour différents fournisseurs de réseaux publicitaires.

La tendance actuelle est à la collaboration entre les fournisseurs de réseaux publicitaires par un mécanisme de mise aux enchères[55].

2.2. Techniques de traçage

La plupart des techniques de traçage et de publicité utilisées pour diffuser les publicités comportementales recourent à une certaine forme de traitement du côté du client. Elles exploitent en effet des informations provenant du navigateur et de l'équipement terminal de l'utilisateur. La principale technique de traçage servant à suivre les utilisateurs sur l'internet repose sur les «cookies traceurs». Les cookies offrent la possibilité de tracer la navigation d'un utilisateur sur une longue

[53] Outre le canal des fournisseurs de réseaux publicitaires, la publicité comportementale peut également passer par une annonce sur un site. Par cette méthode, l'annonceur indique au diffuseur le public ciblé, par des critères qui peuvent dépasser les informations démographiques telles que le triplet classique «tranche d'âge, sexe, pays» pour adopter des critères bien plus précis (mots clés ou centres d'intérêt). Le diffuseur se charge alors d'afficher le contenu publicitaire auprès de la cible choisie, d'appliquer la technique de ciblage et de contrôler le placement et la diffusion de l'annonce. Cette méthode est utilisée sur certaines plateformes de réseaux sociaux qui permettent de cibler les internautes en fonction de leurs centres d'intérêt.

[54] New York Times, «To Aim Ads, Web is Keeping Closer Eye on You», 10 mars 2008. L'article cite des statistiques sur la fréquence à laquelle les grands fournisseurs de réseaux publicitaires tracent les visites de sites web particuliers. Dans le cas du fournisseur de réseau publicitaire de Yahoo!, un utilisateur (américain) moyen était censé être tracé 2,520 fois par mois à la fin 2007. http://www.nytimes.com/2008/03/10/technology/10privacy.html?_r=1&scp=3&sq=%22They%20know%20more%20than%20you%20think%22&st=cse

[55] La plupart des grands fournisseurs de réseaux publicitaires ont mis en place une structure de collaboration avec de nombreux réseaux secondaires. Par exemple: liste des partenaires de Google Adsense: http://www.google.com/support/adsense/bin/answer.py?answer=94149, liste des partenaires de Yahoo!: http://info.yahoo.com/privacy/us/yahoo/thirdparties/. Ce système fonctionne comme suit: le réseau primaire met un espace publicitaire aux enchères entre plusieurs réseaux de publicité et choisit la meilleure offre.

période et, théoriquement, sur plusieurs sites web différents[56].

Cette technique fonctionne habituellement comme suit: le fournisseur de réseau publicitaire dépose généralement un cookie traceur sur l'équipement terminal de la personne concernée[57] la première fois qu'elle visite un site contenant une annonce du même réseau. Le cookie est une courte combinaison alphanumérique stockée (et ensuite récupérée) sur l'équipement terminal de la personne concernée par un fournisseur de réseau[58]. Dans le cadre de la publicité comportementale, le cookie permet à ce dernier de reconnaître un visiteur antérieur qui revient sur ce site web ou consulte un autre site partenaire du fournisseur de réseau publicitaire. Ces visites répétées permettront au fournisseur de réseau d'élaborer un profil du visiteur, qui sera utilisé pour lui transmettre des publicités personnalisées. Comme ces cookies traceurs sont placés par un tiers différent du serveur qui affiche le contenu principal de la page (c'est-à-dire le diffuseur), ils sont souvent appelés «cookies tiers».

Les cookies sont liés à un domaine: un cookie ne peut être lu ou modifié que par un site web issu d'un domaine similaire[59] (par exemple, un cookie placé par un fournisseur de réseau publicitaire a.monsite.com peut être lu par b.monsite.com, mais pas par un fournisseur de réseau publicitaire c.autre.com). Les cookies ont des durées de vie variables. Cette durée peut ou non être prolongée par de nouvelles visites sur le même site (cela dépend d'une décision de conception du programmeur). Soit les «cookies persistants» ont une date d'expiration précise éloignée dans le futur, soit ils restent actifs jusqu'à leur suppression manuelle.

La plupart des navigateurs internet offrent la possibilité de bloquer les cookies tiers. Certains navigateurs gèrent des sessions de navigation «privée», qui détruisent automatiquement tous les cookies créés lorsque la fenêtre de navigation se ferme[60].

Certains fournisseurs de réseaux publicitaires remplacent ou complètent les cookies traceurs traditionnels par de nouvelles techniques de traçage de pointe telles que les «flash cookies» («local shared objects»)[61]. Les «flash cookies» ne peuvent pas être supprimés par les paramètres traditionnels de protection de la confidentialité d'un navigateur.

56 D'autres techniques de traçage reposent, par exemple, sur l'utilisation des adresses IP et des signatures desnavigateurs. L'Electronic Frontier Foundation a étudié le caractère identifiable de la signature individuelle du navigateur (agent d'utilisateur), notamment le logiciel utilisé, la version, la langue et les modules d'extension installés: http://panopticlick.eff.org/. En ce qui concerne les adresses IP, une entreprise américaine nouvellement créée vient d'annoncer qu'elle possédait une base de données de 65 millions d'adresses IP, avec les noms et les adresses: ttp://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=123280.

57 Si une personne concernée utilise différents navigateurs, les cookies seront différents pour chaque navigateur.

58 Cette combinaison alphanumérique peut être utilisée pour des finalités très variées, comme mémoriser les préférences, stocker les informations des sessions de navigation ou identifier une personne concernée par un identifiant unique.

59 Il existe toutefois des solutions simples pour les parties qui coopèrent et souhaitent contourner ces restrictions et partager des cookies entre elles. Un propriétaire de domaine peut configurer son DNS pour autoriser un tiers à utiliser l'un de ses sous-domaines. Le tiers pourra alors partager certains cookies avec le propriétaire de domaine. D'autres techniques font appel à JavaScript pour adresser des requêtes supplémentaires à d'autres serveurs, en autorisant encore plus de parties à relier ou à synchroniser leurs données de traçage (http://blog.kruxdigital.com/2010/02/24/cookie-synching/).

60 Les versions les plus récentes de nombreux navigateurs populaires (internet Explorer 8, Google Chrome, Firefox, Safari, etc.) gèrent des sessions de navigation qui effacent automatiquement tous les cookies installés au cours de la session.

61 Le World Wide Web Consortium ou W3C met au point une norme «DOM Storage» (stockage de «Document Object Model») qui permettra e stocker localement de grandes quantités de données en plaçant des scripts sur l'ordinateur de l'utilisateur.

Il semblerait qu'ils soient expressément utilisés pour rétablir des «cookies traditionnels» qui ont été refusés ou effacés par la personne concernée[62].

Cette pratique est connue sous le nom de *respawning* («résurrection»). Dans le présent avis, le terme «cookies» sera employé pour toutes les techniques fondées sur le principe du stockage et de l'accès à des informations sur l'équipement terminal de l'utilisateur, sauf mention contraire.

Comme indiqué plus haut, un fournisseur de réseau publicitaire isolé ne peut généralement suivre qu'une partie du comportement de navigation de la personne concernée, parce que ses capacités de traçages sont limitées au groupe de diffuseurs qui lui sont liés. Une autre méthode a toutefois été testée récemment, consistant à conclure un partenariat entre le fournisseur de réseau publicitaire et un fournisseur de services internet (FSI) afin de suivre le contenu de la navigation de l'utilisateur et de placer des cookies traceurs dans tous les échanges internet non cryptés[63]. Le groupe de travail n'a été informé d'aucune application de cette technique dans l'Union européenne pour l'instant, mais il considère que son utilisation soulève de grandes questions juridiques dépassant le cadre du traitement des données à caractère personnel, indépendamment de la finalité de l'utilisation des données.

L'analyse de cette technique publicitaire ne relève cependant pas du présent avis.

2.3. Constitution de profils, types d'identifiants

Il existe deux grandes méthodes de constitution de profils d'utilisateurs: ***i)*** **les profils prédictifs** sont établis par déduction en observant le comportement individuel et collectif des utilisateurs dans le temps, notamment en suivant les pages visitées et les publicités qu'ils ont vues ou sur lesquelles ils ont cliqué; ***ii)*** **les profils explicites** sont établis à partir des données à caractère personnel que les personnes concernées fournissent elles-mêmes à un service web, notamment par leur inscription. Ces deux méthodes peuvent être combinées. En outre, les profils prédictifs peuvent devenir explicites plus tard, lorsqu'une personne concernée s'identifie pour entrer sur un site web[64].

Les sociétés de publicité en ligne constituent des profils prédictifs en combinant des

techniques de traçage, des techniques basées sur les cookies et des logiciels d'exploration de données. Le sexe et la tranche d'âge peuvent être déduits de l'analyse des pages que la personne concernée consulte et des annonces qui l'attirent. Le profil fondé sur une analyse des cookies stockés sur son équipement terminal peut être complété par des données agrégées tirées du comportement des personnes présentant des schémas comportementaux similaires dans d'autres contextes. Les systèmes de publicité en ligne classent généralement les personnes concernées dans des segments, soit en fonction de leurs centres d'intérêt, soit par leurs catégories marketing («jardinage», «soins du corps», «électronique», etc.).

La localisation de la personne concernée est également une source primordiale pour le profilage ciblé. Elle peut être déduite de l'adresse IP des terminaux et des points d'accès WiFi, par exemple[65].

62 Les «Flash cookies» sont capables de stocker des informations sur les paramètres et de contourner les préférences de l'utilisateur. Voir Soltani, Ashkan, Canty, Shannon, Mayo, Quentin, Thomas, Lauren et Hoofnagle, Chris Jay, «Flash Cookies and Privacy» (10 août 2009), disponible sur SSRN: http://ssrn.com/abstract=1446862

63 Par exemple, la société Phorm, grâce à sa technique baptisée Webwise, a proposé un service de ciblage comportemental qui procède à une analyse approfondie par paquets des pages consultées par les internautes. Pour fournir ce service, Phorm a conclu des accords de partenariat avec différents FSI.

64 Certains fournisseurs de réseaux publicitaires autorisent des utilisateurs enregistrés à visualiser et à éditer les profils prédictifs qui leur sont associés, au moins dans une certaine mesure.

65 Des informations supplémentaires sur la localisation peuvent être obtenues auprès d'autres sources et utilisées à des fins de profilage.

