CNPD

COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

# Rapport annuel 2014

CNPD

COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

# Rapport annuel 2014

# Table des matières

## Mission

La Commission nationale pour la protection des données (CNPD) est une autorité indépendante instituée par la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Elle est chargée de 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.

Sa mission s'étend également à assurer le respect des dispositions de la loi modifiée du 30 mai 2005 sur la protection de la vie privée dans le secteur des communications électroniques.

Superviser et assurer la transparence par :

- L'examen préalable des traitements soumis à autorisation ;
- La publicité réalisée au moyen du registre des traitements notifiés ;
- Les investigations suite à des plaintes ou de sa propre initiative ;
- L'intervention suite à des violations de données dans le secteur des communications électroniques.

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

# 1 Avant-propos

*Le collège :*
*Georges Wantz, Tine A. Larsen, Thierry Lallemang*

La protection des données à caractère personnel n'a jamais été autant au cœur des préoccupations européennes. L'année 2014 n'était pas seulement marquée par les travaux de révision de la législation européenne en la matière, mais également par deux arrêts de la Cour de Justice de l'Union européenne, celui du 8 avril 2014, qui invalide la directive sur la rétention des données et celui du 13 mai 2014, qui consacre un droit à l'oubli au profit des citoyens[1].

La directive de 1995 sur la protection des données est en cours de révision depuis janvier 2012. Cette réforme vise à conférer au cadre juridique l'effectivité nécessaire à l'ère numérique, de la

[1] La partie 4 « Perspectives » est consacrée à ces arrêts et à leurs conséquences.

globalisation, du Big Data et de l'Internet des objets. Très sensible et vivement discuté au Parlement européen avec plus de 4.000 amendements, le projet de règlement va modifier substantiellement le cadre actuel de la protection des données en Europe et au Luxembourg.

Toutefois, les négociations s'avèrent plus longues que prévu. Le Conseil de l'Union européenne n'a pas encore été en mesure de trouver un accord à la fin de l'année 2014. L'achèvement du train de mesures relatives à la protection des données et le futur de la rétention des données constitueront sans doute des objectifs prioritaires pour la Présidence luxembourgeoise du Conseil de l'Union européenne en 2015.

Le texte n'est pas encore figé, mais prévoit d'ores et déjà un renforcement et une clarification des droits individuels, une conduite préventive et responsable de la part des acteurs privés et publics à l'égard des données à caractère personnel qu'ils collectent, sauvegardent, utilisent et transmettent à des tiers et un renforcement du rôle des autorités de contrôle. Il est également prévu de renforcer le rôle des chargés de la protection des données.

Les différents acteurs devront pouvoir compter sur la CNPD pour les orienter, conseiller et assister dans cette délicate démarche. Dans la version actuelle du projet de règlement, il est prévu que l'autorité de contrôle aura un réel pouvoir de sanction et pourra infliger des amendes aux organismes qui violent les règles allant jusqu'à 100 millions d'euros ou équivalent à 5% de leur chiffre d'affaires.

Grâce au nouveau règlement, qui prévoit une simplification administrative par la suppression des notifications et autorisations préalables, la charge administrative des responsables du traitement, tout comme celle de la CNPD devrait être allégée de sorte à libérer le personnel de cette dernière pour les nouvelles missions prioritaires que le règlement introduira comme le contrôle à posteriori et le rôle accru de guidance.

Depuis sa création en 2002, la CNPD a vu sa charge de travail croître de manière significative. Les dernières années ont été caractérisées par une augmentation importante du nombre de plaintes, de demandes de renseignement et d'avis. À ceci s'ajoutent de plus en plus de dossiers technologiques très complexes avec des implications transfrontalières.

En 2014, l'activité globale de la Commission nationale a été marquée, comme les années précédentes, par une forte croissance. Elle a reçu un nombre record de 207 plaintes, 2.192 demandes de renseignement et 999 demandes d'autorisation préalables. 609 notifications ont été reçues et 22 investigations ont été menées.

La CNPD intervient après avoir reçu une plainte, de sa propre initiative ou lorsqu'elle prend connaissance d'une violation des règles de protection des données à caractère personnel. En mai, elle a lancé une procédure d'investigation auprès de la société eBay, qui avait annoncé qu'elle était devenue victime d'une attaque informatique, qui a compromis la base de données de ses clients. La CNPD a également clôturé l'analyse du contrat des services (MSA) de Microsoft, effectuée en collaboration avec l'autorité française de protection des données CNIL.

La guidance des acteurs privés et publics reste une priorité pour la CNPD. Dans le domaine de la santé, elle accompagne actuellement activement l'agence eSanté dans l'évaluation de leur plateforme d'échange de données. Dans le cadre de ce projet, la CNPD a proposé

# 1 Avant-propos

d'effectuer un « Privacy Impact Assessment » (PIA). Cette démarche consiste à analyser les risques pour les personnes concernées et d'évaluer le respect des principes de protection des données à caractère personnel.

Bien que le nouveau projet de règlement européen sur la protection des données prescrira une telle évaluation préalable pour tous les nouveaux systèmes de traitement potentiellement intrusifs ou susceptibles de comporter des risques particuliers ne soit pas encore en vigueur, l'étendue et le degré de sensibilité du projet du dossier de soins partagés (DSP) justifient d'adopter d'ores et déjà une telle approche de protection des données dès la conception (« Privacy by design »).

C'est aussi dans une optique d'anticipation de la future législation que la CNPD accompagne depuis 2013 le GIE Luxmetering avec une étude d'impact sur la vie privée dans le cadre de la mise en œuvre des futures compteurs d'énergie intelligents (« smart metering »).

La nouvelle brochure relative à la surveillance sur le lieu de travail constitue une mesure supplémentaire prise par la CNPD pour guider les responsables du traitement qui veulent mettre en place un dispositif de surveillance. Éditée en collaboration avec la Chambre des Salariés (CSL), cette publication a comme objectif d'éclairer le lecteur sur les droits et obligations du salarié ainsi que sur les obligations de l'employeur en la matière.

L'autorité de protection des données luxembourgeoise a par ailleurs avisé des projets de loi ou mesures réglementaires concernant notamment la rétention des données, l'organisation du Service de Renseignement de l'Etat, la réforme du statut de l'artiste, l'échange transfrontalier d'informations sur les infractions en matière de sécurité routière, la jeunesse, les subventions de loyer et le classement des établissements d'hébergements touristiques. Outre ces avis formels, la CNPD a été consultée par divers ministères et organismes publics sur la conformité d'une multitude de pratiques ou de projets.

Pour les collaborateurs et services de la CNPD, l'année 2014 était marquée par un changement important au niveau de sa direction. Lors de sa séance du 7 novembre 2014, le Conseil de gouvernement a annoncé la nomination de Tine A. Larsen, Thierry Lallemang et Georges


*Le siège de la CNPD à Belval*

Wantz en tant que membres effectifs. Un défi majeur de la nouvelle Commission sera de moderniser les procédures internes pour permettre à la CNPD d'être prête pour ses nouvelles missions et de recruter davantage de personnel pour préparer la CNPD aux exigences du monde numérique et aux obligations du futur règlement européen.

Luxembourg, le 21 mai 2015

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

# 2 Les activités en 2014

## L'année 2014 en un coup d'œil

### Janvier

27 - La CNPD organise avec l'Université du Luxembourg une table ronde sur le sujet « *Les défis en matière de protection de la vie privée dans un monde interconnecté* »
28 - Journée de la protection des données

### Février

27 - Gérard Lommel est élu vice-président du groupe de travail européen de l'« Article 29 »
28 - La CNPD intervient à la Conférence du Jeune Barreau de Luxembourg pour parler de la surveillance sur le lieu de travail

### Mars

11 - La CNPD participe à la conférence inaugurale de l'Association pour la protection des données au Luxembourg (APDL)
21 - La CNPD intervient lors de la 4e journée des archivistes luxembourgeois
24 - La CNPD émet son avis au sujet de la réforme du statut de l'artiste

### Avril

3 - La CNPD participe à la réunion de coordination annuelle du GPEN
8 - La Cour de Justice de l'UE déclare la directive sur la conservation des données invalide

### Mai

13 - La Cour de Justice de l'UE estime que certains utilisateurs ont le droit de demander aux moteurs de recherche tels que Google de supprimer certains résultats de recherche qui incluent des données à caractère personnel
13 - La CNPD examine la conformité de la législation nationale en matière de rétention des données avec les exigences posées par la CJUE du 8 avril 2014

### Juin

5 - La CNPD participe à la Conférence européenne des autorités de protection des données à Strasbourg
27 - La CNPD décide de lancer une procédure d'investigation suite à l'attaque informatique contre la société eBay

### Juillet

14 - La CNPD émet un avis complémentaire relatif au projet de loi n°6566 facilitant l'échange transfrontalier d'informations concernant les infractions en matière de sécurité routière
14 - La CNPD émet un avis sur les modèles de cartes d'identité pour les membres des Corps diplomatique et consulaire résident et les agents de l'Union européenne et des Organisations internationales ayant leur siège au Luxembourg
21 - La CNPD émet un avis sur le projet de loi n°6410 portant modification de la loi du 4 juillet 2008 sur la jeunesse
21 - La CNPD se prononce sur le projet de loi n°6542 portant introduction d'une subvention de loyer et modifiant la loi modifiée du 25 février 1979 concernant l'aide au logement

## DELIBERATIONS

**629**
Délibérations adoptées

**8**
Avis relatifs à des projets ou propositions de loi ou mesures réglementaires

**25**
Agréments pour les chargés de la protection des données

## FORMALITES PREALABLES

**609**
Notifications reçues

**999**
Demandes d'autorisations

**6.993**
Déclarants (depuis 2002)

## DEMANDES DE RENSEIGNEMENT

**2.192**
Demandes
(+5% par rapport à 2013)

## PLAINTES ET INVESTIGATIONS

**207**
Plaintes
(+16% par rapport à 2013)

**22**
Investigations

## VIOLATIONS DE DONNEES (COMMUNICATIONS ELECTRONIQUES)

**0**
Notifications

**31** - La CNPD émet un avis sur le projet de loi n°6604 relatif au classement des établissements d'hébergement touristique
**31** - La CNPD émet un avis sur le projet de loi n°6675 1) portant organisation du Service de Renseignement de l'Etat; 2) modifiant certaines lois ; 3) abrogeant la loi du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat

### Septembre

**19** - La CNPD participe au séminaire « Les enjeux européens et mondiaux de la protection des données personnelles », organisé par l'Union Internationale des Avocats (UIA) à la Cour de Justice de l'UE

### Octobre

**7** - La CNPD et la Chambre des Salariés présentent une nouvelle publication relative à la surveillance sur le lieu de travail
**16** - Le Luxembourg ratifie la convention sur la cybercriminalité du Conseil de l'Europe
**16** - La CNPD participe à la 36e conférence internationale des commissaires à la protection des données à l'île Maurice

### Novembre

**7** - Le Conseil de gouvernement annonce la nomination de Tine A. Larsen (juriste), Thierry Lallemang (juriste) et Georges Wantz (informaticien) en tant que membres effectifs de la CNPD. Madame Larsen assumera la présidence du collège de la CNPD
**28** - La CNPD participe à une conférence organisée par COPAS sur les dossiers de soins informatisés

### Décembre

**11** - La Cour de Justice de l'UE estime que la directive sur la protection des données s'applique à la vidéosurveillance au domicile d'un particulier si la caméra est dirigée vers la voie publique

# 2 Les activités en 2014

## Le registre public

La loi prescrit la tenue d'un registre public par la CNPD *(http://www.cnpd.public.lu/fr/registre)*. Ce registre permet aux citoyens de vérifier si un responsable (entreprise, administration, etc.) a déclaré ses traitements et s'il est susceptible de détenir des informations les concernant.

Figurent dans ce registre :
- les traitements notifiés à la CNPD,
- les traitements autorisés par la CNPD et
- les traitements surveillés par les chargés de la protection des données figurant sur leurs relevés transmis à la CNPD.

Ne figurent pas dans le registre public :
- les traitements de données exemptés de déclaration et
- les traitements, soumis à autorisation préalable, qui n'ont pas été autorisés.

Le travail de la Commission nationale pendant l'année 2014 était centré sur les activités suivantes :

- Le traitement des notifications et des autorisations préalables ;
- L'analyse des plaintes et demandes de vérification de licéité ;
- Les contrôles et investigations ;
- Les avis concernant les projets de loi et mesures réglementaires ;
- L'information et la sensibilisation du public ;
- Le conseil et la guidance des acteurs publics et privés ;
- Les activités internationales et en particulier la participation aux travaux sur le plan européen.

## 2.1 Supervision de l'application de la loi

### 2.1.1 Formalités préalables

Le législateur luxembourgeois prévoit que tout traitement de données à caractère personnel doit en principe être notifié à la Commission nationale. Les traitements les plus courants sont exempts de déclaration, tandis que certains traitements plus « sensibles » requièrent une autorisation préalable de la CNPD.

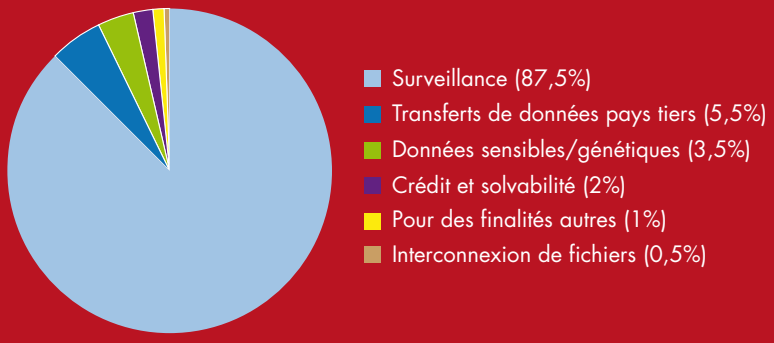
Le nombre total des traitements de données déclarés depuis 2003 s'élève à 22.321. En tout,

## Quels sont les traitements soumis à autorisation ?

| | | |
|---|---|---|
| Surveillance et surveillance sur le lieu de travail | Traitement de données biométriques (contrôle de l'identité de personnes) | Traitement de données génétiques (dans certains cas) |
| Interconnexion de données | Utilisation ultérieure de données pour d'autres objectifs (p.ex. statistiques) | Traitements relatifs au crédit et à la solvabilité de personnes |

Cas spécifiques : transfert de données vers un pays hors UE ne présentant pas un niveau de protection adéquat

## Statistiques demandes d'autorisation 2003-2014




6.993 déclarants/responsables se sont ainsi conformés aux devoirs de déclaration imposés par la loi depuis 2002.

Avec son projet de règlement sur la protection des données, la Commission européenne prévoit de simplifier certaines contraintes administratives, notamment en supprimant les obligations de notification pour les organismes qui traitent des données à caractère personnel.

### *2.1.1.1 Les notifications préalables*

Les traitements de données à caractère personnel non exemptés de déclaration et non soumis à autorisation préalable doivent faire l'objet d'une notification préalable.

Il existe deux types de notifications : les notifications ordinaires et les engagements formels de conformité.

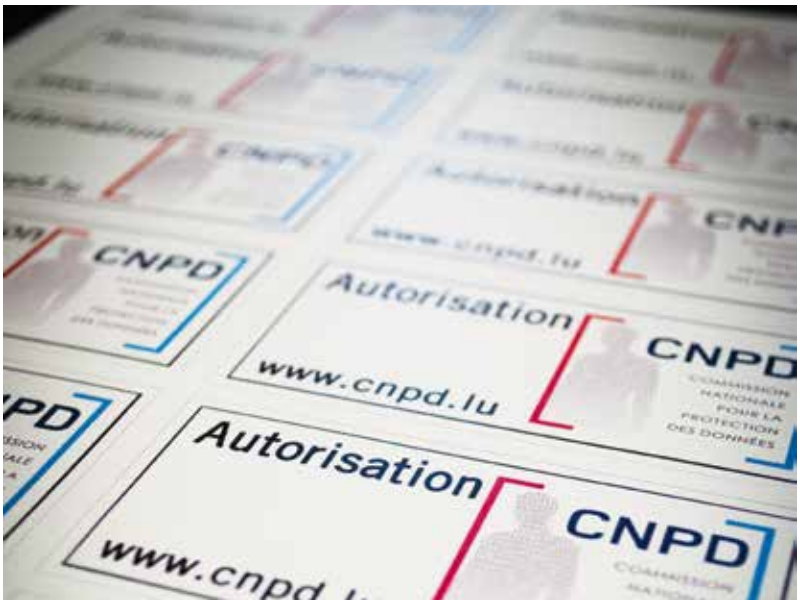
#### Notifications ordinaires

En 2014, la CNPD a reçu 564 notifications ordinaires, ce qui constitue une augmentation de 33% par rapport à l'année précédente. La finalité invoquée le plus souvent était l'administration du personnel. D'autres raisons citées pour traiter des données dans le cadre de notifications étaient : la gestion de la clientèle, la comptabilité, la gestion des fournisseurs ou encore la recherche scientifique.

#### Engagements formels de conformité

La loi prévoit, à côté des notifications ordinaires, une forme simplifiée de notification (« notification unique »). Cette notification unique se limite aux traitements déterminés par la Commission nationale par le biais de « décisions uniques ». Lorsque les traitements en question correspondent en tous points aux conditions fixées dans

# 2 Les activités en 2014




les décisions uniques afférentes, le responsable du traitement adresse à la Commission nationale un engagement formel par lequel il déclare que le traitement est conforme à la description figurant dans la décision unique.

Par sa décision n°108/2007 du 14 septembre 2007, la Commission nationale a défini les modalités des traitements de données que les employeurs (chefs d'entreprise, chefs d'établissement ou leurs délégués) sont amenés à opérer dans le cadre de l'organisation et du déroulement des élections des délégués du personnel, des délégations des jeunes travailleurs et des représentants du personnel dans les comités mixtes d'entreprise et les conseils d'administration des sociétés anonymes.

La CNPD a reçu 651 engagements formels de conformité dans le contexte des élections sociales de 2013. En 2014, elle en a reçu 45.

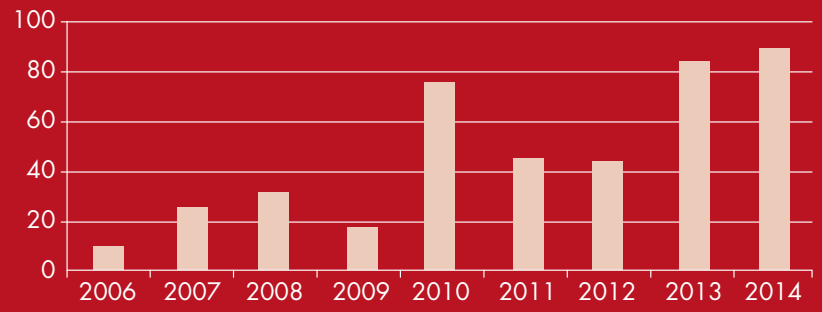
#### *2.1.1.2 Les autorisations préalables*

Les traitements présentant un risque particulier au regard de la vie privée des personnes concernées ne sont possibles que moyennant une autorisation de la Commission nationale. Ces dossiers nécessitent toujours une analyse détaillée et une appréciation circonstanciée et pondérée au cas par cas.

##### Demandes d'autorisation

Le nombre des demandes d'autorisation reçu par la CNPD continue à augmenter : 914 demandes lui ont été soumises

## Transferts vers des pays tiers




en 2014 (contre 833 en 2013). Elle n'a jamais reçu autant de demandes en une année depuis sa création.

La grande majorité des demandes sont relatives à la surveillance. 57% concernent l'exploitation de caméras de surveillance et 21% le contrôle des déplacements de véhicules et de personnes grâce à la géolocalisation. Les demandes concernant les dispositifs de géolocalisation ont augmenté de façon significative en 2014 tandis que celles concernant la vidéosurveillance, l'enregistrement des conversations téléphoniques et la surveillance des outils informatiques sont restées constantes.

### Engagements formels de conformité

En plus des demandes d'autorisation, la Commission nationale a reçu 85 engagements formels de conformité en 2014. La loi prévoit une procédure allégée d'autorisation (« autorisation unique ») pour certains traitements déterminés par la Commission nationale. Il s'agit actuellement de la surveillance électronique des horaires et des accès. Pour pouvoir bénéficier d'une telle autorisation, le responsable du traitement doit adresser un engagement formel par lequel il déclare que le traitement est conforme à la description figurant dans la décision unique de la Commission nationale.

## 2.1.2 Transferts de données hors Union européenne

### *2.1.2.1 Autorisation en cas de transferts de données vers des pays tiers*

En principe, il est interdit de transférer des données à caractère personnel vers des pays situés hors de l'Espace économique européen (Union européenne, Liechtenstein, Norvège et Islande) n'assurant pas une protection adéquate. Si une entreprise veut transférer des données personnelles du Luxembourg vers un destinataire établi en dehors de cette « sphère de sécurité » (pays ayant transposé la directive européenne 95/46/CE), elle devra demander une autorisation préalable à la CNPD.

Il existe toutefois trois exceptions à ce principe :

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

- Les dérogations légales[2] : consentement de la personne concernée, nécessité pour l'exécution d'un contrat conclu dans l'intérêt de la personne concernée, intérêt public important… ;

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

En 2014, la Commission nationale a été saisie de 91 demandes d'autorisation en vue

[2] Conditions énumérées à l'article 19 (1) de la loi modifiée du 2 août 2002 et également prévues dans la directive.

# 2 Les activités en 2014

du transfert de données vers des pays tiers. Ce chiffre est en légère hausse par rapport à l'année précédente. La majorité des demandes émanaient d'entreprises du secteur financier. Les pays de destination étaient le plus souvent les Etats-Unis.

En effet, de plus en plus d'entreprises collaborent avec des partenaires commerciaux et offrent leurs produits et services sur des marchés lointains hors d'Europe. Le développement des échanges commerciaux et la mondialisation ont entraîné un accroissement des transferts de données à caractère personnel dans le cadre de projets de centralisation et d' « outsourcing » de la gestion du personnel, de la clientèle ou des fournisseurs, ainsi que dans le contexte de l'externalisation de leurs activités informatiques.

### *2.1.2.2 Approbation de règles d'entreprise contraignantes*

Les règles d'entreprise contraignantes (« Binding Corporate Rules ») constituent un outil susceptible d'assurer une protection adéquate des données à caractère personnel lorsque celles-ci sont transférées ou traitées en dehors de l'Union européenne.

Elles représentent une alternative juridique intéressante pour les groupes de sociétés qui se voient amenés à transférer régulièrement des données à caractère personnel de leurs sociétés établies sur le territoire de l'UE

vers d'autres entités du groupe situées dans des pays tiers. Les entreprises peuvent adopter ces règles de leur propre initiative et les appliquer aux transferts de données entre les sociétés qui font partie d'un même groupe.

Les « BCR » présentent de nombreux avantages pour un groupe d'entreprises multinationales :

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

Au cours des dernières années, la CNPD a gagné de l'expérience dans ce domaine en prenant le rôle de chef de file dans l'examen des chartes « BCR » du groupe eBay en 2009 et du groupe ArcelorMittal en 2013.

La Commission nationale a par ailleurs analysé et approuvé les règles d'entreprise contraignantes de plusieurs groupes multinationaux lui soumises par d'autres autorités de protection des données européennes.

### 2.1.3 Les chargés de la protection des données

Tout responsable du traitement dispose de la faculté de désigner un chargé de la protection des données. Avant la modification de la loi en 2007, il n'était pas possible de désigner une personne salariée de l'organisme responsable du traitement, mais il fallait recourir à un chargé externe inscrit à la liste des personnes agréées par la CNPD afin d'exercer cette fonction.

Depuis 2007, sur suggestion de la CNPD, les salariés peuvent également être désignés comme chargés, à condition que ces derniers bénéficient d'une certaine indépendance vis-à-vis des responsables du traitement qui les ont désignés et qu'ils disposent du temps approprié pour pouvoir s'acquitter de leurs missions.

Les responsables ayant désigné un chargé de la protection des données sont exemptés du devoir de notification des traitements qu'ils mettent en œuvre. Ces derniers doivent cependant figurer dans le registre des traitements que le chargé doit établir, tenir à jour de façon permanente et transmettre tous les quatre mois à la CNPD.

Le chargé doit surveiller le respect des dispositions de la loi et des règlements d'exécution. A cet effet, il dispose d'un pouvoir d'investigation et d'un droit d'information auprès du responsable du traitement et, corrélativement, d'un droit d'informer le responsable du traitement des formalités à accomplir afin de se conformer aux dispositions légales et réglementaires en la matière. Le chargé doit en outre consulter la Commission nationale en cas de doute quant à la conformité à la loi des traitements mis en œuvre sous sa surveillance.

Avec la désignation d'un chargé, l'expertise de la protection des données fait son entrée dans les entreprises ou autres organismes. Le projet de règlement européen actuellement discuté entend introduire cette fonction du chargé de la protection des données partout dans l'Union européenne.

Depuis 2005, 87 entreprises, associations et organismes publics ont désigné un chargé de la protection des données. À la fin de l'année 2014, 105 personnes physiques ou morales étaient agréées pour exercer l'activité de chargé de la protection des données.