3. Cadre juridique

3.1. Introduction

L'article 5, paragraphe 1, de la directive 2002/58/CE[66] protège la confidentialité des communications en général. Dans le cas concret de l'utilisation de cookies et de dispositifs similaires, la protection de la confidentialité des communications est essentiellement prévue à l'article 5, paragraphe 3. Le présent avis renvoie à la directive 2002/58/CE modifiée (ci-après la «directive «vie privée et communications électroniques»» ou la «directive modifiée «vie privée et communications électroniques»»). Cette dernière ne devra être transposée en droit national par les États membres qu'en mai 2011, mais le groupe de travail y fait déjà référence parce qu'il tient à ce que le présent avis reste valable après la mise en oeuvre de cette directive et, surtout, parce qu'il veut alerter les parties prenantes de la nécessité de se conformer pleinement à l'article 5, paragraphe 3, modifié. Le considérant 66, adopté lors de la modification de la directive «vie privée et communications électroniques» en 2009 ainsi que les considérant 24 et 25 de ladite directive sont également pertinents dans ce contexte.

Compte tenu de l'importance de l'article 5, paragraphe 3, il est utile de reproduire le texte modifié, en indiquant les changements par rapport au texte initial:

> Les États membres garantissent que ~~l'utilisation des réseaux de communication électroniques en vue de stocker~~ le stockage d'informations ~~ou d'accéder~~ à ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur n'est permis qu'à condition que l'abonné ou l'utilisateur ait donné son accord, après avoir reçu, dans le respect de la directive 95/46/CE, une information claire et complète, entre autres sur les finalités du traitement, ~~et que l'abonné ou l'utilisateur ait le droit de refuser un tel traitement par le responsable du traitement des données~~. Cette disposition ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer ou à faciliter la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires ~~à la fourniture d'un~~ au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur.»

Outre la directive «vie privée et communications électroniques», la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après la «directive 95/46/CE») s'applique aux aspects qui ne sont pas expressément couverts par la directive «vie privée et communications électroniques» lorsque des données à caractère personnel sont traitées[67].

3.2. Champ d'application de l'article 5, paragraphe 3, et de la directive 95/46/CE

Il est utile que les acteurs de la publicité comportementale sachent ce qui déclenche

l'obligation de se conformer à l'article 5, paragraphe 3, de la directive «vie privée et

communications électroniques» et à la directive 95/46/CE, respectivement. Pour ce faire, il convient d'examiner le champ d'application de ces deux instruments. Le présent avis examinera tout d'abord le champ d'application matériel des deux directives (points 3.2.1 et 3.2.2) et leur interaction (point 3.2.3). Il se penchera ensuite sur leur champ d'application territorial (point 3.2.4).

66 Directive 2009/136/CE du Parlement européen et du Conseil du 5 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE oncernant le traitement des données à caractère personnel et la pro tection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs.

67 Voir l'article premier, paragraphe 2, de la directive «vie privée et communications électroniques», qui énonce que «[l]es dispositions de la présente directive précisent et complètent la directive 95/46/CE aux fins énoncées au paragraphe 1».

3.2.1. Champ d'application matériel de l'article 5, paragraphe 3

L'article 5, paragraphe 3, exige l'obtention d'un consentement donné en toute connaissance de cause pour stocker ou avoir accès à des informations stockées dans l'équipement terminal d'un abonné ou d'un utilisateur[68]. Étant donné que (i) les cookies traceurs sont des «informations» stockées dans l'équipement terminal de la personne concernée et (ii) que les fournisseurs de réseaux publicitaires y ont accès lorsque les personnes concernées consultent un site web partenaire, l'article 5, paragraphe 3, s'applique pleinement. Par conséquent, tout stockage de cookies ou de dispositifs similaires (de quelque type que ce soit)[69] et toute utilisation ultérieure de cookies précédemment stockés pour obtenir l'accès aux informations des personnes concernées doivent être conformes à l'article 5, paragraphe 3.

L'article 5, paragraphe 3, s'applique aux «informations» (stockées et/ou consultées). Il ne qualifie pas ces informations. Le fait que ces dernières soient des données à caractère personnel au sens de la directive 95/46/CE n'est pas une condition préalable à l'application de cette disposition. Le considérant 24 justifie cette approche en précisant que «*l'équipement terminal de l'utilisateur … ainsi que toute information stockée sur cet équipement relèvent de la vie privée de l'utilisateur, qui doit être protégée au titre de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales*». C'est la protection d'un domaine réputé relever de la vie privée de la personne concernée qui est l'élément déclencheur des obligations visées à l'article 5, paragraphe 3, et non le fait que les informations soient ou non des données à caractère personnel.

Le groupe de travail avait déjà souligné dans l'avis 1/2008[70] que l'article 5, paragraphe 3, est une disposition générale, applicable non seulement aux services de communications électroniques, mais aussi à tout autre service lorsque ces techniques sont utilisées. Par ailleurs, l'article 5, paragraphe 3, s'applique, que l'entité qui place le cookie soit un responsable du traitement ou un sous-traitant.

3.2.2. Champ d'application matériel de la directive 95/46/CE: traitement des données à caractère personnel

Lorsqu'en raison du placement d'un cookie ou d'un dispositif similaire, et de la récupération d'informations par son intermédiaire, les informations collectées peuvent être considérées comme des données à caractère personnel, la directive 95/46/CE s'applique également, en plus de l'article 5, paragraphe 3.

Le groupe de travail observe que les techniques de publicité comportementale décrites dans le présent avis impliquent souvent le traitement de données à caractère personnel, telles qu'elles sont définies à l'article 2 de la directive 95/46/CE et interprétées par ce groupe de travail[71]. Il existe à cela plusieurs raisons: ***i)*** normalement, la publicité comportementale implique la collecte d'adresses IP et le traitement d'identifiants uniques (par le cookie). L'utilisation des dispositifs comportant un identifiant d'utilisateur unique permet de pister les utilisateurs d'un ordinateur donné, même en cas d'utilisation d'adresses IP dynamiques. En d'autres termes, ces dispositifs permettent d'identifier les personnes concernées, même si leurs noms ne sont pas connus. *ii)* En outre, les informations collectées dans le cadre de la publicité comportementale *ont trait* (c'est-à-dire sont relatives) aux caractéristiques ou au comportement d'une personne et servent à

68 La directive «vie privée et communications électroniques» fait mention d'abonnés et d'utilisateurs. Les abonnés recouvrent à la fois les personnes physiques ou les personnes concernées (au sens de la irective 95/46/CE) et les personnes morales. Le terme «utilisateur» ésigne les personnes concernées qui utilisent un service de communications électroniques, sans s'y être nécessairement abonnées. Par souci de cohérence, le présent avis utilise, dans toute la mesure du possible, le terme «personne concernée».

69 L'article 5, paragraphe 3, est neutre en termes de technologie et, dès lors, applicable non seulement aux cookies, mais également à toute autre technique utilisée pour stocker ou accéder à des informations stockées sur l'équipement terminal des personnes physiques (logiciels espions ou malveillants, etc.).

70 Avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche, adopté le 4 avril 2008.

71 Voir l'interprétation de la notion de données à caractère personnel dans l'avis 4/2007 sur le concept des données à caractère personnel, adopté par le groupe de travail le 20 juin 2007.

l'influencer[72]. La possibilité de relier à tout moment les profils à des informations directement identifiables fournies par la personne concernée, telles que des informations liées à l'enregistrement sur un site web, conforte encore ce point de vue. D'autres scénarios peuvent aboutir à une identification: fusions, pertes de données, et disponibilité croissante sur l'internet de données à caractère personnel combinées à des adresses IP.

3.2.3. Interaction entre les deux directives

Dès lors que les deux directives s'appliquent, il convient de déterminer les dispositions applicables de chacune d'entre elles. À cet égard, le considérant 10 de la directive «vie privée et communications électroniques» déclare que la directive 95/46/CE est applicable notamment «*à tous les aspects de la protection des droits et libertés fondamentaux qui n'entrent pas expressément dans le cadre de la présente directive, y compris les obligations auxquelles est soumis le responsable du traitement des données à caractère personnel et les droits individuels*».

Il s'agit d'une application de la doctrine selon laquelle un acte régissant une question spécifique (***lex specialis***) prime sur un acte ne régissant qu'une question générale (***lex generalis***).

Conformément à ce qui précède, l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques», qui porte sur le consentement en toute connaissance de cause, sera directement applicable. La directive 95/46/CE sera pleinement applicable, hormis en ce qui concerne les dispositions qui sont spécifiquement couvertes par la directive «vie privée et communications électroniques», lesquelles correspondent essentiellement à l'article 7 de la directive 95/46/CE sur la légitimation des traitements de données[73]. Les autres dispositions de la directive 95/46/CE, y compris les principes relatifs à la qualité des données, aux droits de la personne concernée (accès, effacement, opposition), à la confidentialité et à la sécurité du traitement et aux transferts de données vers des pays tiers, seront pleinement applicables.

3.2.4. Champ d'application territorial de l'article 5, paragraphe 3, et de la directive 95/46/CE

Le champ d'application territorial du cadre juridique susvisé est déterminé par une combinaison de l'article 3, paragraphe 1, de la directive «vie privée et communications électroniques»[74] et de l'article 4, paragraphe 1, points a) et c), de la directive 95/46/CE[75].

Dans des avis précédents, le groupe de travail a donné des orientations sur le concept d'établissement et le recours à des moyens, visés à l'article 4, paragraphe 1, points a) et c), respectivement, qui déterminent

[72] Dans son avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche, adopté le 4 avril 2008, le groupe de travail a confirmé que, dans la plupart des cas, les cookies et les adresses IP doivent être considérés comme des données à caractère personnel. On peut, en effet, lire dans cet avis: «Lorsqu'un «cookie» contient un identifiant d'utilisateur unique, celui-ci est clairement une donnée à caractère personnel. L'utilisation de «cookies» persistants ou de dispositifs similaires comportant un identifiant d'utilisateur unique permet de pister les utilisateurs d'un ordinateur donné, même n cas d'utilisation d'adresses IP dynamiques. Les données relatives au comportement qui sont générées par le recours à ces dispositifs permettent d'affiner encore les caractéristiques personnelles de la personne concernée».

[73] Le principe du traitement loyal et licite, consacré par l'article 6, aragraphe 1, point a), peut être compris comme étant inclus dans l'article 5, paragraphe 3, dans la mesure où la loyauté renvoie à la transparence, qui en est une condition.

[74] Le champ d'application de la directive «vie privée et communications électroniques» est défini à son article 3, paragraphe 1, en vertu duquel l'article 5, paragraphe 3, s'applique au stockage ou à l'obtention d'accès à des informations stockées dans l'équipement terminal des personnes concernées qui utilisent des services de communications publiques dans l'UE.

[75] Les deux critères d'application de la directive (ou plutôt du droit national qui la transpose) sont les suivants:
i) lorsque le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement, en application de l'article 4, paragraphe 1, point a), et ii) lorsque le responsable du traitement n'est pas établi sur le territoire de l'UE et a recours, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire de l'UE, en application de l'article 4, paragraphe 1, point c).

l'application de la directive 95/46/CE[76]. Ces orientations sont pleinement applicables aux fournisseurs de réseaux de publicité en ligne.