# 2 Les activités en 2014

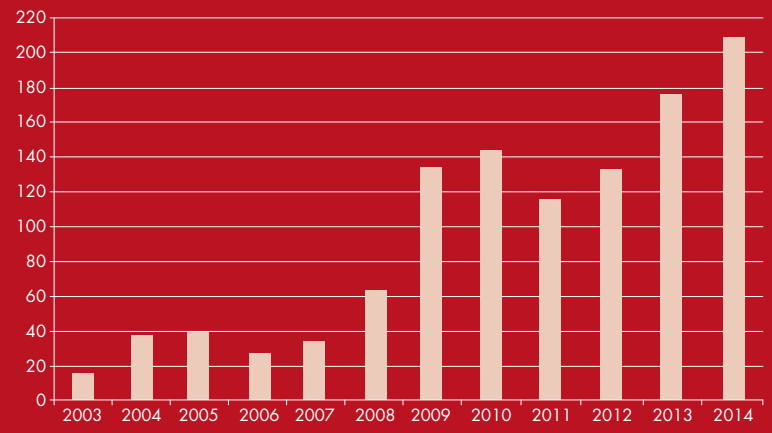
## 2.1.4 Demandes de vérification de licéité et plaintes

En 2014, la Commission nationale a reçu un nombre total de 207 plaintes et de demandes de vérification de licéité. Le nombre de personnes ayant fait appel à la CNPD lorsqu'elles ont estimé qu'il y a eu violation de la loi ou entrave à l'exercice de leurs droits a ainsi atteint à nouveau un niveau record.

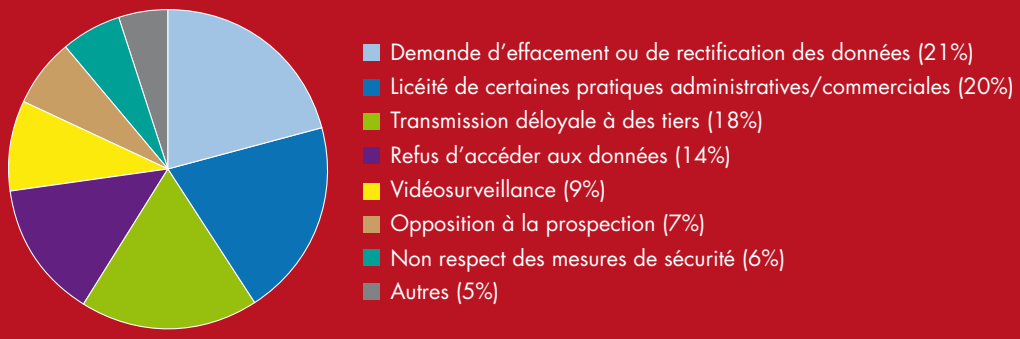
Deux tiers des plaintes proviennent d'autres États membres de l'Union européenne, que ce soit par l'intermédiaire des autorités de protection des données qui agissent au nom de leurs propres citoyens ou directement par les ressortissants étrangers. Cela résulte de la présence de nombreuses sociétés multinationales ayant choisi d'établir leur siège européen à Luxembourg et pour lesquelles la CNPD est l'autorité compétente pour assurer le respect de la législation nationale en matière de protection des données. 62% des plaintes visent en effet des entreprises offrant des services sur Internet.

21% des plaintes concernent des demandes d'effacement ou

## Evolution du nombre de plaintes




## Motif des plaintes




de rectification de données qui, d'après les plaignants, n'ont pas été respectées.

Dans 20% des cas, les plaignants ont demandé à la CNPD de vérifier la licéité de certaines pratiques administratives ou commerciales. De nombreuses personnes remettent également en cause les conditions générales de certains commerces ou de services en ligne. D'autres n'étaient pas d'accord avec la durée de conservation de certaines données (p.ex. : historique d'achat) ou voulaient savoir s'il est licite pour les entreprises de demander des documents officiels comme la carte d'identité à des fins de vérification d'identité.

La transmission de données à des tiers non autorisés a également fait l'objet de plaintes récurrentes (18%). Cela inclut par exemple les plaintes concernant l'envoi de courriels confidentiels mais distribués de façon collective et visible à tous les destinataires (« CC » au lieu de « BCC »).

La Commission nationale a également dû intervenir lorsque des responsables du traitement ont refusé aux citoyens d'accéder à leurs données, lorsqu'ils ont ignoré leurs requêtes ou lorsqu'ils ne leur ont pas donné assez de renseignements par rapport aux obligations légales à respecter en matière de droit d'information et d'accès (14%). À ce titre, les fermetures, respectivement les suspensions, de comptes clients, notamment par les sociétés de commerce en ligne, font l'objet de plaintes récurrentes. Dans de tels cas, les citoyens demandent l'assistance de la CNPD parce qu'en raison des informations parfois insuffisantes qui leurs sont fournies par lesdites sociétés, ils ne comprennent pas toujours les raisons pour lesquelles le statut de leur compte a changé.

# 2 Les activités en 2014

La CNPD reçoit aussi régulièrement des plaintes relatives au droit d'opposition et celles où les citoyens estiment n'avoir jamais consenti à être prospectés. Elle a dû intervenir à plusieurs reprises dans des cas d'envois de courriels ou de SMS non sollicités ou encore dans des cas où les plaignants ont voulu connaître l'origine des données utilisées par les organisations/ sociétés en vue de les prospecter.

La Commission nationale a par ailleurs reçu les premières demandes de citoyens qui veulent exercer leur « droit à l'oubli » contre le référencement de publications les concernant dans les moteurs de recherche Internet. Les citoyens peuvent en effet s'adresser à la CNPD ou au tribunal s'ils sont convaincus d'avoir une raison légitime pour faire supprimer lesdits liens de référencement, mais que leur demande a été refusée par le moteur de recherche. Il est possible d'introduire de telles demandes depuis que la Cour de justice européenne a rendu, en mai 2014, un arrêt reconnaissant le « droit à l'oubli » selon lequel tout citoyen européen peut demander à ce que ses données à caractère personnel n'apparaissent plus dans les résultats de moteurs de recherche en ligne si celles-ci sont erronées ou plus pertinentes.

Finalement, la Commission nationale a été saisie d'un nouveau genre de plaintes concernant l'accès aux données du registre national des personnes physiques. En effet, il était dans l'intention du législateur d'éviter que des agents publics commettent des abus en consultant des données personnelles, figurant dans des fichiers communaux et le registre national des personnes physiques, pour des finalités autres que celles qui rentrent dans le strict cadre de leurs attributions professionnelles.

C'est dans cette optique que le législateur a reconnu à chaque citoyen un droit d'accès prévu à l'article 38 de la loi du 19 juin 2013 relative à l'identification des personnes physiques. A ce titre, la CNPD relève que la loi modifiée du 2 août 2002 érige en infraction pénale le fait de détourner des données à caractère personnel de leur finalité légitime initiale.

### 2.1.5 Contrôles et investigations

Pour veiller au respect de la législation applicable en matière de protection des données, la Commission nationale dispose de pouvoirs d'investigation au titre desquels elle peut directement accéder aux locaux où a lieu le traitement ainsi qu'aux données faisant l'objet du traitement. Il y a lieu de rappeler qu'en vertu des dispositions de la loi, ce pouvoir d'investigation exclut les locaux d'habitation (voir également : « Caméras filmant les propriétés avoisinantes »).

## Affaire NSA/PRISM : suite à une demande de vérification de licéité concernant Skype et Microsoft au Luxembourg

En juin 2013, une affaire d'espionnage massif des communications électroniques avait été publiée par les journaux Guardian et Washington Post suite aux révélations d'Edward Snowden. Plusieurs entreprises multinationales, parmi lesquelles figurent Google, Yahoo, Facebook, Microsoft, Apple et AOL, avaient été soupçonnées d'avoir volontairement permis à la National Security Agency (NSA) aux Etats-Unis d'accéder à leurs serveurs informatiques à des fins de surveillance d'e-mails, de chats, de photos, vidéos et d'autres données stockées par des millions d'internautes dans le monde.

A la suite de ces révélations concernant le programme de surveillance américain connu sous le nom de « PRISM », la CNPD avait reçu deux demandes de vérification de licéité qui visaient les sociétés Skype Communications S.à r.l. et Microsoft Luxembourg S.à r.l..

À l'issue de son enquête en novembre 2013, la CNPD n'avait pas pu constater de violation des dispositions luxembourgeoises de la législation sur la protection des données à caractère personnel des deux entreprises mises en cause. L'autorité de contrôle luxembourgeoise avait d'ailleurs statué ne disposer d'aucun élément permettant de conclure à un transfert massif et disproportionné de données de la part des deux sociétés basées au Luxembourg à la NSA.

Un des requérants, Monsieur Max Schrems, exploitant du site « Europe vs. Facebook », ne s'était pas contenté des résultats de l'analyse de la CNPD et avait décidé, en mars 2014, d'introduire un recours contre la CNPD devant le tribunal administratif de Luxembourg. En effet, le requérant était persuadé que le transfert des données de la filiale européenne située au Luxembourg vers les Etats-Unis, malgré l'accord dit « Safe Harbor » entre la Commission Européenne et les Etats-Unis qui autorise un tel transfert, violait la législation luxembourgeoise et européenne. En novembre 2014, le requérant s'est toutefois désisté de l'instance, alors que dans le même contexte, quelques mois plus tôt, il avait saisi la « High Court » d'Irlande d'un recours contre l'autorité de protection de données irlandaise, qui avait d'office refusé de traiter sa plainte contre la filiale irlandaise de Facebook introduite pour les raisons identiques qu'au Luxembourg. Suite à ce recours, la High Court d'Irlande a saisi la Cour de justice de l'Union européenne d'une question préjudicielle concernant la validité d'un transfert de données de l'Union Européenne vers une société aux Etats-Unis sur base de l'accord « Safe Harbor ». Cette affaire est toujours pendante devant ladite Cour de justice.

# 2 Les activités en 2014

La Commission nationale n'intervient donc pas seulement lorsque des cas d'atteinte à la législation sur la protection des données lui sont signalés, mais aussi de sa propre initiative, notamment dans un but de prévention. Elle a effectué 22 contrôles et investigations en 2014, que ce soit dans le cadre de la vidéosurveillance, de la surveillance sur le lieu de travail ou encore lorsqu'elle a pris connaissance d'une attaque informatique ou d'une faille de sécurité.

Les quelques cas d'espèce suivants illustrent les investigations opérées par la CNPD.

#### 2.1.5.1 *Lancement d'une procédure d'investigation suite à l'attaque informatique contre la société eBay*

La Commission nationale a décidé d'agir suite au communiqué public de la société eBay en mai 2014 annonçant qu'elle a été victime d'une attaque informatique qui a compromis la base de données de ses clients.

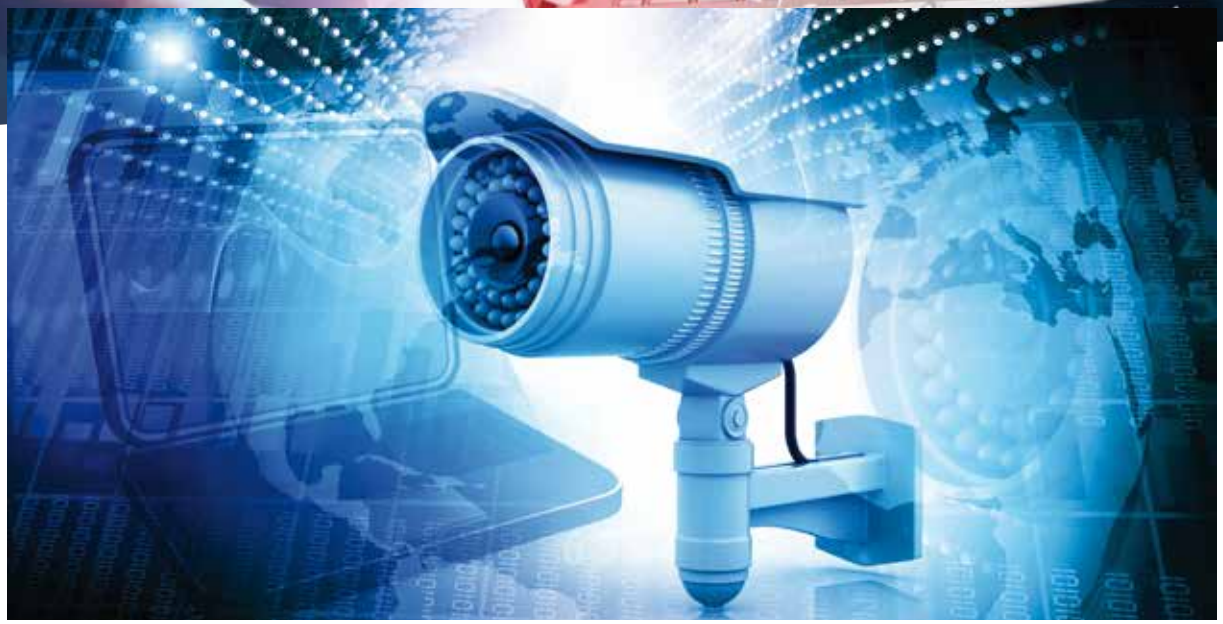
Les utilisateurs qui résident dans l'Union Européenne sont contractuellement liés à la société eBay Europe S.à r.l., établie au Luxembourg. La CNPD a ouvert une procédure d'investigation (qui au moment de la rédaction du présent rapport n'est pas encore clôturée) pour examiner les circonstances et conséquences de la violation de l'intégrité et de la confidentialité des informations personnelles des utilisateurs d'eBay.

#### 2.1.5.2 *Piratage de caméras de surveillance*

En novembre 2014, la presse luxembourgeoise s'est fait l'écho d'un site internet russe sur lequel se trouvaient des liens actifs vers de multiples webcams, moniteurs-bébés et des caméras de surveillance à travers le monde entier. Les images contenaient des salons privés, des chambres d'enfants, des cours intérieures privées, des salles de gymnastique, les intérieurs de magasins, etc. Parmi ces liens se trouvaient, d'après les articles de presse, également des caméras luxembourgeoises.

Après s'être assurée que les systèmes de vidéosurveillance des zones de sécurité opérés par la Police grand-ducale (dites « VISUPOL ») n'avaient pas été attaqués, la CNPD a lancé une investigation portant sur les autres systèmes de surveillance luxembourgeois qui avaient été victimes du piratage. D'après les informations collectées par elle, le site web en question contenait effectivement des liens actifs vers de multiples webcams montrant toutes sortes d'images privées.

Au vu des résultats de son investigation, la CNPD a décidé de dénoncer les faits auprès du



procureur d'Etat, conformément à l'article 32 paragraphe 8 de la loi.

Suite à ce piratage, la CNPD a, en collaboration avec CASES, également publié une fiche pratique[3] informant le grand public des risques et des précautions à prendre en cas d'utilisation de webcams ou d'autres objets connectés.

#### *2.1.5.3 Vidéosurveillance*

**Caméras filmant les propriétés avoisinantes ou la voie publique**

En raison des plaintes que la Commission nationale reçoit chaque année concernant des installations de vidéosurveillance à l'intérieur ou à l'extérieur des maisons d'habitation privées (notamment par des voisins qui s'estiment « observés »), il y a lieu de rappeler que dans le cadre du pouvoir d'investigation lui conféré par la loi modifiée du 2 août 2002, la Commission nationale a un accès direct aux locaux où a lieu le traitement de données et peut procéder aux vérifications nécessaires. Toutefois, la loi ne permet pas d'exercer ce pouvoir d'investigation dans des locaux d'habitation (article 32 paragraphe (7) de la loi modifiée de 2002).

En d'autres termes, la Commission nationale peut procéder à des contrôles sur place dans des lieux d'habitation privés uniquement avec l'accord et sur invitation des personnes qui y sont domiciliées. Comme un tel accord fait défaut dans la plupart des cas, la Commission nationale recommande, de façon générale, de dénoncer ces installations de vidéosurveillance à la police ou au Parquet.

**Vidéosurveillance sans autorisation**

Comme les années précédentes, la Commission nationale a été saisie de plusieurs plaintes concernant des caméras de vidéosurveillance installées sans autorisation, c'est-à-dire en violation des dispositions de la loi modifiée du 2 août 2002.

Dans ces cas, la CNPD a demandé aux entreprises concernées de cesser immédiatement l'utilisation de la vidéosurveillance et leur a rappelé que le non-respect des dispositions de la loi est passible de sanctions pénales.

### 2.1.6 Secteur des communications électroniques

#### *2.1.6.1 Violations de données dans le secteur des communications électroniques*

Conformément au règlement (UE) No. 611/2013 de la Commission européenne du 24 juin 2013 (entré en vigueur le 25 août 2013), les fournisseurs de services de communications électroniques accessibles au public, tels que les entreprises de téléphonie fixe/mobile ou les fournisseurs d'accès à Internet, doivent avertir la CNPD endéans les 24 heures suivant le constat d'une violation de sécurité et de confidentialité des données à caractère personnel et, de surcroît, informer leurs abonnés au cas où l'incident constaté est susceptible d'affecter

[3] http://www.cnpd.public.lu/fr/dossiers-thematiques/nouvelles-tech-communication/webcams-objets-connectes/index.html

défavorablement le niveau de protection de leur vie privée et des données les concernant.

Afin de faciliter la tâche aux fournisseurs de services de communications électroniques, la Commission nationale a élaboré un formulaire de notification d'une violation de sécurité. Celui-ci est disponible sur le site Internet de la CNPD et reprend toutes les questions pertinentes auxquelles les fournisseurs devront répondre dans une telle situation.

En 2014, aucune violation de données dans le secteur des communications électroniques n'a été signalée à la CNPD.

#### *2.1.6.2 Rétention de données de trafic et de localisation*

La directive européenne 2006/24/CE sur la rétention des données a été transposée au niveau national par la loi du 24 juillet 2010 modifiant la loi du 30 mai 2005 sur la protection de la vie privée dans le secteur des communications électroniques. 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. Un des enjeux majeurs de cette directive est 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.

La Commission nationale transmet annuellement à la Commission européenne des statistiques sur la conservation des données au titre des articles 5 et 9. A cet effet, les fournisseurs de services ou opérateurs conservent et continuent 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 pas pu être satisfaites. »*

En 2014, des informations ont été transmises aux autorités compétentes (Police judiciaire et Justice) dans 1.430 cas (contre 1.445 en 2013). Dans 457 cas, les demandes de données n'ont pas pu être satisfaites. Au total, les autorités compétentes ont fait 1.887 demandes auprès des opérateurs. Ce chiffre a diminué par rapport à l'année 2013 où 2.245 demandes avaient été faites.

## Les séances de délibération de la Commission nationale

Le collège se réunit en principe une fois par semaine en séance de délibération. Une partie importante de ces séances est consacrée à l'examen des dossiers de demande d'avis ou d'autorisation. Au cours de 20 séances en 2014, la Commission nationale a adopté 629 délibérations, dont notamment :

- 594 autorisations ;
- 8 avis relatifs à des projets ou propositions de loi et mesures réglementaires ;
- 25 agréments pour des chargés de la protection des données.

## 2.2 Avis et recommandations

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

En 2014, la Commission nationale a émis 8 avis dans le cadre de projets de loi ou de règlements grand-ducaux :

1. Avis à l'égard du projet de loi n°6612 relatif 1) au titre d'artiste, 2) aux mesures sociales au bénéfice des artistes professionnels indépendants et des intermittents du spectacle, 3) à la promotion de la création artistique (Délibération n°69/2014 du 24 mars 2014) ;

2. Avis quant à la conformité de la loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection des personnes à l'égard du traitement des données dans le secteur des communications électroniques et des articles 67-1, 88-2 et 88-4 du Code d'instruction criminelle avec les exigences posées par l'arrêt du 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12 pour 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 (Délibération n°214/2014 du 13 mai 2014) ;

3. Avis complémentaire relatif au projet de loi n°6566 facilitant l'échange transfrontalier d'informations concernant les infractions en matière de sécurité routière (Délibération n°324/2014 du 14 juillet 2014) ;

4. Avis à l'égard du projet de règlement grand-ducal déterminant les modèles de cartes d'identité pour les membres des Corps diplomatique et consulaire résident et les agents de l'Union européenne et des Organisations internationales ayant leur siège au Luxembourg (Délibération n°325/2014 du 14 juillet 2014) ;

5. Avis relatif au projet de loi n°6410 portant modification de la loi du 4 juillet 2008 sur la jeunesse (Délibération n°338/2014 du 21 juillet 2014) ;

6. Avis à l'égard du projet de loi n°6542 portant introduction d'une subvention de loyer et modifiant la loi modifiée du 25 février 1979 concernant l'aide au logement (Délibération n°339/2014 du 21 juillet 2014) ;

7. Avis relatif au projet de loi n°6604 relatif au classement des établissements d'hébergement touristique (Délibération n°352/2014 du 31 juillet 2014) ;

# 2 Les activités en 2014

8. Avis à l'égard du projet de loi n°6675 1) portant organisation du Service de Renseignement de l'Etat; 2) modifiant certaines lois ; 3) abrogeant la loi du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat (Délibération n°353/2014 du 31 juillet 2014).

### 2.2.1 Réforme du statut de l'artiste

Faisant suite à la demande lui adressée par Madame la Ministre de la Culture, la Commission nationale a présenté ses réflexions et commentaires au sujet du projet de loi n°6612 relatif 1) au titre d'artiste, 2) aux mesures sociales au bénéfice des artistes professionnels indépendants et des intermittents du spectacle, 3) à la promotion de la création artistique.

L'objectif principal de ce projet de loi est d'adapter la loi modifiée du 30 juillet 1999 aux réalités vécues par les artistes et intermittents du spectacle. Cette réforme prévoit, entre autres, l'introduction d'un titre d'artiste, l'indemnisation des artistes en cas d'inactivité ou encore la prise en compte des congés de maladie, de maternité et parental.

Selon l'article 15 du projet de loi, il est prévu de donner aux agents du Ministère de la Culture un accès direct à trois fichiers dans un double objectif de contrôle effectif et de réponse rapide aux demandes. Il s'agit du registre général des personnes physiques et morales, du fichier des salariés, des indépendants et des employeurs, géré par le Centre commun de la sécurité sociale et du fichier relatif aux demandeurs d'emploi. Un tel accès laisse toujours courir un risque pour la vie privée des personnes concernées.

Selon la Commission nationale, le nombre d'artistes concernés par le dispositif envisagé demeure très restreint par rapport au nombre de personnes non concernées, mais dont les données seraient consultables par l'administration. Le principe de proportionnalité et de nécessité n'est donc pas respecté au regard des finalités envisagées.

Pour cette raison, la CNPD a proposé la mise en place d'une solution technique qui permettrait de garantir que les agents du ministère de la culture puissent seulement accéder aux données des personnes qui ont introduit une demande. Pour le cas où cette solution ne serait pas techniquement faisable, la Commission nationale a proposé de suivre la position du Conseil d'Etat. Celui-ci a estimé qu' « *il convient d'éviter au maximum les interconnexions entre des bases de données personnelles établies par les administrations étatiques. Ceci pourrait se faire en demandant aux requérants d'aide d'inclure à leurs demandes,*

*des certificats émanant de l'Administration de l'emploi, du Fonds national de solidarité et du Centre commun de la sécurité sociale* ». Cette solution éliminerait en effet les risques potentiels posés par un accès direct aux fichiers et registres d'autres administrations.

### 2.2.2 Rétention des données

Monsieur le Ministre de la Justice a saisi la Commission nationale d'une demande d'examen de la conformité de la législation luxembourgeoise avec les exigences posées par la Cour de Justice de l'Union Européenne dans son arrêt du 8 avril 2014 par lequel elle a invalidé la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données modifiant la directive 2002/58/CE.

L'obligation de conservation des données de trafic et de localisation relatives aux communications électroniques a été introduite dans notre législation par la loi du 30 mai 2005 sur base de l'article 15 § 1er de la directive 2002/58/CE. Après avoir ramené à 6 mois le délai de conservation initialement fixé à 12 mois (loi du 27 juillet 2007), le législateur a transposé la directive 2006/24/CE en modifiant la loi du 30 mai 2005 par les dispositions de la loi du 24 juillet 2010 assorties par ailleurs d'un règlement grand-ducal du même jour qui en a réglé les modalités d'application (déterminant les catégories de données visées).

Les modalités d'accès aux données font l'objet des dispositions des articles 67-1 (loi du 29 juillet 2010) et des articles 88-1 à 88-5 (loi du 30 mai 2005) du Code d'instruction criminelle.

Dans son arrêt du 8 avril 2014, la Cour a retenu la vaste ampleur et le caractère intrusif de l'ingérence dans l'exercice de ces droits fondamentaux que comporte l'obligation faite aux fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communication de conserver les données de trafic et de localisation des utilisateurs par la directive incriminée. La directive a été invalidée compte tenu de la portée de cette ingérence et l'absence de proportionnalité et de règles claires et suffisantes imposant des limites et mesures de sauvegarde. Il convient donc de noter que la CJUE a interdit d'obliger la rétention des données dans les conditions de la directive 2006/24/CE sans pour autant invalider le principe même d'une rétention de données rendue obligatoire par des législations nationales.