3.3. Rôles et responsabilités des différents acteurs

Comme indiqué plus haut, la publicité comportementale nécessite plusieurs acteurs, à savoir les fournisseurs de réseaux publicitaires, les diffuseurs et les annonceurs. Il importe d'évaluer leurs rôles respectifs pour déterminer leurs obligations au titre de la législation actuelle sur la protection des données. À cet égard, le groupe de travail note ce qui suit:

Les fournisseurs de réseaux publicitaires:

D'une part, les obligations énoncées à l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» s'appliquent à ceux qui placent des cookies et/ou récupèrent des informations à partir des cookies déjà stockés dans l'équipement terminal de la personne concernée. Au regard de l'article 5, paragraphe 3, il importe peu que l'entité qui place ou lit le cookie soit un responsable du traitement ou un sous-traitant. Dans le cadre de la publicité comportementale, cette interprétation fait peser l'obligation d'obtenir un consentement informé sur les fournisseurs de réseaux publicitaires.

D'autre part, dans le même temps, lorsque la publicité comportementale implique le traitement de données à caractère personnel, les fournisseurs de réseaux publicitaires peuvent également être responsables du traitement. Cet élément est capital dès lors que des obligations supplémentaires découlant de l'application de la directive 95/46/CE sont applicables. Les fournisseurs de réseaux publicitaires contrôlent en effet entièrement les finalités et les moyens du traitement.

Ils «louent» des espaces sur les sites web des diffuseurs pour y placer leurs annonces; ils définissent et lisent les informations des cookies et, le plus souvent, ils collectent l'adresse IP et d'autres données éventuelles révélées par le navigateur. En outre, les fournisseurs de réseaux publicitaires utilisent les informations collectées sur le comportement de navigation des internautes afin de constituer des profils et de choisir et diffuser des publicités qui seront affichées en fonction de ce profil. Dans ce scénario, les fournisseurs de réseaux publicitaires agissent donc clairement comme des responsables du traitement.

Les diffuseurs:

Les diffuseurs, quant à eux, louent des espaces sur leurs sites web aux réseaux publicitaires afin qu'ils affichent des publicités. Ils élaborent leurs sites web de manière à ce que les navigateurs des visiteurs soient automatiquement redirigés vers la page web du fournisseur de réseau publicitaire (qui enverra alors un cookie et diffusera une publicité personnalisée). Cette méthode pose la question de la responsabilité des diffuseurs dans le traitement des données.

Comme l'a récemment indiqué le groupe de travail[77], la question de savoir si un diffuseur peut être considéré comme coresponsable du traitement avec le fournisseur de réseau publicitaire dépendra des conditions qui régissent la collaboration entre le diffuseur et ledit fournisseur. À cet égard, le groupe de travail observe que, généralement, lorsque les fournisseurs de réseaux publicitaires envoient des publicités personnalisées, les diffuseurs y contribuent en configurant leurs sites web de manière à ce que lorsqu'un utilisateur visite un site web du diffuseur, son navigateur soit automatiquement redirigé vers la page web du fournisseur de réseau publicitaire. Ce faisant, le navigateur de l'utilisateur transmettra son adresse IP au fournisseur de réseau publicitaire, qui enverra le cookie et la publicité ciblée. Dans ce cas de figure, il importe de relever que les diffuseurs ne transmettent pas l'adresse IP du visiteur au fournisseur de réseau publicitaire. En effet, c'est le navigateur du visiteur qui communique automatiquement cette information au fournisseur de réseau publicitaire. Cependant, cette communication

[76] Voir le document WP 56 du 30 mai 2002 sur l'application internationale du droit de l'UE en matière de protection des données au traitement des données à caractère personnel sur internet par des sites web établis en dehors de l'UE et, plus récemment, l'avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche, adopté le 4 avril 2008.

[77] Avis 1/2010 sur les notions de «responsable du traitement» et de sous-traitant», adopté le 16 février 2010.

n'est possible que parce que le diffuseur a configuré son site web de manière à ce que le visiteur de son site soit automatiquement redirigé vers le site web du fournisseur de réseau publicitaire. En d'autres termes, le diffuseur *déclenche* le transfert de l'adresse IP, qui constitue la première étape nécessaire pour permettre le traitement ultérieur effectué par le fournisseur de réseau publicitaire afin d'envoyer des publicités ciblées. Par conséquent, même si, sur le plan technique, le transfert des données de l'adresse IP est effectué par le navigateur de la personne qui consulte le site web du diffuseur, ce n'est pas cette personne qui déclenche le transfert. La personne voulait uniquement visiter le site web du diffuseur. Elle n'avait pas l'intention de visiter le site web du fournisseur de réseau publicitaire. À l'heure actuellement, ce cas de figure est courant.

Par conséquent, le groupe de travail considère que les diffuseurs assument une certaine responsabilité dans le traitement des données, qui découle de la transposition en droit national de la directive 95/46/CE et/ou d'autres actes législatifs nationaux[78]. Cette responsabilité ne couvre certes pas l'ensemble des opérations de traitement nécessaires à l'envoi de publicités comportementales, par exemple, le traitement réalisé par le fournisseur de réseau publicitaire consistant à dresser des profils qui serviront ensuite à diffuser des publicités ciblées, mais elle couvre la première étape, c'est-à-dire la partie initiale du traitement des données que constitue le transfert de l'adresse IP, lequel intervient lorsque des personnes physiques consultent leurs sites web. En effet, les diffuseurs facilitent ce transfert et codéterminent les finalités pour lesquelles il a lieu, à savoir envoyer aux visiteurs des publicités ciblées. Pour ces raisons, ils assument une part de la responsabilité en qualité de responsables du traitement. Cette responsabilité ne nécessite toutefois pas qu'ils se conforment à l'ensemble des obligations imposées par les directives.

À cet égard, il convient d'interpréter le cadre juridique avec une certaine souplesse, en n'appliquant que ses dispositions pertinentes. Les diffuseurs ne détiennent pas d'informations à caractère personnel; il ne serait dès lors pas logique de leur appliquer certaines des obligations prévues par la directive, comme le droit d'accès. En revanche, comme on le verra plus loin, l'obligation d'informer les particuliers du traitement des données leur est pleinement applicable.

Outre ce qui précède, ainsi que l'indiquait l'avis susvisé du groupe de travail, les diffuseurs sont coresponsables dès lors qu'ils collectent et transfèrent des données à caractère personnel concernant les visiteurs de leurs sites (nom, adresse, âge, localisation, etc.) au fournisseur de réseau publicitaire. Dans la mesure où les diffuseurs agissent comme des responsables du traitement, ils sont liés par les obligations imposées par la directive 95/46/CE concernant la partie du traitement des données qu'ils contrôlent. Dans ce contexte, à l'instar des fournisseurs de réseaux publicitaires, les diffuseurs «*veillent à ce que la complexité et les technicités du mécanisme de publicité comportementale ne les empêchent pas de trouver les moyens appropriés de se conformer aux obligations qui incombent aux responsables du traitement, et garantir le respect des droits des personnes concernées*»[79].

En résumé, les diffuseurs doivent être conscients du fait qu'en concluant des contrats avec des réseaux publicitaires, en vertu desquels des données à caractère personnel des visiteurs de leurs sites sont mises à la disposition de fournisseurs de réseaux publicitaires, ils assument une part de responsabilité à l'égard de ces visiteurs. La portée de leur responsabilité, notamment la mesure dans laquelle ils deviennent des responsables du traitement, doit être analysée au cas

[78] Le groupe de travail relève que l'obligation d'information et d'autres obligations éventuelles peuvent découler de principes généraux du droit (droit des contrats et en matière de responsabilité civile délictuelle) ainsi que de la législation sur la protection des consommateurs en matière de pratiques commerciales des entreprises vis-à-vis des consommateurs, telle que la directive 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs ans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) n° 2006/2004 du Parlement et du Conseil («directive sur les pratiques commerciales déloyales»).

[79] Avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant». http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_fr.pdf

par cas en tenant compte des conditions particulières de leur collaboration avec les fournisseurs de réseaux publicitaires, telles qu'elles sont stipulées dans les contrats de service. Dès lors, ces contrats conclus entre diffuseurs et fournisseurs de réseaux publicitaires devraient définir les rôles et responsabilités des deux parties dans le cadre de leur collaboration décrite dans le contrat.

Les annonceurs:

Lorsqu'une personne concernée clique sur une annonce et visite le site web de l'annonceur, ce dernier peut tracer quelle campagne a entraîné le clic publicitaire. Si l'annonceur saisit l'information de ciblage (par exemple, certaines données démographiques telles que «jeunes mamans» ou un groupe d'intérêt comme «amateur de sports extrêmes») et la combine avec le comportement de navigation ou les données d'inscription de la personne concernée, il est alors un responsable autonome du traitement des données pour cette partie du traitement.

Le présent avis se concentre sur les traitements de données effectués par le fournisseur de réseau publicitaire et par le diffuseur, consistant à envoyer des publicités ciblées. Il ne se prononce pas sur les éventuels traitements de données supplémentaires que pourraient effectuer les annonceurs évoqués plus haut.

4. Obligation d'obtenir un consentement informé

La règle générale énoncée dans la première phrase de l'article 5, paragraphe 3, fait obligation aux États membres de garantir «*que le stockage d'informations, ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur n'est permis qu'à condition que l'abonné ou l'utilisateur ait donné son accord, après avoir reçu, dans le respect de la directive 95/46/CE, une information claire et complète, entre autres sur les finalités du traitement*». Le libellé de cet article a changé lors de la modification de la directive «vie privée et communications électroniques» en 2009. Les changements apportés dans la version modifiée clarifient et renforcent la nécessité d'obtenir un consentement informé préalable des utilisateurs31. Le groupe de travail considère que l'analyse juridique développée ci-dessous est pertinente et valable en ce qui concerne tant la version actuelle que la version modifiée de l'article 5, paragraphe 3.

La section suivante examine diverses manières de satisfaire les exigences mentionnées à l'article 5, paragraphe 3. Après la discussion sur le consentement, le groupe de travail donne des orientations sur l'obligation d'information.

4.1. Obligation d'obtenir le consentement préalable des personnes concernées pour diffuser des publicités comportementales

Conformément à l'article 5, paragraphe 3, un fournisseur de réseau publicitaire qui souhaite stocker ou obtenir l'accès à des informations stockées dans l'équipement terminal d'un utilisateur peut le faire: *i)* s'il a fourni à l'utilisateur une information claire et complète dans le respect de la directive 95/46/CE, entre autres, sur les finalités du traitement et *ii)* s'il a obtenu l'accord de l'utilisateur pour stocker ou obtenir l'accès à des informations stockées sur son équipement terminal, après avoir fourni l'information visée sous *i)*.

Il ressort des termes mêmes de l'article 5, paragraphe 3, que *i)* l'accord doit être obtenu *avant* que le cookie soit placé et/ou que les informations stockées dans l'équipement terminal de l'utilisateur soient collectées, ce qui est généralement appelé «consentement préalable», et *ii)* un consentement informé ne peut être obtenu que si l'information préalable sur l'envoi et les finalités du cookie *a été donnée à l'utilisateur.* Dans ce contexte, il importe de souligner que, pour que le consentement soit valable, quelles que soient les circonstances dans lesquelles il a été donné, il doit être donné librement, être exprès et constituer une manifestation éclairée des souhaits de la personne concernée. Ce consentement doit être obtenu avant que les données à caractère personnel ne soient collectées, sans quoi les personnes concernées ne comprendraient pas pleinement qu'elles donnent leur consentement et

à quoi elles consentent. Le consentement doit en outre être révocable.

Les sections suivantes examinent si un consentement sous la forme d'un paramétrage du navigateur ou d'une option d'*opt-out* offerte par les fournisseurs de réseaux publicitaires satisfait aux exigences de l'article 5, paragraphe 3.

4.1.1. Consentement passant par la configuration des paramètres du navigateur

Les diffuseurs et les fournisseurs de réseaux publicitaires qui pratiquent la publicité comportementale placent des cookies traceurs dans l'équipement terminal d'une personne concernée lorsque celle-ci consulte un site web faisant partie du réseau publicitaire. Cette installation est systématique, à moins que le navigateur de l'utilisateur ne soit configuré pour rejeter les cookies. Concrètement, dès que le cookie est placé et que la personne concernée navigue sur la page web où l'annonce a été affichée, la personne est en mesure de prendre connaissance des cookies et de la manière dont il faut configurer le navigateur pour les contrôler. Ces informations sont fournies par les diffuseurs et les fournisseurs de réseaux publicitaires. Ces responsables du traitement incluent généralement dans leurs conditions générales et/ou dans leur politique de confidentialité des informations sur les cookies tiers utilisés à des fins de publicité comportementale, en précisant éventuellement les utilisations/finalités de base de ces cookies et le moyen de les éviter en configurant le navigateur. Cependant, cette pratique ne satisfait pas aux exigences de l'article 5, paragraphe 3, en particulier dans sa version modifiée, qui met l'accent sur la fourniture préalable des informations et sur l'obtention d'un consentement préalable (avant le début du traitement).

Le considérant 66 de la directive «vie privée et communications électroniques» modifiée mentionne que le consentement de l'utilisateur peut être exprimé par l'utilisation des paramètres appropriés d'un navigateur ou d'une autre application «*lorsque cela est techniquement possible et effectif, conformément aux dispositions pertinentes de la directive 95/46/CE*». Ce n'est pas là une dérogation à l'article 5, paragraphe 3, mais plutôt un rappel que, dans cet environnement technologique, un consentement peut être exprimé de différentes façons – lorsque cela est techniquement possible et effectif et conforme aux autres exigences pertinentes pour qu'un consentement soit valablement donné. Dans ce contexte, il convient de se demander comment déterminer les conditions dans lesquelles les paramètres du navigateur répondront aux exigences de la directive 95/46/CE et constitueront un consentement valable «*dans le respect de la directive 95/46/CE*». Le groupe de travail considère que cela ne surviendra que dans un nombre très limité de cas, pour les raisons exposées ci-dessous.

Tout d'abord, compte tenu de la définition et des conditions du consentement valable prévues à l'article 2, point h), de la directive 95/46/CE, en règle générale, les personnes concernées ne sauraient être réputées avoir donné leur consentement simplement parce qu'elles ont acheté/utilisé un navigateur ou une autre application qui permet, par défaut, la collecte et le traitement de leurs informations. Les personnes concernées moyennes ne sont pas au courant du traçage de leur comportement de navigation, des finalités de celui-ci, etc. Elles ne savent pas toujours comment paramétrer le navigateur pour refuser les cookies, même si une explication figure dans les politiques de confidentialité. Il est donc fallacieux de considérer que, de manière générale, l'absence d'action de la personne concernée (elle n'a pas configuré les paramètres du navigateur pour qu'il refuse les cookies) est une manifestation claire et sans équivoque de sa volonté. Comme le groupe de travail l'a indiqué dans son avis 1/2008 précité, «[*l]a responsabilité de leur traitement [des cookies] ne peut être réduite à la responsabilité qui incombe à l'utilisateur de prendre, ou de ne pas prendre, certaines précautions dans les paramètres de son navigateur*». À l'heure actuelle, sur les quatre principaux navigateurs, un seul bloque les cookies tiers par défaut dès l'installation du navigateur. Les trois autres grands navigateurs sont configurés par défaut pour autoriser tous les cookies. Ainsi, les cookies sont envoyés et les informations sont collectées avant l'obtention du consentement, ce qui est donc contraire

à l'obligation d'obtenir le consentement préalable de l'utilisateur[80].

Ensuite, pour que le paramétrage des navigateurs puisse être la manifestation d'un consentement informé, il ne devrait pas être possible de «contourner» le choix fait par l'utilisateur en configurant le navigateur. Or, dans la pratique, les cookies effacés peuvent aisément être «ressuscités» par des «flash cookies», permettant ainsi au fournisseur de réseau publicitaire de continuer à suivre l'utilisateur. Dès lors que cette possibilité technique existe et que son utilisation se répand, on peut douter que le paramétrage du navigateur soit la manifestation d'un consentement informé, valable et effectif.

Enfin, le consentement qui passe par la configuration des paramètres du navigateur pour recevoir des cookies en vrac implique que les utilisateurs accepteront tout traitement futur, éventuellement sans être informés des finalités ou des utilisations du cookie. Un consentement général à tout traitement ultérieur, sans en connaître les circonstances, ne saurait constituer un consentement valable[81].

Par conséquent, pour qu'un navigateur ou toute autre application puisse «exprimer» un consentement valable, il doit d'abord résoudre les problèmes décrits ci-dessus. Dans les faits, cela signifie que:

(a) les navigateurs, ou toute autre application, qui refusent par défaut les cookies tiers et demandent à la personne concernée d'effectuer une action positive pour accepter à la fois le paramétrage et la transmission continue des informations contenues dans les cookies par des sites web spécifiques peuvent exprimer un consentement valable et effectif. En revanche, si les paramètres du navigateur sont préconfigurés pour accepter tous les cookies, le consentement ne serait pas conforme à l'article 5, paragraphe 3, dans la mesure où, en règle générale, un tel consentement ne saurait constituer une véritable manifestation de la volonté de la personne concernée. Ce consentement ne serait ni exprès ni préalable (au traitement). S'il est vrai qu'une personne concernée pourrait effectivement avoir décidé de conserver un paramétrage acceptant tous les cookies tiers, il ne serait pas réaliste que les fournisseurs de réseaux publicitaires supposent que la grande majorité des personnes concernées dont les navigateurs sont «configurés» pour accepter des cookies, a effectivement exercé ce choix;

(b) les navigateurs, ensemble ou avec d'autres outils d'information, y compris la coopération des fournisseurs de réseaux publicitaires et des diffuseurs, devraient donner des informations claires, complètes et parfaitement visibles afin de garantir que le consentement est donné en toute connaissance de cause. Pour répondre aux exigences de la directive 95/46/CE, les navigateurs devraient transmettre, au nom du fournisseur de réseau publicitaire, les informations pertinentes concernant les finalités des cookies et le traitement ultérieur des données. Par conséquent, les avertissements généraux sans référence explicite au réseau publicitaire qui place le cookie sont insuffisants.

Le groupe de travail est d'avis que, si les conditions susvisées ne sont pas remplies, ce n'est pas en fournissant des informations ni, dans une certaine mesure, en augmentant la capacité de l'utilisateur de refuser les cookies (en expliquant la procédure à suivre) que, d'une manière générale, on obtiendra un consentement informé au sens de l'article 5, paragraphe

[80] Une complication supplémentaire réside dans le fait que les trois navigateurs susvisés transmettent encore les informations des cookies existants, même lorsque les paramètres du navigateur sont configurés pour refuser les (nouveaux) cookies tiers. En d'autres termes, les informations sur les cookies qui ont été placés avant que le navigateur soit configuré pour les refuser continueront à être envoyées au fournisseur de réseau publicitaire. À l'heure actuelle, un seul grand logiciel de navigation permet aux utilisateurs de bloquer la configuration et la transmission des données provenant des cookies tiers (c'est-à-dire également les cookies placés avant que le navigateur ne soit configuré pour refuser les cookies). Il en résulte que les cookies qui ont été placés lors de la visite d'un seul site web (par exemple, un moteur de recherche ou un site de réseau social) peuvent toujours être lus par ce site lorsque l'utilisateur consulte un site partenaire de ce premier site web.

[81] Comme l'a déclaré le groupe de travail dans son document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995, adopté le 25 novembre 2005, à propos des futurs transferts de données: «L'importance du fait que le consentement soit un acte positif exclut de facto tout système par lequel la personne concernée n'aurait le droit de s'opposer au transfert qu'après qu'il a eu lieu: le consentement spécifique à un transfert doit être authentiquement exigé pour que celui-ci puisse avoir lieu».

3, de la directive «vie privée et communications électroniques» et de l'article 2, point h), de la directive 95/46/CE.

Étant donné l'importance que revêt le paramétrage du navigateur pour garantir que la personne concernée donne effectivement son consentement au stockage de cookies et au traitement des informations la concernant, il paraît essentiel que les navigateurs soient munis de paramètres de protection de la confidentialité par défaut. En d'autres termes, il faut qu'ils incluent le paramètre «non-acceptation et non-transmission de cookies tiers». Pour compléter cette disposition et la rendre plus efficace, les navigateurs devraient imposer aux utilisateurs de recourir à un «assistant de protection de la confidentialité» lorsqu'ils installent leur navigateur pour la première fois ou le mettent à jour, et prévoir une procédure simple leur permettant de choisir en cours d'utilisation. Le groupe de travail invite instamment les concepteurs de navigateur à prendre des mesures urgentes en ce sens et à coordonner leur action avec les fournisseurs de réseaux publicitaires.

4.1.2. Consentement et exercice des options d'«opt-out»

Les fournisseurs de réseaux publicitaires proposent de plus en plus souvent des mécanismes d'«opt-out» permettant aux utilisateurs de refuser de recevoir des publicités ciblées[82]. Pour activer ce mécanisme, la personne concernée doit se rendre sur le site web du fournisseur de réseau publicitaire et préciser qu'il ne veut pas être tracé aux fins de la diffusion de publicités ciblées. Ces mécanismes se veulent un complément et, dans une certaine mesure, une solution aux problèmes, décrits plus haut, que pose le consentement passant par la configuration des paramètres du navigateur.