Dans son avis, la CNPD a analysé en détail les conditions de validité qui devront être remplies par les lois nationales pour encadrer l'obligation de conservation d'une part, et de celles nécessaires au niveau de l'accès aux données par les autorités d'autre part. La CNPD a recommandé l'élaboration d'un projet de loi visant à amender

les dispositions actuellement en cours sur plusieurs points, parmi lesquels la redéfinition de la condition correspondant à l'objectif de lutte contre la criminalité grave et organisée et le terrorisme par un critère plus approprié de qualification et d'incrimination des faits qui font l'objet de l'enquête. Selon la CNPD, le seuil définissant les incriminations des faits pour lesquels l'article 67-1 du Code d'instruction criminelle (premier alinéa) permet l'accès aux données est déjà apparu en 2010 comme sensiblement trop bas pour correspondre à l'objectif fixé de prévention et poursuite de la criminalité grave et de la lutte contre le terrorisme et la criminalité internationale organisée.

### 2.2.3 Echange transfrontalier d'informations sur les infractions en matière de sécurité routière

La Commission nationale a avisé les amendements de la Commission parlementaire compétente au sujet du projet de loi n°6566 facilitant l'échange transfrontalier d'informations concernant les infractions en matière de sécurité routière.

Son premier avis relatif à ce projet de loi a été adopté en date du 25 juillet 2013. Dans son second avis, elle s'est concentrée sur les questions traitant des aspects portant sur la protection des données, soulevées plus particulièrement par l'amendement 6 portant sur l'article 7 initial (nouvel article 6).

Pour ce qui est de l'exercice du droit d'accès des personnes concernées, la CNPD n'a pas partagé les arguments et explications fournis dans le commentaire de l'amendement 6 pour lequel la solution envisagée est un droit d'accès indirect à exercer par l'intermédiaire de l'autorité de contrôle instituée par l'article 17 (2) de la loi modifiée du 2 août 2002. Elle a maintenu à cet égard ses propositions formulées dans son avis du 25 juillet 2013, à savoir l'organisation d'un accès direct en faveur des personnes concernées qui s'exerce auprès de la Police grand-ducale.

La Commission nationale a également réitéré la proposition formulée dans son avis du 25 juillet 2013, à savoir de *« conférer au droit d'accès un certain automatisme en prévoyant notamment une information automatique à l'adresse des personnes concernées dès que la Police grand-ducale transmet des données à un autre Etat membre. Un tel mécanisme permettrait aux personnes concernées une transparence effective et un meilleur contrôle de leurs données et garantirait qu'un autre Etat membre ne puisse éventuellement abuser du système d'échange de données ».*

### 2.2.4 Cartes diplomatiques, de légitimation et consulaires

La Commission nationale a avisé le projet de règlement grand-ducal déterminant les modèles de cartes d'identité pour les membres des Corps diplomatique et consulaire résidents et les agents de l'Union européenne et des Organisations internationales ayant leur siège au Luxembourg. Elle a limité ses observations aux questions traitant des aspects portant sur la protection des données.

L'un des objectifs principaux du projet de règlement grand-ducal consiste à préciser les données traitées par le Ministère des Affaires étrangères et appelées à figurer sur les cartes diplomatiques, de légitimation et consulaires, ainsi que dans un registre des cartes diplomatiques, de légitimation et consulaires, en application de la loi du 7 août 2012 relative à la carte d'identité pour les membres des Corps diplomatique et consulaire résident et les agents de l'Union européenne et des Organisations internationales ayant leur siège au Luxembourg.

L'article 2A du projet de règlement grand-ducal détermine les catégories de données à caractère personnel contenues sur les cartes, alors que l'article 2B établit un registre des cartes qui contient certaines données présentes sur les cartes ainsi que des données supplémentaires. La Commission nationale s'est demandé s'il n'aurait pas été préférable de définir dans un premier article les finalités du traitement, les catégories des données traitées par le Ministère ainsi que les autres caractéristiques de traitement de données, pour ensuite indiquer dans un second article quelles sont parmi ces données collectées et utilisées celles qui sont appelées à être inscrites sur les cartes. En effet, le fichier (registre) qui sera créé servira de base pour la gestion des demandes de cartes ainsi que la confection des cartes.

La CNPD a ensuite encore fait quelques commentaires et recommandations :

- Il pourrait être utile de détailler un peu plus le type d'informations collectées.

- Une autre disposition pourrait spécifier parmi les données contenues dans le fichier (registre) celles qui figurent sur les cartes.

- Pour des raisons de cohérence de terminologie avec la loi du 2 août 2002, il est suggéré de parler de « fichier » plutôt que de « registre » des cartes.

- Concernant la durée de conservation des données à caractère personnel traitées par le Ministère, la CNPD note avec satisfaction que le paragraphe (3) de l'article 2A du projet de règlement grand-ducal précise que les données biométriques ne sont conservées que pendant une durée de deux mois après la délivrance d'une carte diplomatique, de légitimation ou consulaire et sont, à l'expiration de ce délai, automatiquement et irréversiblement supprimées.

- Il pourrait être utile d'indiquer les durées de conservation des données à caractère personnel autres que biométriques.

- Il est également nécessaire de prévoir un système de journalisation des accès, ce qui constitue une garantie appropriée contre les risques d'abus.

### 2.2.5 Jeunesse

La Commission nationale a avisé le projet de loi n°6410 portant modification de la loi modifiée du 4 juillet 2008 sur la jeunesse.

Elle a limité ses observations aux questions traitant des aspects portant sur la protection des données, soulevées plus particulièrement par l'article 29 du texte coordonné (comprenant les amendements gouvernementaux) du projet de loi. Cet article a pour objet la création et l'exploitation d'un fichier de données à caractère

# Les activités en 2014

personnel relatif à la gestion des demandes et du contrôle des paiements des chèques-service accueil.

La Commission nationale a préconisé que le texte précise l'origine des différentes catégories de données. Dans l'hypothèse où les données seraient transmises par d'autres administrations, en l'occurrence via un accès aux fichiers de ces administrations par le ministère de la Famille et de l'Intégration, la Commission nationale a estimé nécessaire que soit prévue la mise en place d'une solution technique permettant de garantir, d'un point de vue informatique, que les agents du ministère puissent seulement accéder aux données concernant les personnes qui ont introduit une demande de chèques-service accueil, à l'exclusion des données relatives au reste de la population.

La CNPD s'est également posé la question de la nécessité pour le ministère de connaître la présence réelle de l'enfant bénéficiaire dans la structure. Il lui a semblé que cette information permette, le cas échéant, de constater d'éventuels abus. Si tel est le cas, il serait utile de le préciser selon la CNPD, afin de pouvoir apprécier la nécessité et le caractère adéquat de cette information.

Quant aux catégories de données relatives aux prestataires, la CNPD s'est demandé quel est le lien de la collecte de ces données avec la finalité invoquée au paragraphe (1) de l'article 29, à savoir la gestion des demandes introduites dans le cadre du chèque-service accueil et du contrôle des paiements. En ce sens, il y aurait lieu de rajouter une finalité supplémentaire au paragraphe (1), du type « gestion des prestataires des services d'accueil ». En tout état de cause, la Commission nationale a estimé que la photo du personnel encadrant ne peut pas être collectée.

La CNPD ne voit par ailleurs pas en quoi la publication de certaines catégories de données dans un portail édité par le ministère s'avère nécessaire aux fins de la gestion administrative et du suivi des dossiers de demandes des chèques-service accueil, respectivement de la gestion des prestataires des services accueil.

Concernant l'accès aux données, la Commission nationale s'est demandé pour quelle raison des tiers non autorisés pourraient recevoir communication des données, à moins que les auteurs du projet de loi précisent les finalités et les catégories de données pour lesquels une communication de données serait nécessaire. Pour ce qui est de l'accès aux données par les agents du Ministère de la Famille et de l'Intégration, la Commission nationale a recommandé de

préciser davantage les modalités d'accès aux données présentes dans le fichier.

Finalement, la CNPD a estimé nécessaire de prévoir un système de journalisation des accès, ce qui constitue une garantie appropriée contre les risques d'abus. En ce qui concerne la durée de conservation, la CNPD a estimé que celle-ci paraissait excessivement longue par rapport aux finalités des traitements de données concernées.

### 2.2.6 Subvention de loyer

La Commission nationale a avisé le projet de loi n°6542 portant introduction d'une subvention de loyer et modifiant la loi modifiée du 25 février 1979 concernant l'aide au logement.

L'objectif principal du projet de loi est l'introduction d'une subvention de loyer en faveur de ménages à faible revenu, afin de leur faciliter l'accessibilité à un logement du marché locatif privé ainsi que d'améliorer leurs conditions de logement. L'article 14*sexies* prévoit un accès des agents du ministère du Logement à certains fichiers d'autres administrations dans le cadre de demandes de subvention de loyer. Il prévoit également de manière implicite la création d'un fichier en vue de la gestion et du suivi administratif des dossiers des demandeurs d'une subvention de loyer.

La Commission nationale a estimé que le principe de la tenue d'un tel fichier devrait aussi être précisé dans le texte du projet de loi, tandis que les modalités et conditions d'utilisation (catégories de données traitées, leur utilisation et leur obtention, etc.) pourraient être fixées dans un règlement grand-ducal.

L'article 14*sexies* du projet de loi permet l'accès par le ou les gestionnaires du dossier du ministère du Logement aux fichiers issus du Centre commun de la sécurité sociale, de l'Administration des contributions directes et du Fonds national de sécurité, dont les missions publiques ne présentent a priori pas de lien direct avec celles du ministère du Logement.

La Commission nationale a compris que cet accès du ministère du Logement aux fichiers ou registres d'autres administrations pourrait permettre d'atteindre la finalité envisagée, à savoir l'objectif de simplification administrative et de gain de temps pour la population cible et pour les services d'aide au logement. Cependant, elle a estimé que le principe de proportionnalité et de nécessité n'était pas respecté au regard de la finalité envisagée. En effet, cet article permettrait un accès aux données contenues dans des fichiers concernant une partie très importante de la population alors que le nombre de personnes concernées par le dispositif envisagé demeure relativement restreint.

La CNPD a ainsi proposé la mise en place d'une solution technique qui permettrait de garantir, d'un point de vue informatique, que le ou les gestionnaires du dossier du ministère du Logement puissent seulement accéder aux données concernant les personnes qui ont introduit une demande au titre de l'article 14quinquies du projet de loi sous objet, à l'exclusion des données relatives au reste de la population.

Dans le cas où cette solution n'apparaîtrait pas techniquement envisageable ou nécessiterait des moyens déraisonnables pour pouvoir être mise en œuvre, la Commission nationale a proposé de suivre la position du Conseil d'Etat. Celui-ci a estimé que « *ces informations pourront être fournies par les ménages eux-mêmes, nul besoin n'existant pour instaurer un droit d'accès aux fichiers de diverses administrations au profit du service du ministère du Logement. (…) Si les auteurs entendent éviter des abus ou le risque de ne pas se voir remettre les renseignements demandés, il serait plus facile de demander aux personnes concernées de fournir les réponses dans un certain délai et de les informer que, faute d'obtention de ces renseignements, le versement de l'aide sera arrêtée jusqu'à obtention des renseignements utiles* ». Cette solution éliminerait

en effet les risques potentiels posés par un accès aux fichiers d'autres administrations.

Finalement, la CNPD a estimé également nécessaire de prévoir un système de journalisation des accès, ce qui constitue une garantie appropriée contre les risques d'abus.

### 2.2.7 Classement des établissements d'hébergement touristique

La Commission nationale s'est prononcée au sujet des avant-projets (entretemps devenus projets) de loi et de règlement grand-ducal relatifs au classement des établissements d'hébergement touristique.

Leur objectif consiste à définir les différents types d'établissements d'hébergement touristique, à établir un système de classification ainsi qu'à détailler les modalités de classement, voire de sanction de ces établissements. A ces fins, le ministère des Classes Moyennes et du Tourisme tient un registre des établissements d'hébergement touristique. La tenue de ce registre ainsi que les possibilités pour le ministère de recourir à certaines catégories de données font l'objet d'un chapitre dédié du projet de loi (« Chapitre 3 – Traitement de données nominatives »), qui comporte un article 13. La Commission nationale a limité ses observations aux questions traitant des aspects portant sur la protection des données, soulevées plus particulièrement par ledit article 13.

La Commission nationale a suggéré d'aligner la terminologie utilisée dans le cadre de l'article 13 du projet de loi sur les termes définis dans la loi du 2 août 2002. Dans cette optique, « traitement des données nominatives » deviendrait « traitement de données à caractère personnel », et « registre » deviendrait « fichier » ou « fichier de données à caractère personnel ».

La CNPD s'est aussi demandé s'il ne serait pas également préférable, pour des raisons de cohérence avec la loi du 2 août 2002, d'indiquer qu'un traitement de données à caractère personnel est mis en œuvre et d'en définir le responsable du traitement (le ministre), les finalités (qui sont déjà reprises dans la version actuelle de l'article 13), les catégories de données à caractère personnel traitées ainsi que l'origine de ces dernières (qu'il y aurait lieu de préciser).