Ces mécanismes d'«opt-out» fondés sur des cookies sont les bienvenus et doivent être encouragés puisqu'ils simplifient la possibilité technique actuellement offerte aux personnes concernées de refuser les publicités. Cependant, en principe, ces mécanismes n'expriment pas un consentement des personnes concernées. Ce n'est que dans des cas individuels très spécifiques que l'on pourrait parler de consentement implicite, par exemple lorsqu'un utilisateur expérimenté, qui est informé de la pratique de la publicité comportementale, sait qu'il peut la refuser mais choisit de poser l'acte volontaire de ne pas le faire (en particulier, s'il le fait avant qu'un cookie ne lui ait été envoyé). En revanche, ce mécanisme ne convient pas pour obtenir un consentement informé de l'utilisateur moyen, pour des raisons analogues à celles mentionnées dans le cas du paramétrage du navigateur, à savoir:

d'une part, en règle générale, les utilisateurs ne sont pas au courant de la collecte de données, de ses utilisations, du fonctionnement de la technologie et, surtout, de la façon dont ils doivent procéder pour exercer un «opt-out». En conséquence, dans la pratique, très peu de gens exercent l'option «d'opt-out», non parce qu'ils ont décidé, en toute connaissance de cause, d'accepter les publicités comportementales, mais parce qu'ils ne se rendent pas compte qu'en ne procédant pas à un «opt-out», ils acceptent en fait ces publicités;

d'autre part, le consentement implique une participation active de la personne concernée avant la collecte et le traitement des données. Or le mécanisme d'«opt-out» se réfère souvent à une «non»-réaction de la personne concernée après le début du traitement. En outre, dans le cadre de ce mécanisme, il n'y a pas de participation active: la volonté de la personne concernée est simplement supposée ou implicite. Cela ne remplit pas les conditions à satisfaire pour qu'un consentement soit juridiquement valable.

Eu égard à ce qui précède, le groupe de travail considère que les mécanismes d'«opt-out» fondés sur des cookies ne donnent pas aux utilisateurs moyens la faculté véritable de consentir ou non à recevoir des publicités comportementales. Dès lors, ces mécanismes ne remplissent pas la condition posée par l'article 5, paragraphe 3.

4.1.3. Les mécanismes de consentement par «opt-in» préalable se prêtent mieux à la manifestation d'un consentement informé

Le groupe de travail est d'avis que les mécanismes d'«opt-in» préalable, qui requièrent une action positive de la personne concernée pour manifester son

[82] Voir, par exemple, l'option d'«opt-out» prévue par la Network Advertising Initiative, qui offre la possibilité de sortir de différents réseaux: http://www.networkadvertising.org/managing/opt_out.asp.

consentement avant l'envoi du cookie à cette personne, sont davantage conformes à l'article 5, paragraphe 3. Évoquant le consentement comme base juridique du traitement, le groupe de travail a récemment confirmé ce point de vue: «*Les évolutions technologiques invitent également à un examen attentif du consentement. En pratique, l'article 7 de la directive 95/46/CE n'est pas toujours correctement appliqué, en particulier dans le contexte de l'internet, où un consentement implicite ne conduit pas toujours à un consentement non équivoque [comme le prévoit l'article 7, point a), de la directive]. Pour permettre aux personnes concernées de s'exprimer davantage en amont du traitement de leurs données à caractère personnel, il faut que le consentement soit donné explicitement (il faut par conséquent un accord préalable) pour l'ensemble du traitement basé sur le consentement*»[83].

Dans un précédent avis traitant de cette question, le groupe de travail36 recommandait la mention de messages spécifiques: «*Dans le cas des cookies, l'utilisateur devrait être averti avant leur réception, leur stockage ou leur transmission … Le message devrait préciser, dans un langage généralement compréhensible, quelles informations vont être stockées dans le cookie et à quelles fins, ainsi que la période de validité de celui-ci*». Après avoir reçu ces informations, la personne concernée devrait avoir la possibilité d'indiquer si elle souhaite être profilée à des fins de publicité comportementale.

Le groupe de travail est conscient des problèmes pratiques actuels que pose l'obtention d'un consentement, en particulier lorsque celui-ci est nécessaire chaque fois qu'un cookie est lu afin d'envoyer une publicité ciblée. Pour éviter ce problème, en application du considérant 25 de la directive «vie privée et communications électroniques» («*[…]le droit de refuser ces dispositifs [cookies] peu[ven]t être offert[s] en une seule fois … durant des connexions subséquentes*»), l'acceptation d'un cookie par l'utilisateur pourrait être interprétée comme valable non seulement pour l'envoi du cookie, mais aussi pour la collecte ultérieure de données provenant de ce cookie. En d'autres termes, le consentement obtenu pour le placement du cookie et pour l'utilisation des informations aux fins d'envoyer des publicités ciblées couvrirait les «lectures» postérieures du cookie ayant lieu à chaque fois que l'utilisateur visite un site web partenaire du fournisseur de réseau publicitaire qui a placé le cookie.

Or, sachant que *i)* cette pratique signifierait que les personnes physiques acceptent «une fois pour toutes» d'être suivies et que *ii)* ces personnes pourraient simplement «oublier» qu'elles ont accepté, par exemple un an plus tôt, d'être suivies, le groupe de travail considère que certaines garanties devraient être mises en place. Il propose, notamment, trois types de mesure: premièrement, limiter la portée du consentement dans le temps. Le consentement à être suivi ne devrait pas être valable «une fois pour toutes» mais pour une durée limitée, par exemple un an. À l'expiration de ce délai, les fournisseurs de réseaux publicitaires devraient obtenir un nouveau consentement. Cela serait réalisable si les cookies avaient une durée de vie limitée après leur placement dans l'équipement terminal de l'utilisateur (et leur durée de vie ne devrait pas être prolongée); deuxièmement, les risques évoqués plus haut seraient encore atténués par des mesures d'information supplémentaires, qui sont abordées à la section 4.2.1 ci-dessous; troisièmement, un consentement donné librement est toujours révocable. Les personnes concernées devraient avoir la possibilité de révoquer aisément leur consentement à être suivies à des fins de publicité comportementale. À cet effet, il est essentiel de fournir des informations claires sur cette possibilité et sur la manière de l'exercer (voir la section 4.2 ci-dessous).

Le groupe de travail encourage les professionnels de la publicité à mettre en oeuvre les mesures décrites ci-dessus ou des solutions alternatives impliquant une action positive préalable des utilisateurs concernant l'acceptation ***i)*** du placement du cookie et ***ii)*** de l'utilisation du cookie pour les pister sur les sites web qu'ils consultent afin de leur envoyer des publicités comportementales. Cela peut aussi inclure la conception des navigateurs et les technologies de navigation.

[83] Le groupe de travail reconnaît le travail accompli par certaines associations, comme «L'avenir de la protection de la vie privée» en vue de promouvoir l'utilisation d'icônes à des fins d'information.

4.1.4 Consentement informé: les enfants

Dans son avis 2/2009, le groupe de travail avait étudié la question de la protection des données à caractère personnel des enfants[84]. Les problèmes liés à l'obtention d'un consentement informé sont en effet encore plus aigus dans le cas des enfants.

Outre les exigences décrites plus haut (et ci-dessous) pour qu'un consentement soit valable, dans certains cas, le consentement des enfants doit être donné par leurs parents ou d'autres représentants légaux. En l'espèce, cela signifie que les fournisseurs de réseaux publicitaires devront informer les parents de la collecte et de l'utilisation d'informations concernant leurs enfants et obtenir leur consentement avant de collecter et d'exploiter ces informations à des fins de ciblage comportemental des enfants[85].

Eu égard à ce qui précède, et compte tenu de la vulnérabilité des enfants, le groupe de travail est d'avis que les fournisseurs de réseaux publicitaires ne devraient pas proposer de catégoriesde centres d'intérêt destinées à diffuser des publicités comportementales ou à influencer des enfants.

4.2. Obligation de fournir des informations dans le cadre de la publicité comportementale

La transparence est une condition essentielle pour qu'une personne physique puisse donner son consentement à la collecte et au traitement ultérieur de données la concernant. Ainsi qu'il est expliqué plus haut, dans le cadre de la publicité comportementale, il se peut que les utilisateurs ne connaissent pas ou ne comprennent pas la technologie sur laquelle repose la publicité comportementale, ni même qu'ils sont ciblés par ce type de publicité. Il est donc capital de veiller à ce que des informations suffisantes et effectives soient fournies d'une manière qui atteindra les internautes. Les personnes concernées ne seront véritablement en mesure d'exercer un choix que si elles sont informées.

4.2.1 Quelles sont les informations à fournir et par qui?

L'article 5, paragraphe 3, prévoit que l'utilisateur doit recevoir une information «*dans le respect de la directive 95/46/CE, entre autres sur les finalités du traitement*». L'article 10 de la directive 95/46/CE traite de la fourniture de cette information[86].

En ce qui concerne la publicité comportementale, les personnes concernées devraient être informées, entre autres choses, de l'identité du fournisseur de réseau publicitaire et des finalités du traitement. La personne concernée doit être clairement informée que le cookie permettra au fournisseur de réseau publicitaire de collecter des informations sur la consultation d'autres sites web, les publicités qui ont été affichées, celles sur lesquelles elle a cliqué, le moment, etc.

Il devrait être expliqué en termes simples que le cookie servira à constituer des profils destinés à la diffusion de publicités ciblées. Le considérant 25 de la directive «vie privée et communications électroniques» impose que les informations fournies soient «*claires et précises*». Des mentions telles que «*les annonceurs et d'autres tiers peuvent également utiliser leurs propres cookies ou balises*» sont clairement insuffisantes.

S'agissant de la manière dont ces informations devraient être communiquées, le considérant 25 exige qu'elle soit «*la plus conviviale possible*». Le groupe de travail considère que la fourniture d'un minimum d'informations directement sur l'écran, de manière interactive, aisément visibles et compréhensibles, serait le meilleur moyen de se conformer à ce principe[87]. Il importe que les informations soient aisément accessibles et extrêmement visibles. Ces informations

84 Avis sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier des écoles): http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp160_fr.pdf.

85 Cela s'ajoute à la législation et aux normes applicables en matière de publicité.

86 Il impose notamment de préciser l'identité du responsable du traitement, les finalités du traitement, ainsi que les destinataires des données et l'existence d'un droit d'accès, dans la mesure où ces informations supplémentaires sont nécessaires pour assurer un traitement loyal des données.