La Commission nationale a par ailleurs estimé nécessaire

- de préciser dans le texte les catégories de données collectées et utilisées ;

- d'indiquer l'origine des données à caractère personnel traitées par le ministre et

- de prévoir une disposition réglant la durée de conservation des données à caractère personnel.

### 2.2.8 Organisation du Service de Renseignement de l'Etat

La Commission nationale a avisé le projet de loi n°6675 1) portant organisation du Service de Renseignement de l'Etat ; 2) modifiant certaines lois et 3) abrogeant la loi du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat. Elle a limité ses observations aux questions traitant des aspects portant sur la protection des données et plus particulièrement aux articles 3, 4 et 5 du projet de loi.

La CNPD a noté qu'il est important de décrire les missions du SRE. Plus les missions sont formulées de manière précise, plus le cercle des personnes susceptibles d'être concernées par les traitements de données effectués par le service de renseignement sera restreint. D'un autre côté, au regard de l'évolution des menaces que le SRE doit tenter d'anticiper et prévenir, une telle description ne peut pas être trop détaillée non plus. Dès lors, le bon fonctionnement des mécanismes de contrôle tels que prévus par le projet de loi joue un rôle d'autant plus crucial afin d'éviter des abus tels que constatés dans le passé récent.

La communication d'informations à caractère personnel entre le SRE et d'autres autorités et institutions ne peut avoir lieu qu'à condition que le principe de proportionnalité soit respecté.

En ce qui concerne l'échange de données avec des autorités et services de renseignements étrangers ainsi que l'applicabilité du droit communautaire, la CNPD s'est référée aux explications données par le groupe de travail « Article 29 » dans son avis 04/2014 sur la surveillance des communications électroniques à des fins de renseignement et de sécurité nationale.

L'article 5 paragraphe (1) alinéa 2 prévoit que les conditions et modalités du traitement des données à caractère personnel du SRE doivent être précisées dans un règlement grand-ducal. La CNPD a estimé que l'adoption de ce texte réglementaire est d'une importance cruciale d'un point de vue protection des données et sécurité juridique. Dès lors, il aurait été judicieux de joindre en même temps un projet de règlement grand-ducal au projet de loi sous examen, d'autant plus qu'un tel règlement grand-ducal n'a jamais vu le jour sous l'empire de la loi actuelle du 15 juin 2004.

La CNPD a noté avec satisfaction que l'on s'est inspiré de l'article 48-24 du Code d'Instruction criminelle en ce qui concerne la traçabilité des accès prévue par le paragraphe (3) de l'article 5 du projet. Toutefois, elle a considéré que la loi devrait également prévoir que le système informatique par lequel l'accès direct est opéré doit être aménagé de sorte que le motif de la consultation puisse être retracé, c'est-à-dire documenté dans le système informatique, à l'instar de ce qui est prévu pour les procureurs, les membres des parquets et les membres du personnel de l'administration judiciaire par l'article 48-24 paragraphe (4) lettre (b) du Code d'Instruction criminelle et pour les officiers et agents de police judiciaire par l'article 34-1 de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la police.

## 2.3 Information du public

L'information des citoyens comme des responsables du traitement est une priorité de la Commission nationale, afin de faire connaître les droits et devoirs respectifs de chacun. Elle mène des actions de sensibilisation du public, informe le grand public à travers son site Internet et participe à des formations et conférences.

### 2.3.1 Actions de sensibilisation du public

À l'occasion de la journée de la protection des données, la CNPD et le Centre Interdisciplinaire

# Les activités en 2014

pour la Sécurité, la Fiabilité et la Confiance (SnT) de l'Université du Luxembourg ont organisé une table ronde intitulée « Les défis en matière de protection de la vie privée dans un monde interconnecté »[4]. Le 28 janvier est la date de la célébration de la Journée de la protection des données, organisée annuellement depuis 2007 par le Conseil de l'Europe avec le soutien de la Commission européenne. L'objectif de cette journée est de sensibiliser les citoyens au sujet de leurs droits et devoirs dans le contexte de la protection de la vie privée et de la protection des données.

Cette date correspond à l'anniversaire de la signature le 28 janvier 1981 de la « Convention 108 » du Conseil de l'Europe, qui a été le premier instrument international juridiquement contraignant en la matière. Depuis plus de 30 ans, la loi vise à protéger tout citoyen contre l'utilisation abusive des données le concernant et à assurer la transparence quant à l'utilisation des fichiers et des traitements effectués à partir de ses données personnelles.

La CNPD a également participé au Safer Internet Day, qui a été célébré dans le monde entier sous le slogan « Tous ensemble pour un Internet meilleur » (« Let's create a better Internet together »). Cette journée, qui est une initiative de la Commission européenne, est organisée par Insafe chaque année au mois de février pour promouvoir une utilisation plus sûre et responsable des nouveaux médias. Au Luxembourg, BEE SECURE s'occupe de la coordination de cet événement.

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

La Commission nationale est intervenue régulièrement dans les médias pour commenter les sujets ayant trait à la protection des données et à la protection de la vie privée.

En 2014, le collège a accordé plus de 30 interviews aux organes de presse. Parmi les thèmes traités, citons : le dossier de soins partagé, la surveillance sur le lieu de travail, la rétention des données, l'arrêt de la Cour de justice européenne sur le droit à l'oubli, la faille de sécurité d'eBay, Google Street View, drones, etc.

### 2.3.3 Outil de communication : le site Internet

Le site web de la Commission nationale est destiné à la fois aux responsables du traitement et au grand public.

Les responsables du traitement peuvent y accomplir les formalités prescrites par la loi. Afin de les guider de la manière la plus claire possible, la Commission

[4] Voir partie 3.3 pour plus d'informations à ce sujet.


nationale y met à disposition des rubriques et formulaires dédiés (ex : formulaire de demandes d'autorisation en matière de vidéosurveillance et de transferts de données vers des pays tiers, engagements formels de conformité, formulaires de notification, demande d'agrément pour les chargés de la protection des données, etc.).

Quant au grand public, il peut s'informer sur les sujets qui ont dominé l'actualité dans le domaine de la protection des données et de la vie privée. Le site offre aussi une information de base sur la protection des données et sur les droits et obligations respectifs. Les internautes intéressés peuvent élargir leurs connaissances par la consultation de dossiers thématiques.

Le site permet également de consulter le registre public des traitements et enfin de contacter la Commission nationale pour toute question, demande de renseignement complémentaire ou pour déposer une plainte.

### 2.3.4 Formations et conférences

À côté de l'information du grand public, la Commission nationale participe aussi régulièrement à des formations, conférences et séminaires pour sensibiliser des publics plus spécialisés aux enjeux de la protection des données.

Le 22 janvier, la CNPD a participé à une matinée d'échange sur « La qualité au service des patients », organisée par Deloitte en collaboration avec la Fédération des Hôpitaux luxembourgeois. Le président de la CNPD est intervenu lors de la table ronde intitulée « La dématérialisation du suivi patient : le dossier électronique ». Cette conférence était structurée autour des principaux résultats de la seconde enquête lancée par Deloitte, qui portait notamment sur l'apport des nouvelles technologies dans le parcours de soins du patient et les évolutions comportementales en matière de prévention.

Le 27 janvier, à la veille de la journée européenne de la protection des données, M. Gérard Lommel a participé à la table ronde intitulée « Les défis en matière de protection de la vie privée dans un monde interconnecté », organisée par la CNPD et le Centre Interdisciplinaire pour la Sécurité, la Fiabilité et la Confiance (SnT) de l'Université du Luxembourg[5].

Le 30 janvier, le Bureau d'Information du Parlement européen au Luxembourg a organisé une conférence intitulée « La protection des données des citoyens de l'UE à l'ère numérique ». M. Frank Engel (député européen luxembourgeois), M. Ammar Alkassar (expert en sécurité et cryptographie) et M. Gérard Lommel ont discuté la réforme des règles de la protection des données au niveau européen à l'occasion de la Journée de la protection des données. La présentation de M. Lommel a porté sur la conciliation de la protection des données avec le développement de l'économie numérique.

[5] Voir partie 3.3 pour plus d'informations.

# 2 Les activités en 2014

Le 28 février, le président de la CNPD était l'invité de la Conférence du Jeune Barreau de Luxembourg à l'auditoire de la banque BGL pour parler de la surveillance sur le lieu de travail.

Le 11 mars, le président de la CNPD est intervenu lors de la conférence inaugurale de l'Association pour la protection des données au Luxembourg (APDL). « La création de l'APDL constitue un saut qualitatif important dans le domaine de la protection des données », a estimé le président dans son discours d'introduction. Il s'est réjoui de « l'enthousiasme suscité par la nouvelle association » dont plus de 130 membres ont assisté à la conférence inaugurale et a constaté que « la protection des données est considérée comme un atout et non comme une contrainte ».

Le 21 mars, le président de la CNPD a donné une présentation sur la conciliation de la protection des données avec la vocation des archives lors de la 4e journée des archivistes luxembourgeois. Le thème principal de la journée était « Les archives et la protection des données personnelles. Les clivages entre législation, recherche et travail archivistique ». Des représentants du Parquet général du Luxembourg, de nombreuses institutions d'archives luxembourgeoises et étrangères, ainsi qu'un grand nombre de chercheurs et d'historiens se sont rencontrés au Cercle Cité à Luxembourg-Ville. Ils y ont discuté du cadre légal et juridique en matière de protection de données, son implication sur le travail d'historien ainsi que

la manière dont les archivistes concilient la protection des données avec le libre accès aux informations. Au terme de leurs débats, les participants ont pu conclure que la recherche et la protection des données peuvent être conciliées. Les archivistes sont des partenaires aussi bien des autorités chargées de la protection des données que de la communauté des chercheurs. Ils veillent à ce que la vie des individus soit protégée tout en étant les garants d'un accès libre aux informations. Le compromis entre la vocation des archives et la protection des données doit néanmoins être sanctionné par un texte légal harmonisant les lois existantes.

Le 16 mai, M. Gérard Lommel a participé à une discussion sur l'arrêt « Google » de la Cour de justice de l'Union européenne et de ses conséquences. La Cour a estimé que certains utilisateurs ont le droit de demander aux moteurs de recherche tels que Google de supprimer les résultats de recherche qui incluent des données à caractère personnel. Cette discussion, à laquelle a également participé M. Jan Guth du Chaos Computer Club, a eu lieu dans le cadre de l'événement « Youth on the Move » de la représentation de la Commission européenne du Luxembourg.

Le 18 juin, le président de la CNPD a participé à une table ronde avec Me Cyril Pierre-Beausse sur « Les changements induits par la modernisation du cadre juridique européen dans la protection des données », organisée par l'Association Luxembourgeoise des Compliance Officers du Secteur Financier (ALCO).

Les 18 et 19 juin, M. Alain Herrmann du service informatique et nouvelles technologies est intervenu dans une table ronde sur les « Privacy Impact Assessments » lors des Rencontres de la Sécurité au Casino 2000 à Mondorf-les-Bains. Placés sous la thématique de l' « intrusion informatique - Mythe ou Réalité », ces deux jours étaient dédiés aux workshops puis aux tables rondes, conférences et échanges avec une vingtaine de sponsors présents.

Les 19 et 20 septembre s'est tenu dans la grande salle d'audience de la Cour de Justice de l'Union européenne un séminaire sur la protection des données, organisé par la Commission Vie privée et Droits de l'homme numérique de l'Union Internationale des Avocats (UIA). Le séminaire a eu lieu sous le Haut Patronage de M. Xavier Bettel, Premier Ministre du Luxembourg et de M. Vassilios Skouris, Président de la Cour de Justice de l'Union Européenne. M. Gérard Lommel, en sa qualité de vice-président du groupe de travail de l'Article 29, et M. Paul Nemitz de la Commission européenne, ont introduit le séminaire. Dans sa présentation, M. Lommel, a expliqué les points clés du nouveau principe d' « accountability » pour les entreprises dans le projet de règlement européen sur la protection des données.

Le 28 novembre, M. Alain Herrmann a participé à une conférence organisée par la Fédération des prestataires de soins COPAS, intitulée « Dossier de Soins informatisé et Dossier de Soins Partagé ». Sa présentation a porté sur les précautions et obligations en matière de protection des données dans le domaine de la santé.

Outre ces différentes participations, les membres de la Commission nationale ont donné des cours de formation à l'Institut National d'Administration Publique (INAP) les 24 et 25 juin.

## 2.4 Conseil et guidance

### 2.4.1 Concertation avec les organisations représentatives sectorielles, les principaux acteurs économiques, l'État et les organismes publics

La sensibilité croissante du public à l'égard des questions de protection des données implique des efforts accrus de l'équipe de la CNPD, qui doit fournir une guidance appropriée aux acteurs tant du secteur public

# 2 Les activités en 2014

que du secteur privé. Ceux-ci se tournent vers elle pour vérifier la conformité de leurs pratiques ou projets à l'égard des dispositions légales applicables.