87 Ceci est conforme à une recommandation antérieure du groupe de travail, à savoir la recommandation 2/2001 concernant certaines exigences minimales pour la collecte en ligne de données à caractère personnel dans l'Union européenne (WP 43), adoptée le 17 mai 2001: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp43fr.pdf.

essentielles ne peuvent donc pas être cachées dans des conditions générales et/ou dans des déclarations sur la politique de confidentialité.

Le groupe de travail reconnaît que, sur le plan technique, il peut exister différentes manières de fournir l'information, et il fait appel à la créativité des acteurs dans ce domaine. Il a appris que certains fournisseurs de réseaux publicitaires ont commencé à élaborer de nouvelles manières de communiquer les informations et il se réjouit de cette évolution. Les icônes placées autour des publicités sur le site web du diffuseur et menant vers des informations supplémentaires sont des exemples d'une telle évolution, que le groupe de travail juge tout à la fois positive et nécessaire.

Compte tenu de la possibilité, évoquée à la section 4.1.3, que l'acceptation d'être suivies, donnée une fois par les personnes physiques, couvre toutes les lectures ultérieures du cookie, le groupe de travail juge essentiel que les fournisseurs de réseaux publicitaires trouvent des moyens d'informer ***régulièrement*** les utilisateurs que le suivi est en cours. À moins que des rappels clairs et non équivoques, recourant à des moyens simples, ne soient adressés aux personnes concernées, il est très probable qu'après un certain temps, ces dernières auront oublié que le suivi se poursuit et qu'elles y ont consenti. À cet égard, le groupe de travail serait tout à fait favorable à la création d'un symbole et de messages associés qui avertiraient les consommateurs qu'un fournisseur de réseau publicitaire suit leur comportement de navigation afin de diffuser des publicités ciblées. Ce symbole serait très utile non seulement pour rappeler le suivi aux personnes concernées, mais également pour vérifier si elles souhaitent maintenir ou révoquer leur consentement.

Une autre question pertinente est celle de savoir ***qui doit fournir les informations***: le diffuseur, le fournisseur de réseau publicitaire, ou les deux? Au final, les personnes concernées devraient recevoir des informations aisément accessibles et extrêmement visibles. Comme il est expliqué plus loin, la coopération entre les diffuseurs et les fournisseurs de réseaux publicitaires paraît essentielle.

Le groupe de travail observe que, par application de l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques», l'obligation de fournir les informations nécessaires et d'obtenir le consentement des personnes concernées incombe en dernier ressort à la partie qui envoie et lit le cookie. Dans la plupart des cas, il s'agit du fournisseur de réseau publicitaire. Lorsque des diffuseurs sont coresponsables du traitement, par exemple lorsqu'ils transfèrent directement des informations identifiables aux fournisseurs de réseaux publicitaires, ils sont également liés par l'obligation d'informer la personne concernée du traitement ultérieur des données la concernant.

En outre, comme le relève la section 3.3 ci-dessus, les diffuseurs partagent avec les fournisseurs de réseaux publicitaires la responsabilité du traitement des données effectué dans le cadre de la diffusion de publicités comportementales. Plus particulièrement, cette responsabilité couvre la première étape du traitement, à savoir le transfert de l'adresse IP aux fournisseurs de réseaux publicitaires qui intervient lorsqu'une personne consulte leur site web et est redirigée vers le site web du fournisseur de réseau publicitaire.

Du fait de cette responsabilité, les diffuseurs ont certaines obligations envers les personnes concernées, qui découlent directement de la directive 95/46/CE41. Le groupe de travail est notamment d'avis que les diffuseurs sont liés par l'obligation de fournir aux personnes concernées des informations sur le traitement des données qui a lieu lorsque leur navigateur est redirigé, et sur les finalités pour lesquelles les données seront utilisées ultérieurement par les fournisseurs de réseaux publicitaires. Les informations devraient porter non seulement sur le transfert de l'adresse IP destiné à l'affichage de publicités, mais aussi sur le traitement ultérieur des données effectué par les fournisseurs de réseaux publicitaires, y compris le placement de cookies.

Le groupe de travail n'entend bien évidemment pas que les informations soient fournies deux fois (la première par le fournisseur de réseau publicitaire, la seconde par le diffuseur). Il considère que, dans ce domaine, une coopération s'impose entre les fournisseurs de réseaux publicitaires et les diffuseurs afin qu'ils décident qui fournira l'information et comment. Il invite donc instamment ces deux parties à ne ménager aucun

effort pour produire les mentions les plus efficaces et informer au mieux les internautes sur la manière dont fonctionne la publicité comportementale dans chaque cas particulier. Une telle coopération est d'autant plus nécessaire que les fournisseurs de réseaux publicitaires sont, en principe, invisibles pour les personnes concernées. En effet, l'utilisateur interagit avec le site visité, c'est-à-dire avec le site web du diffuseur. C'est pourquoi, du point de vue de l'utilisateur, il est plus normal qu'il reçoive l'information de ce site. Cela peut se faire de différentes façons; le diffuseur peut, par exemple, prévoir un espace sur son site web où les fournisseurs de réseaux publicitaires peuvent afficher les informations requises.

Dans l'exercice de leurs fonctions, les autorités chargées de la protection des données examineront si des mesures appropriées ont été adoptées pour faire mieux connaître ces pratiques et les droits des personnes concernées correspondantes.

5. Autres obligations et principes découlant de la directive 95/46/CE

Outre l'article 5, paragraphe 3, les responsables du traitement doivent veiller au respect de toutes les obligations imposées par la directive 95/46/CE qui n'empiètent pas sur les dispositions dudit article. Ils doivent notamment se conformer aux obligations examinées cidessous.

5.1. Obligations relatives à des catégories particulières de données

Les données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale ainsi que les données relatives à la santé et à la vie sexuelle sont considérées comme sensibles en vertu de l'article 8 de la directive 95/46/CE. Or le groupe de travail considère qu'il existe un grave risque de porter atteinte aux données à caractère personnel si ce type d'informations est utilisé à des fins de diffusion de publicités comportementales. Tout ciblage des personnes concernées sur la base d'informations sensibles ouvrirait la voie à des abus. En outre, étant donné la nature sensible de ces informations et les situations potentiellement gênantes qui pourraient survenir si des personnes recevaient des publicités qui révèlent, par exemple, leurs préférences sexuelles ou leur activité politique, l'offre ou l'utilisation de catégories de centres d'intérêt révélant des données sensibles doit être découragée.

Si, malgré tout, des fournisseurs de réseaux publicitaires offrent et utilisent des catégories de centres d'intérêt révélant des informations sensibles, ils doivent se conformer aux dispositions de l'article 8 de la directive 95/46/CE. Ainsi, si un fournisseur de réseau publicitaire traitait le comportement d'une personne physique afin de «la placer» dans une catégorie de centres d'intérêt indiquant une préférence sexuelle particulière, il effectuerait un traitement de données sensibles au sens de l'article 8 de la directive 95/46/CE. Or cet article interdit un tel traitement, hormis dans des circonstances spécifiques. De ce fait, la seule base juridique susceptible de légitimer le traitement de ces données serait le consentement préalable explicite et distinct, prévu à l'article 8, paragraphe 2, point a). L'exigence d'obtenir une manifestation positive, préalable et distincte du consentement de la personne concernée signifie qu'en aucun cas un mécanisme de consentement par «opt-out» ne satisferait cette exigence légale. Cela implique également que ce consentement ne saurait être obtenu en procédant à un paramétrage du navigateur. Pour collecter et traiter licitement ce type d'information, les fournisseurs de réseaux publicitaires devraient mettre en place des mécanismes leur permettant d'obtenir un consentement préalable exprès, distinct du consentement recueilli pour le traitement des données en général.

5.2. Respect des principes relatifs à la qualité des données

L'article 6 de la directive 95/46/CE énonce différents principes que doit respecter le responsable du traitement. À cet égard, les aspects suivants sont particulièrement pertinents.

Le groupe de travail n'ignore pas que les profils collectés et utilisés à des fins de publicité comportementale pourraient potentiellement être utilisés pour d'autres finalités. Ils pourraient ainsi servir à développer de nouveaux services dont la nature n'a pas encore été décidée.

Or, une telle éventualité est subordonnée au respect de l'article 6, paragraphe 1, point b), qui pose le ***principe de limitation des finalités***. Ce principe interdit tout traitement de données à caractère personnel incompatible avec les finalités légitimant la collecte initiale. En d'autres termes, les utilisations secondaires incompatibles d'informations collectées et stockées à des fins de publicité comportementale seraient contraires à l'article 6, point b), de la directive 95/46/CE.

Ainsi, lorsque des réseaux publicitaires font partie d'un groupe d'entreprises offrant des services multiples, en principe, le réseau publicitaire ne peut pas utiliser les données collectées à des fins de publicité comportementale pour ces autres services (à moins qu'il puisse être démontré que les finalités sont compatibles). Pour les mêmes raisons, les réseaux publicitaires ne peuvent pas compléter les informations collectées à des fins de publicité comportementale par d'autres données.

Si des réseaux publicitaires souhaitent utiliser des informations, rassemblées à des fins de publicité comportementale, pour des finalités secondaires incompatibles, par exemple d'autres services, il leur faudra appliquer et respecter une autre disposition juridique, à savoir l'article 7 de la directive 95/46/CE. Ils devront donc informer les personnes concernées et, dans la plupart des cas, obtenir leur consentement, conformément à l'article 7, point a). L'article 6, paragraphe 1, point e), impose l'effacement des données lorsqu'elles ne sont plus nécessaires à la réalisation de la finalité pour laquelle elles ont été collectées (***principe de rétention***). Le respect de ce principe impose de limiter le stockage des données. En conséquence, les entreprises doivent préciser et respecter des délais spécifiques de conservation des données.

Conformément à ce qui précède, les informations relatives au comportement des utilisateurs doivent être supprimées lorsqu'elles ne sont plus nécessaires à la constitution d'un profil. Les durées de conservation illimitées ou excessivement longues sont contraires à l'article 6, paragraphe 1, point e), de la directive. Le groupe de travail a constaté que les périodes de conservation varient chez les grands fournisseurs de réseaux publicitaires, certains ayant des durées illimitées tandis que d'autres limitent la durée de conservation à trois mois.

Dès lors, le groupe de travail invite instamment les fournisseurs de réseaux publicitaires à adopter des dispositions destinées à garantir que les informations collectées à chaque lecture d'un cookie sont immédiatement effacées ou anonymisées dès que la nécessité de les conserver a disparu. Chaque responsable de traitement doit être en mesure de justifier la nécessité d'un délai de conservation donné. Le groupe de travail insiste pour que les fournisseurs de réseaux publicitaires apportent la justification de la durée de conservation qu'ils jugent nécessaire au vu des finalités que poursuit le traitement des données.