En 2014, la Commission nationale a participé à plus de 92 réunions avec les acteurs du secteur public et à 77 réunions avec ceux du secteur privé. Elle était, entre autres, en relation avec les ministères, administrations et organes publics suivants :

- Ministère de la Fonction publique et de la Réforme administrative : échange de données CNPF en matière d'allocations familiales et d'aide pour études supérieures pour les besoins du service chargé des subventions d'intérêts ; Commission du registre national ;
- Ministère de la Justice: réforme du régime des publications en matière de droit des sociétés ; protection des données judiciaires et policières, transposition de la décision-cadre 2008/977 ; réunion GAFI (Groupe d'action financière) ;
- Service des Communications et des Médias : réforme du cadre européen sur la protection des données ;
- Ministère de la Justice : rétention des données, réforme du casier judiciaire, fichier prostitution ;
- Ministère des Finances : FATCA (« Foreign Account Tax Compliance Act ») ;
- Ministère des Affaires étrangères : règlement européen relatif aux frontières intelligentes, projet de coopération au développement luxembourgeois ;
- Ministère de la Fonction publique et de la Réforme administrative : échange de données CNPF en matière d'allocations familiales et d'aide pour études supérieures pour les besoins du service chargé des subventions d'intérêts ; Commission du registre national ;
- SMILE (« Security Made in Luxembourg ») du Ministère de l'Economie: Smart Metering, outil de « Data Protection Impact Assessment » ;
- Archives nationales de Luxembourg: avant-projet de loi sur l'archivage électronique.

Parmi les entreprises multinationales implantées au Luxembourg, la Commission nationale a notamment rencontré eBay/Paypal, Amazon et Microsoft.

La Commission nationale est aussi intervenue périodiquement dans les travaux de la Commission Consultative des Droits de l'Homme (CCDH), de la Commission du registre

national des personnes physiques (dont elle est membre depuis juin 2013) et du Comité des statistiques publiques. Depuis 2013, un membre de la Commission nationale fait partie du Comité des statistiques publiques en tant qu'observateur. Ce Comité a été institué auprès du Ministère de l'Economie et du Commerce extérieur par la loi modifiée du 10 juillet 2011 portant organisation de l'Institut national de la statistique et des études économiques.

Dans le domaine de la recherche, elle était en lien avec le Comité National d'Ethique et de Recherche (CNER), le CEPS INSTEAD (Enquête SHARE sur la santé, le vieillissement et la retraite) ou encore avec le Réseau d'étude sur le marché du travail et de l'emploi (RETEL), qui a consulté la CNPD dans le cadre d'un projet de création d'un data warehouse, dont l'objectif est de mieux connaître le marché de l'emploi.

Dans le domaine de la santé, la Commission nationale continue à participer activement aux travaux de l'agence « e-santé », notamment en ce qui concerne la mise en œuvre du dossier de soins partagés (DSP). Elle a par ailleurs poursuivi sa coopération avec la Fédération des Hôpitaux Luxembourgeois pour promouvoir les bonnes pratiques en matière de protection des données au niveau du fonctionnement quotidien des hôpitaux.

### 2.4.2 Demandes de renseignements

La Commission nationale a reçu un nombre record de 2.192 demandes de renseignement en 2014. Dans la majorité des cas, il s'agissait de questions juridiques relatives à la législation ou de requêtes relatives aux formalités à accomplir pour mettre en œuvre un traitement de données.

Elle a répondu à 1.776 demandes par téléphone et à 416 par écrit. Plus que la moitié des demandes émanaient d'entreprises. Les autres provenaient d'administrations publiques, d'avocats et de citoyens qui s'adressent aussi régulièrement à la Commission nationale.

## 2.5 Recherche

En 2011, la Commission nationale et le Centre Interdisciplinaire pour la Sécurité, la Fiabilité et la Confiance (SnT) de l'Université du Luxembourg ont lancé un programme commun de recherche intitulé « *Legal issues in Data protection, Cloud Computing and Privacy* ».

La coopération se base sur trois principaux domaines d'analyse :

- les nouveaux développements de la législation européenne en matière de protection des données ;
- les défis technologiques tels que le cloud computing et leurs répercussions pour les acteurs publics et privés du site luxembourgeois ;
- le concept de « privacy by design », qui garantit que la protection de la vie privée est intégrée dans les nouvelles pratiques technologiques et commerciales dès leur conception, au lieu de les ajouter ultérieurement sous forme de compléments.

Le programme de recherche commun répond à des questions fondamentales de la protection des données dans un environnement technologique moderne. Les résultats contribueront à sensibiliser le public et aideront à définir des solutions « made in Luxembourg » qui pourront servir d'exemples pour faire face aux nouveaux défis dans ce domaine dès le début.

## 2.6 Travail au niveau international

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

# Les activités en 2014

sa complexité. La Commission nationale, représentée par un ou plusieurs de ses membres, a participé en 2014 à 40 réunions et à différents groupes de travail au niveau européen.

Il s'agit notamment :

- du groupe de travail « Article 29 » (établi en vertu de l'article 29 de la directive 95/46/CE), qui regroupe toutes les autorités européennes ainsi que le Contrôleur européen à la protection des données (CEPD). Dans ce cadre, la Commission nationale a participé aux sous-groupes suivants :
  - « Technologies » ;
  - « International Transfers » ;
  - « Future of Privacy » ;
- du Comité consultatif de la Convention 108 du Conseil de l'Europe (T-PD) ;
- du « Groupe de Berlin », dédié à la protection des données dans le secteur des communications électroniques ;
- du séminaire européen d'échanges d'expériences dans le traitement des cas pratiques (« Case Handling Workshop ») ;
- du Working Party on Information Exchange and Data Protection (DAPIX) – (Groupe de travail au niveau du Conseil de l'Union européenne) ;
- de la conférence de printemps des commissaires européens à la protection des données ;
- de la conférence internationale des commissaires à la protection des données et de la vie privée à l'île Maurice ;
- de la réunion annuelle du Global Privacy Enforcement Network (GPEN).

Par ailleurs, les membres de l'autorité de contrôle de l'article 17 (comprenant deux membres de la CNPD) ont participé en alternance aux réunions des autorités conjointes de contrôle européennes d'Europol, du système d'information « Schengen », du système d'information européen des autorités douanières (CIS), du système d'information européen des visas (VIS) ainsi que du système d'information européen Eurodac.

### 2.6.1 Le groupe « Article 29 »

Le groupe de travail, institué par l'article 29 de la directive 95/46/CE sur la protection des données (ci-après le groupe « Article 29 » ou « G29 »), est un organe consultatif indépendant. L'objectif de cet organisme, réunissant l'ensemble des autorités nationales de protection des données à l'échelle européenne, est d'examiner les questions relatives à la protection des données et


de promouvoir une application harmonisée de la directive dans les 28 États membres de l'Union européenne.

Parmi les sujets traités par le groupe de travail en 2014, citons :

- la révision du cadre légal européen de la protection des données ;
- l'arrêt de la Cour de Justice de l'UE reconnaissant un droit à l'oubli (arrêt « Costeja ») ;
- la rétention des données ;
- le « Big Data » ;
- le cloud computing ;
- les règles d'entreprises contraignantes pour les sous-traitants ;
- les conditions d'utilisation de Google et de Microsoft ;
- l'accord « Safe Harbor ».

Pour les années 2014 et 2015, le groupe de travail a indiqué que ses priorités seraient :

- de préparer le nouveau cadre légal en matière de protection des données ;
- de relever le défi de la globalisation ;
- de répondre aux défis technologiques ;
- d'assurer une coopération en matière d'application de la loi.

Lors de la 94e réunion du 26 et 27 février 2014, Isabelle Falque-Pierrotin de l'autorité française CNIL a été nommée présidente et succède à Jacob Kohnstamm de l'autorité néerlandaise, qui a présidé le G29 pendant quatre ans.

La plénière du G29 a aussi élu deux nouveaux vice-présidents : Gérard Lommel de la CNPD et Wojciech Rafal Wiewiórowski de l'autorité polonaise. Ils ont remplacé Christopher Graham (Royaume-Uni) et Igor Nemec (République tchèque).

La durée du mandat du président et des vice-présidents est de deux ans renouvelables.

Les principaux documents de travail de 2014 du groupe sont résumés ci-dessous et peuvent être téléchargés sur Internet[6].

#### *2.6.1.1 Notification des violations de données à caractère personnel*

Le 25 mars 2014, le groupe de travail a adopté un avis dans lequel il fournit des orientations aux responsables du traitement afin de les aider à décider s'il convient de notifier aux personnes concernées les éventuelles « violations de données à caractère personnel ».

[6] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/

# Les activités en 2014

Bien que cet avis porte sur l'obligation actuellement imposée aux fournisseurs de communications électroniques au titre de la directive 2009/136/CE modifiant la directive 2002/58/CE (transposée au Luxembourg par la loi du 28 juillet 2011 modifiant la loi du 30 mai 2005), il contient des exemples issus de nombreux secteurs et présente une série de bonnes pratiques à l'intention de tous les responsables du traitement.

La directive 2009/136/CE exige qu'une notification soit adressée à l'autorité compétente pour tous les cas de violation de données. Toutefois, le présent avis analyse les violations de données à caractère personnel qui nécessitent une notification aux personnes concernées. Le groupe de l'Article 29 décrit ce que les responsables du traitement devraient faire lors de la mise en œuvre de leur système afin d'éviter la violation de données à caractère personnel en premier lieu, voire les mesures qui doivent être prises au départ pour que le responsable du traitement ne soit pas tenu de notifier les personnes concernées.

L'avis répond également à certaines questions essentielles relatives aux violations de données à caractère personnel et à l'application de la directive 2009/136/CE.

#### *2.6.1.2 Surveillance des communications électroniques par les services de renseignement*

Suite aux révélations concernant des programmes de surveillance comme PRISM, le groupe de l'Article 29 a publié, le 10 avril 2014, un avis dans lequel il réclame davantage de transparence des Etats et appelle à un contrôle renforcé des activités des services de renseignement.

Les autorités de protection des données européennes ont souligné l'illégalité de la surveillance massive, systématique et sans distinction des citoyens européens par les services de renseignement. Selon le groupe, une telle surveillance ne peut être justifiée par la seule lutte contre le terrorisme ou d'autres considérations de sécurité publique.

Dans son avis, le groupe de travail a notamment recommandé que :

- les citoyens doivent être informés et bénéficier de garanties adéquates de protection de leurs données lorsque celles-ci sont collectées et transférées ;
- la nécessité d'instaurer un contrôle effectif et indépendant des services de renseignement dans lequel les autorités de protection des données jouent un rôle ;

- la finalisation des négociations sur la réforme de la protection des données par les institutions de l'UE ;

- l'adoption d'un traité international contraignant afin de donner aux citoyens des garanties fortes en matière d'activités des services de renseignement.

#### 2.6.1.3 *Techniques d'anonymisation*

Dans son avis sur les techniques d'anonymisation du 10 avril 2014, le groupe de travail a d'abord évalué l'effectivité en matière de protection des données des techniques existantes. Ensuite, il a donné des recommandations aux responsables du traitement pour l'utilisation de ces techniques en tenant compte du risque résiduel d'identification inhérent à chacune d'elles.

De nombreux acteurs, en particulier dans le domaine de la recherche, utilisent des techniques d'anonymisation afin de valoriser les données qu'ils détiennent. Le G29 a clarifié dans son avis qu'un processus d'anonymisation est un traitement ultérieur au sens de la directive 95/46/CE et que les données pseudonymisées ne peuvent être considérées comme anonymes. La pseudonymisation n'est qu'une mesure de sécurité permettant de réduire la probabilité de trouver un lien entre un ensemble de données et l'identité d'une personne.

Les principales techniques d'anonymisation, à savoir la randomisation et la généralisation, sont décrites dans l'avis. Il y est notamment question d'ajout de bruit, de permutation, de confidentialité différentielle, d'agrégation, de k-anonymat, de l-diversité et de t-proximité. Les principes, les points forts et les points faibles de ces techniques sont expliqués, de même que les erreurs courantes et les échecs qui se rapportent à l'utilisation de chaque technique.

Selon cet avis, les techniques d'anonymisation peuvent apporter des garanties en matière de respect de la vie privée et peuvent servir à créer des procédés d'anonymisation efficaces, mais uniquement si leur application est correctement conçue – ce qui suppose que les conditions préalables (le contexte et les objectifs) du processus d'anonymisation soient clairement définis de façon à parvenir à l'anonymisation visée, tout en produisant des données utiles. Le choix de la solution optimale devrait s'opérer au cas par cas, en utilisant éventuellement une combinaison de techniques différentes, sans perdre de vue les recommandations pratiques formulées dans cet avis.