Lorsqu'un particulier demande l'effacement de son profil et/ou exerce son droit de révoquer son consentement, ces actions obligent le fournisseur de réseau publicitaire à effacer ou à supprimer rapidement les données de la personne concernée dans la mesure où la base juridique nécessaire (c'est-à-dire le consentement) autorisant le traitement cesse d'exister.

5.3. Droits des personnes concernées

Les responsables de traitement doivent permettre aux personnes concernées par le traitement d'exercer leurs droits d'accès, de rectification, d'effacement et d'opposition, tels qu'ils sont énoncés aux articles 12 et 14 de la directive sur la protection des données.

Le groupe de travail est au courant des initiatives des fournisseurs de réseaux publicitaires, consistant à donner accès aux catégories de centres d'intérêt auxquelles les personnes concernées ont été associées sur la base du cookie «numéro ID»[88]. Ces nouveaux outils permettent aux utilisateurs d'accéder aux catégories de centres d'intérêt auxquelles ils sont associés, mais aussi de les modifier et de les supprimer.

[88] Voir le «Ad Interest Manager» de Yahoo à l'adresse: http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/. Voir également la page «Gestionnaire de préférences pour les annonces» de Google à l'adresse: http://www.google.com/ads/preferences/html/about.html.

Le groupe de travail est favorable à ces initiatives qui contribuent à rendre effectif le droit des personnes d'avoir facilement accès à leurs données à caractère personnel et de les corriger. Il insiste auprès des fournisseurs de réseaux publicitaires afin qu'ils mettent en place des procédures visant à informer les particuliers sur ces outils et à les rendre aussi visibles que possible pour les personnes concernées, de sorte que l'utilisateur moyen soit effectivement en mesure de les utiliser.

5.4. Autres obligations

L'article 17 de la directive impose aux responsables du traitement et aux sous-traitants de mettre en oeuvre les ***mesures techniques et d'organisation*** appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, la diffusion et d'autres formes de traitement illicite. Le respect des obligations de sécurité contraindra les fournisseurs de réseaux publicitaires à mettre en oeuvre des mesures techniques et organisationnelles de pointe pour garantir la sécurité et la confidentialité des données.

En application de l'article 18 de la directive 95/46/CE, le responsable du traitement peut être tenu de ***notifier le traitement*** de données à caractère personnel aux autorités chargées de la protection des données, à moins qu'il n'en soit dispensé.

Par conséquent, si le droit national l'impose, le fournisseur de réseau publicitaire doit notifier le traitement des données. En outre, si les données font l'objet d'un transfert à l'extérieur de l'UE, par exemple vers des serveurs situés dans des pays tiers, le fournisseur de réseau publicitaire doit s'assurer que les dispositions relatives aux transferts de données à caractère personnel vers des pays tiers sont respectées (articles 25 et 26 de la directive 95/46/CE).

6. Conclusions et recommandations

Les techniques de publicité comportementale permettent aux annonceurs, essentiellement des fournisseurs de réseaux publicitaires, de suivre les particuliers lorsqu'ils surfent sur l'internet, afin de constituer des profils et de s'en servir pour diffuser des publicités ciblées. Dans la plupart des cas, les particuliers ignorent tout simplement qu'ils font l'objet de cette pratique.

Le groupe de travail s'inquiète fortement des conséquences que cette pratique de plus en plus répandue pourrait avoir sur la protection des données et de la vie privée. Bien que la législation en la matière impose, entre autres, d'obtenir un consentement informé des particuliers pour recourir à cette pratique, dans la réalité, il est extrêmement douteux que l'utilisateur moyen sache qu'on suit son comportement afin de lui envoyer des annonces personnalisées, et encore plus douteux qu'il soit consentant.

Jusqu'à présent, les procédures par lesquelles les professionnels fournissent des informations et permettent aux particuliers de décider s'ils veulent être suivis ont échoué. Les mentions contenues dans les conditions générales et/ou dans les politiques de confidentialité, souvent rédigées en termes obscurs, sont loin de satisfaire aux exigences de la législation sur la protection des données. Dans certains États membres, les professionnels ont toutefois consenti quelques efforts pour combler les lacunes du droit existant par des mesures d'autorégulation. Ces efforts sont les bienvenus dans la mesure où ils précisent les principes généraux énoncés dans le cadre réglementaire. Cependant, de l'avis du groupe de travail, il reste encore beaucoup à faire. Les professionnels du secteur doivent accroître leurs efforts pour se conformer à la législation désormais renforcée.

Par le présent avis, le groupe de travail souhaite guider les parties prenantes, en particulier les fournisseurs de réseaux publicitaires et les diffuseurs, afin qu'ils se conforment au cadre législatif en vigueur tel qu'il est interprété ici. À cet effet, le présent avis expose le point de vue du groupe de travail sur la manière d'interpréter la législation sur la protection des données régissant la pratique de la publicité comportementale. Il appelle en outre les professionnels à présenter des mesures techniques et d'autre nature en vue de se conformer au cadre décrit dans le présent avis, et à échanger de vues avec le groupe de travail sur ces mesures. À l'issue d'une certaine période de «discussion», le groupe de travail évaluera la situation et prendra les mesures appropriées nécessaires. En attendant, il invite

instamment les parties concernées à mettre en oeuvre les recommandations décrites ci-dessous.

6.1. Législation applicable

- Le cadre juridique de l'UE régissant l'utilisation des cookies est essentiellement constitué par l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques»[89].
- L'article 5, paragraphe 3, s'applique chaque fois que des «informations», comme un cookie, sont stockées dans l'équipement terminal d'un internaute ou récupérées à partir de celui-ci. Le caractère personnel de ces informations n'est pas une condition préalable.
- En outre, la directive 95/46/CE s'applique aux aspects qui ne sont pas spécifiquement couverts par la directive «vie privée et communications électroniques» chaque fois que des données à caractère personnel sont traitées. La publicité comportementale repose sur l'utilisation d'identifiants qui permettent de dresser des profils très détaillés de l'utilisateur, lesquels seront, dans la plupart des cas, considérés comme des données à caractère personnel.

6.2. Compétence territoriale – établissement

- La directive 95/46/CE s'applique au traitement de données effectué lorsque des diffuseurs et des fournisseurs de réseaux publicitaires font de la publicité comportementale, en vertu de l'article 4, paragraphe 1, points a) et c), de la directive 95/46/CE et de l'article 3 de la directive «vie privée et télécommunications électroniques». Les avis et recommandations existants du groupe de travail en la matière sont pleinement applicables.

6.3. Rôles et responsabilités

- Les fournisseurs de réseaux publicitaires sont soumis aux obligations imposées par l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» dans la mesure où ils placent des cookies et/ou récupèrent des informations à partir de cookies déjà installés dans l'équipement terminal des personnes concernées. Ce sont également des responsables du traitement dans la mesure où ils déterminent les finalités et les moyens essentiels du traitement des données.
- Les diffuseurs assument une part de la responsabilité incombant au responsable du traitement en ce qui concerne la première phase du traitement, c'est-à-dire lorsque, par la manière dont ils configurent leurs sites web, ils déclenchent le transfert de l'adresse IP de l'utilisateur vers les fournisseurs de réseaux publicitaires (ce qui permet le traitement ultérieur). Cette responsabilité entraîne quelques obligations limitées en termes de protection des données (voir plus loin). En outre, lorsque les diffuseurs transfèrent directement des données à caractère personnel identifiables aux fournisseurs de réseaux publicitaires, ils sont réputés coresponsables du traitement.

6.4 Obligations et droits

Fournisseurs de réseaux publicitaires:

- L'article 5, paragraphe 3, de la directive «vie privée et communications électroniques», qui établit l'obligation d'obtenir un consentement informé préalable, s'applique aux fournisseurs de réseaux publicitaires.
- Le paramétrage du navigateur ne peut être la manifestation d'un consentement que dans des cas très limités. Notamment, si les navigateurs sont configurés par défaut pour rejeter tous les cookies (le navigateur étant configuré pour cette option) et si l'utilisateur a modifié les paramètres pour accepter positivement les cookies, s'il a été pleinement informé du nom du responsable du traitement, du traitement lui-même, de ses finalités et des données qui sont collectées. Par conséquent, le navigateur doit, seul ou en combinaison avec d'autres moyens, transmettre effectivement des informations claires, complètes et parfaitement visibles au sujet du traitement.

[89] La version modifiée de la directive «vie privée et communications électroniques» doit entrer en vigueur en mai 2011.

- Les fournisseurs de réseaux publicitaires devraient encourager les fabricants/concepteurs de navigateurs et collaborer avec eux afin de concevoir des navigateurs qui protègent la vie privée.

- En règle générale, les mécanismes d'«opt-out» fondés sur des cookies ne sont pas une solution adéquate pour obtenir le consentement informé de l'utilisateur. En effet, dans la plupart des cas, le consentement de l'utilisateur est considéré comme implicite s'il ne procède pas à un «opt-out». Or, dans la pratique, très peu de personnes exercent cette option d'«opt-out», non parce qu'elles ont décidé en toute connaissance de cause d'accepter les publicités comportementales, mais parce qu'elles ne savent pas qu'un traitement a lieu, et encore moins comment procéder à un «opt-out».

- Les fournisseurs de réseaux publicitaires devraient abandonner au plus tôt les mécanismes d'«opt-out» et adopter des mécanismes d'«opt-in» préalable. Les dispositifs destinés à obtenir un consentement informé et valable devraient nécessiter une action positive de la personne concernée, par laquelle elle déclare accepter l'envoi de cookies et le suivi ultérieur de son comportement de navigation aux fins de lui adresser des annonces personnalisées.

- Conformément au considérant 25 de la directive «vie privée et communications électroniques», le fait qu'un utilisateur accepte de recevoir un cookie pourrait également emporter son acceptation des lectures ultérieures du cookie et, partant, du suivi de sa navigation sur l'internet. Il ne serait pas nécessaire de demander le consentement de la personne concernée à chaque lecture du cookie. Cependant, afin que la personne concernée demeure informée du suivi dans le temps, les fournisseurs de réseaux publicitaires devraient: i) limiter la portée du consentement dans le temps; ii) offrir la possibilité de révoquer aisément le consentement de la personne concernée à être suivie à des fins de diffusion de publicités comportementales et iii) créer un symbole ou un autre outil qui devrait être visible sur tous les sites web où le suivi a lieu (les sites web partenaires du fournisseur de réseau publicitaire). Ce symbole servirait non seulement à rappeler aux utilisateurs le suivi dont ils font l'objet, mais également à vérifier s'ils souhaitent encore être suivis ou s'ils veulent révoquer leur consentement.

- Les fournisseurs de réseaux devraient se conformer aux obligations qu'impose la directive 95/46/CE et qui n'empiètent pas directement sur l'article 5, paragraphe 3, à savoir le principe de limitation des finalités et les obligations liées à la sécurité.

- De surcroît, les fournisseurs de réseaux publicitaires devraient permettre aux particuliers d'exercer leurs droits d'accès, de rectification et d'effacement. Le groupe de travail est favorable à la pratique adoptée par certains fournisseurs de réseaux publicitaires, qui consiste à offrir aux personnes concernées la possibilité de consulter les catégories de centres d'intérêt qui leur ont été associées, et de les modifier.

- Les fournisseurs de réseaux publicitaires devraient appliquer des politiques de conservation des données qui garantissent que les informations collectées à chaque lecture d'un cookie sont automatiquement supprimées après un délai justifié (nécessaire au traitement). Cela s'applique également aux autres techniques de traçage utilisées pour la publicité comportementale, comme les applets JavaScript installées dans le navigateur web de l'utilisateur.

Fournisseurs de réseaux publicitaires et diffuseurs:

- Pour qu'un consentement soit valable, l'utilisateur doit recevoir des informations parfaitement visibles. En aucun cas la mention de la publicité comportementale dans les conditions générales et/ou dans la politique de confidentialité ne peut suffire. À cet égard, la pratique de la publicité comportementale étant peu connue dans la moyenne, des efforts devraient être déployés pour modifier cette situation.

- Les fournisseurs de réseaux publicitaires et les diffuseurs sont tenus de fournir des informations aux utilisateurs en vertu de l'article 10 de la directive 95/46/CE. Concrètement, ils devraient veiller à ce que les particuliers soient, à tout le moins, informés de l'identité du responsable (entité) du placement du cookie et de la collecte des informations connexes. En outre, les utilisateurs devraient être informés, en termes simples: (a) que le cookie servira à créer des profils; (b) du type d'informations qui seront collectées pour constituer ces profils; (c) que les profils serviront à diffuser des annonces ciblées et (d) que le cookie permettra l'identification de l'utilisateur dans de multiples sites web.
- Les fournisseurs de réseaux publicitaires et les diffuseurs devraient afficher les informations directement sur l'écran, de manière interactive et, si nécessaire, par des messages en couches. En tout état de cause, l'information doit être aisément accessible et extrêmement visible.
- Les icônes placées sur le site web du diffuseur, autour de l'annonce, avec des liens vers des informations supplémentaires, sont de bons exemples. Le groupe de travail invite instamment les fournisseurs de réseaux publicitaires et les diffuseurs à faire preuve de créativité dans ce domaine.

Fait à Bruxelles, le 22 juin 2010

Pour le groupe de travail
Le président
Jacob KOHNSTAMM

Recommandation CM/Rec (2010)13 du Comité des Ministres aux Etats membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage

Elaborée par le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE 198) et adoptée par le Comité des Ministres le 23 novembre 2010, lors de la 1099ème réunion des Délégués des Ministres

Le Comité des Ministres,

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres ;

Constatant que les technologies de l'information et de la communication (TIC) permettent la collecte et le traitement de données à grande échelle, y compris pour les données à caractère personnel, dans le secteur public comme dans le secteur privé ; constatant que les TIC sont utilisées à des fins très diverses, notamment pour des services largement acceptés et appréciés par la société, les consommateurs et l'économie ; constatant par ailleurs que le développement continu de technologies convergentes pose de nouveaux défis en matière de collecte et de traitement ultérieur des données ;

Constatant que la collecte et le traitement peuvent se produire dans différentes situations à différentes fins et concerner différents types de données, telles que les informations sur la circulation et les demandes d'internautes, les habitudes d'achat, activités, mode de vie et comportement des consommateurs, les informations concernant les usagers d'appareils de télécommunication, y compris les données de géolocalisation, ainsi que celles provenant en particulier des réseaux sociaux, des systèmes de vidéosurveillance, des systèmes biométriques et des systèmes d'identification par radiofréquence (FRID) préfigurant l'« internet des objets » ; constatant qu'il est souhaitable d'évaluer les différentes situations et fins d'une manière différenciée ;

Constatant que les données ainsi collectées sont notamment traitées par des logiciels de calcul, de comparaison et de corrélation statistique, dans le but de dégager des profils qui pourraient être utilisés de maintes manières à différentes fins et pour différents usages par l'appariement des données de plusieurs individus ; constatant que le développement des TIC permet de réaliser ces opérations à un coût relativement faible ;

Considérant que, par cette mise en relation d'un grand nombre de données individuelles, mêmes anonymes, la technique du profilage peut avoir des incidences pour les personnes concernées en les plaçant dans des catégories prédéterminées, très souvent à leur insu ;

Considérant que les profils, lorsqu'ils sont attribués à une personne concernée, permettent de générer des nouvelles données à caractère personnel qui ne sont pas celles que la personne concernée a communiquées au responsable de traitement ou dont elle peut raisonnablement présumer la connaissance par le responsable de traitement ;

Considérant que le manque de transparence, voire l'« invisibilité », du profilage et le manque de précision qui peut découler de l'application automatique de règles d'inférence préétablies risquent de faire peser de graves menaces sur les droits et libertés de l'individu ;

Considérant en particulier que la protection des droits fondamentaux, et notamment le droit à la vie privée et à la protection des données à caractère personnel, suppose l'existence de sphères de vie différentes et indépendantes où chaque individu peut contrôler l'usage qu'il/elle fait de son identité ;

Considérant que le recours au profilage peut être dans l'intérêt légitime de la personne qui l'utilise comme de celle qui se le voit appliquer, notamment en conduisant à une meilleure segmentation des marchés, en permettant l'analyse du risque ou de la fraude, ou encore en adaptant l'offre à la demande par la fourniture de meilleurs services ; et considérant que le profilage peut donc présenter des avantages pour l'utilisateur, l'économie et la société dans son ensemble ;

Considérant néanmoins que le profilage d'un individu peut avoir pour conséquence de le priver de manière injustifiée de l'accès à certains biens ou services et porte donc atteinte au principe de non-discrimination ;

Considérant par ailleurs que les techniques de profilage, lorsqu'elles mettent en évidence des corrélations entre des données sensibles au sens de l'article 6 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108, ci-après la « Convention n° 108 ») et d'autres données, peuvent permettre de générer de nouvelles données sensibles concernant une personne identifiée ou identifiable ; considérant par ailleurs que ce profilage peut exposer les individus à des risques particulièrement élevés de discrimination et d'atteintes à leurs droits personnels et à leur dignité ;

Considérant que le profilage des enfants peut avoir des conséquences graves pour eux durant toute leur vie et, étant donné qu'ils ne sont pas à même d'exprimer seuls un consentement libre, spécifique et éclairé lors de la collecte de données à caractère personnel à des fins de profilage, il est nécessaire de prendre des mesures spécifiques et appropriées de protection de l'enfance afin de tenir compte de l'intérêt supérieur de l'enfant et du développement de sa personnalité, conformément à la Convention des Nations Unies relative aux droits de l'enfant ;

Considérant que l'utilisation de profils, même de manière légitime, sans précautions ni garanties particulières, est susceptible de porter gravement atteinte à la dignité de la personne de même qu'à d'autres libertés et droits fondamentaux, y compris aux droits économiques et sociaux ;

Persuadé qu'il est donc nécessaire de réglementer le profilage en termes de protection des données à caractère personnel, afin de sauvegarder les libertés et droits fondamentaux des individus, notamment le droit à la vie privée, et de prévenir la discrimination fondée sur le sexe, la race ou l'origine ethnique, la religion ou les convictions, le handicap, l'âge ou l'orientation sexuelle ;

Rappelant à cet égard les principes généraux relatifs à la protection des données de la Convention n° 108 ;

Rappelant que toute personne doit avoir le droit d'accéder aux données la concernant et considérant qu'elle devrait connaître la logique qui sous-tend le profilage ; sachant que ce droit ne devrait pas porter atteinte aux droits et libertés d'autrui, en particulier ne pas nuire aux secrets commerciaux, à la propriété intellectuelle ou au droit d'auteur protégeant les logiciels ;

Rappelant la nécessité de respecter les principes déjà établis par d'autres recommandations pertinentes du Conseil de l'Europe, en particulier la Recommandation Rec(2002)9 sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance et la Recommandation Rec(97)18 concernant la protection des données à caractère personnel collectées et traitées à des fins statistiques ;

Tenant compte de la Convention du Conseil de l'Europe sur la cybercriminalité (STE n° 185 – Convention de Budapest), qui contient des dispositions relatives à la conservation, à la collecte et à l'échange de données, conformément aux conditions et sauvegardes visant à assurer une protection adéquate des droits de l'homme et des libertés ;

Tenant compte à la fois de l'article 8 de la Convention européenne des droits de l'homme (STE n° 5), tel qu'il est interprété par la Cour européenne des droits de l'homme, et des risques nouveaux engendrés par l'utilisation des technologies de l'information et de la communication ;

Considérant que la protection de la dignité humaine et d'autres droits et libertés fondamentaux dans le cadre du profilage ne peut être effective que si, et seulement si, toutes les parties prenantes contribuent ensemble à un profilage loyal et licite des individus ;

Tenant compte du fait que la mobilité des individus, la mondialisation des marchés et l'utilisation des nouvelles technologies nécessitent des échanges d'informations transfrontières, y compris dans le cadre du profilage, et requièrent une protection des données équivalente dans tous les Etats membres du Conseil de l'Europe,

Recommande aux gouvernements des Etats membres :

1 d'appliquer l'annexe à la présente recommandation à la collecte et au traitement des données à caractère personnel utilisées dans le cadre du profilage en prenant notamment des mesures pour que les principes contenus dans l'annexe à la présente recommandation soient reflétés dans leur droit et leur pratique ;

2. d'assurer une large diffusion des principes contenus dans l'annexe à la présente recommandation parmi les personnes, les autorités publiques et les organismes publics et privés, notamment ceux qui concourent ou recourent au profilage, tels que les concepteurs et fournisseurs de logiciels, les concepteurs de profils, les fournisseurs de services de communication électronique et les prestataires de service de la société de l'information, ainsi que parmi les instances compétentes en matière de protection des données et les organismes de normalisation ;

3. d'inciter ces personnes, autorités publiques et organismes publics et privés à introduire et à promouvoir des mécanismes d'autorégulation, tels que des codes de conduite, qui assurent le respect de la vie privée et la protection des données, et à mettre en place des technologies inspirées de l'annexe à la présente recommandation.

Le collège :
Pierre WEIMERSKIRCH, Gérard LOMMEL et Thierry LALLEMANG

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

Commission Nationale
pour la Protection
des Données

41, avenue de la gare, L-1611 Luxembourg
Siège : L-4100 Esch-sur-Alzette
téléphone : +352 26 10 60 -1 - Fax : +352 26 10 60 - 29

www.cnpd.lu