Enfin, les responsables du traitement des données devraient être conscients qu'un ensemble de données anonymisées peut encore présenter des risques résiduels pour les personnes concernées. En effet, d'une part, l'anonymisation et la ré-identification sont des domaines de recherche très actifs où de nouvelles découvertes sont régulièrement publiées et, d'autre part, même des données anonymisées, comme les statistiques, peuvent servir à étoffer des profils existants, créant ainsi de nouveaux problèmes en termes de protection des données. C'est pourquoi l'anonymisation ne doit pas être considérée comme un exercice ponctuel: il appartient aux responsables du traitement des données de réévaluer régulièrement les risques associés.

#### 2.6.1.4 *Rétention des données*

La directive européenne 2006/24/CE du 15 mars 2006 sur la conservation des données a été invalidée par la Cour de justice de l'Union européenne, qui l'a déclarée disproportionnée et trop intrusive.

Dans leur déclaration commune du 1er août 2014, les autorités de protection des données européennes, réunies dans le groupe de l'Article 29, ont salué la décision de la Cour et ont fait appel à la Commission européenne de fournir une guidance sur les conséquences de l'arrêt au niveau européen et au niveau des Etats membres.

La Cour a estimé dans son arrêt du 8 avril 2014 que

# Les activités en 2014

*« la directive comporte une ingérence d'une vaste ampleur et d'une gravité particulière dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel sans que cette ingérence soit limitée au strict nécessaire ».*

Le G29 a par ailleurs demandé aux Etat membres et aux institutions européennes d'évaluer les conséquences de cet arrêt sur les législations nationales.

### *2.6.1.5 Développement du « Big Data »*

Le 16 septembre 2014, le G29 a présenté ses réflexions sur l'impact du développement du « Big Data » sur la protection des données à caractère personnel. Le groupe de travail est conscient des avantages potentiels du Big Data. Toutefois, ces opérations nécessitant le traitement de vastes quantités de données soulèvent de nombreuses questions en matière de protection de la vie privée.

Selon le groupe, le cadre légal européen sur la protection des données est applicable aux opérations Big Data en matière de traitement de données à caractère personnel. Certaines parties prenantes estiment que des principes comme la limitation de la finalité et la minimisation des données devraient être revus à l'aube du Big Data. Si le groupe reconnaît que l'application de ces principes aux opérations de Big Data exige une réflexion novatrice, il n'a aucune raison de penser que la directive de 1995 ne soit plus valide ou appropriée pour le développement du Big Data. En effet, le groupe a estimé que le respect du cadre légal représente un élément clé pour créer un climat de confiance pour les citoyens.

Même si les opérations de Big Data ne contiennent pas toujours des données à caractère personnel, ils requièrent une attention particulière. Des traits d'individus spécifiques peuvent être distingués grâce à la puissance de calcul des ordinateurs.

Le groupe a par ailleurs noté que de nombreux développements qualifiés aujourd'hui de Big Data – comme le développement de services de santé, la centralisation de fichiers de services répressifs ou encore la publicité comportementale en ligne – ont déjà été implémentés dans le cadre des règles de protection des données existantes.

Le groupe de travail est également conscient qu'en raison de la compétition internationale en matière de Big Data, différents cadres légaux régionaux, nationaux et internationaux pourraient être applicables simultanément et cela entraînerait des défis importants en matière de


conformité. Dans ce contexte, le groupe a estimé qu'une meilleure coopération entre les différentes autorités de contrôle était nécessaire au niveau mondial.

### *2.6.1.6 Internet des objets*

En date du 16 septembre 2014, le groupe de travail a publié un avis sur l'Internet des objets pour contribuer à identifier et à contrôler les risques dérivés de ces activités où les droits fondamentaux des citoyens sont en cause.

L'Internet des objets désigne une infrastructure dans laquelle des milliards de puces sont intégrées dans des objets quotidiens qui ont été conçus pour enregistrer, traiter, conserver et transférer des données et interagir avec d'autres objets ou systèmes par un réseau. Des nouvelles applications et services sont offerts grâce à la collecte et la combinaison de ces données sur les individus, que ce soit en mesurant des données spécifiques à leur l'environnement ou en observant ou analysant leurs habitudes.

Dans son avis, le G29 a décidé de se concentrer sur trois développements de l'Internet des objets : l'informatique vestimentaire (« wearable computing »), la mesure de soi (« Quantified Self ») et la domotique. Le « wearable computing » désigne des objets quotidiens, des vêtements, des montres ou des lunettes dans lesquelles sont insérés des capteurs pour étendre leurs fonctionnalités. Des objets pour la mesure de soi sont conçus pour être portés par des individus qui veulent enregistrer des informations sur leurs habitudes et leur style de vie (p.ex. analyse du sommeil, distances parcourues, calories brûlées, etc.). Grâce à la domotique, il est possible de contrôler à distance via Internet des objets quotidiens tels que les thermostats, les machines à laver ou encore les détecteurs de fumée.

Le développement de l'Internet des objets suscite de nouveaux défis en matière de protection de la vie privée. Non contrôlé, ce développement pourrait avoir comme conséquence une forme de surveillance des individus qui pourrait être considérée comme illégale en droit européen. L'internet des objets soulève aussi des questions importantes en matière de sécurité. Dans son avis, le G29 a mis l'accent sur les problèmes et les défis suivants :

- le manque de contrôle de l'utilisateur sur ses données ;
- la difficulté ou impossibilité d'obtenir un consentement valide des personnes concernées ;
- des utilisations des données à des fins autres que celles pour lesquelles elles ont été collectées ;
- la détection d'habitudes et le profilage dans le domaine privé et à l'intérieur de la maison ;

- les possibilités limitées de rester anonyme en utilisant ces services ;
- le risque de renoncer à la sécurité en faveur de l'efficacité.

En conclusion de son document, le G29 a fait plusieurs recommandations aux acteurs dans le domaine de l'Internet des objets :

- Avant le lancement de nouvelles applications, les risques sur la vie privée des personnes concernées devraient être évalués avec un « Privacy Impact Assessment ».
- Les acteurs devraient appliquer les principes du « Privacy by Design » (protection de la vie privée dès la conception) et « Privacy by Default » (les paramètres doivent être réglés de façon à protéger la vie privée des personnes concernées par défaut).
- Les personnes concernées doivent pouvoir contrôler leurs données à tout moment (autodétermination informationnelle).
- Les méthodes d'information, d'offrir le droit de refuser ou de demander le consentement doivent être facile à comprendre.

À côté des conseils généraux ci-dessus, le groupe de travail a aussi adressé des recommandations spécifiques aux développeurs d'applications, aux constructeurs d'appareils et aux plateformes sociales.

#### *2.6.1.7 Empreinte digitale d'appareil (« device fingerprint »)*

Le 25 novembre 2014, le G29 a publié un avis sur les empreintes digitales d'appareil (en anglais « device fingerprint »), qui suscitent d'importantes préoccupations en matière de protection des données.

Une empreinte digitale d'appareil est une information collectée sur un dispositif informatique distant à des fins d'identification. Celle-ci peut être utilisée pour identifier totalement ou partiellement un internaute ou un appareil même lorsque les « cookies » sont désactivés.

Plusieurs services en ligne ont notamment proposé le « device fingerprinting » comme alternative aux témoins de connexion HTTP pour collecter des statistiques sur leurs visiteurs ou pour suivre leurs actions en ligne sans demander leur consentement.

Or, le G29 a retenu dans son avis que l'article 5(3) de la directive ePrivacy (2002/58/CE, modifiée par la directive 2009/136/CE) est applicable aux empreintes digitales d'appareil. Comme pour les cookies, il est seulement possible d'utiliser les empreintes digitales


d'appareil de l'utilisateur à condition de recevoir son consentement explicite, sauf exceptions.

#### *2.6.1.8 Arrêt de la Cour de Justice de l'UE sur le droit à l'oubli*

Le 25 novembre 2014, le groupe de l'article 29 a adopté des lignes directrices concernant l'implémentation de la décision de la Cour de Justice de l'Union européenne sur le « droit à l'oubli » (C-131/12).

L'arrêt prévoit expressément que l'exercice du droit au déréférencement n'affecte que les résultats obtenus après une recherche effectuée sur la base du nom d'une personne et ne se traduit pas par la suppression du lien dans les indexes du moteur de recherche. En d'autres mots, l'information originale sera toujours accessible en ligne en effectuant une recherche sur d'autres termes ou en consultant directement le site source.

Le groupe de travail a estimé que le déréférencement ne doit pas se limiter aux versions européennes de Google. Lorsqu'il y a une désindexation, celle-ci doit aussi avoir lieu sur les autres déclinaisons du moteur de recherche, comme par exemple google.com. Cela concerne aussi les déclinaisons internationales d'autres moteurs de recherche comme Bing ou Yahoo.

Le G29 a par ailleurs dressé une liste des critères communs que les autorités de protection des données appliqueront pour traiter les plaintes qu'elles reçoivent suite à des refus de déréférencement par les moteurs de recherche. La liste contient 13 critères qui doivent être considérés comme des outils de travail flexibles qui aideront les autorités dans la prise de décision. Les critères seront appliqués au cas par cas et en accord avec les dispositions nationales applicables.

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

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

En 2014, le T-PD s'est penché principalement sur :

- la modernisation de la Convention 108 ;

# 2 Les activités en 2014

- les technologies médicales et leurs implications en matière de protection de données ;
- la cybercriminalité ;
- la protection des données à caractère personnel utilisées à des fins d'emploi ;
- l'utilisation de données à caractère personnel dans le secteur de la police ;
- la protection des données et le « Big Data ».

Le Comité consultatif a aussi continué à promouvoir la célébration de la Journée pour la protection des données et a fait en sorte que la sensibilisation et l'éducation à la protection des données demeurent des éléments essentiels du travail des différentes parties prenantes.

### Le CAHDATA a approuvé les propositions de modernisation de la Convention 108

Le Comité ad hoc sur la protection des données (CAHDATA) du Conseil de l'Europe a approuvé le 3 décembre 2014, après discussion et amendements correspondants, les propositions de modernisation de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108), lors de sa troisième et dernière réunion tenue à Strasbourg du 1 au 3 décembre 2014.

Le projet de protocole d'amendement qui sera préparé sur la base du texte approuvé, sera transmis aux Comité des Ministres pour examen et adoption.

### Le Luxembourg a ratifié la convention sur la cybercriminalité du Conseil de l'Europe

Par la loi du 18 juillet 2014, le Luxembourg a ratifié la Convention du Conseil de l'Europe sur la cybercriminalité, ouverte à la signature à Budapest le 23 novembre 2001, ainsi que son Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques.

Cette convention est le seul instrument international contraignant concernant la question de la cybercriminalité. Elle sert de ligne directrice pour tout pays élaborant une législation exhaustive en matière de cybercriminalité, mais aussi de cadre pour la coopération internationale contre la cybercriminalité parmi les Etats parties.

Il s'agit du premier traité international sur les infractions pénales commises via l'Internet et d'autres réseaux informatiques traitant en particulier des infractions portant atteinte aux

droits d'auteurs, de la fraude liée à l'informatique, de la pornographie enfantine, ainsi que des infractions liées à la sécurité des réseaux. Elle contient également une série de pouvoirs de procédures tels que la perquisition de réseaux informatiques et l'interception.

Son principal objectif, énoncé dans le préambule, est de poursuivre « une politique pénale commune destinée à protéger la société contre le cybercrime, notamment par l'adoption d'une législation appropriée et la stimulation de la coopération internationale ».

## 2.6.3 Le « Groupe de Berlin »

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

En 2014, le groupe a adopté des documents de travail sur le « Big Data » et sur l'utilisation d'appareils privés sur le lieu de travail (« BYOD – Bring Your Own Device ») lors de deux réunions à Skopje et à Berlin. Ces documents peuvent être téléchargés sur le site Internet du groupe de travail[7].

### *2.6.3.1 Big Data et protection de la vie privée*

Le terme « Big Data » désigne l'utilisation d'une énorme quantité de données, contrôlées par des entreprises, des autorités et d'autres organisations qui les analysent à l'aide d'algorithmes.

Les données sont partout. La quantité de données au niveau mondial augmente de 50% chaque année. 90% des données mondiales ont été générées lors des deux dernières années. La majorité de ces données sont générées par les consommateurs à travers des interactions sur des services en ligne. Avec l'émergence de l'Internet des objets, de nouveaux flux de données seront créés. Il est estimé qu'il y aura plus de 50 milliards de capteurs en 2015. Ces capteurs peuvent communiquer avec d'autres ordinateurs ou objets intelligents et transférer des données vers un service de cloud.

Big Data représente un défi important pour la protection de

[7] http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group

# Les activités en 2014

la vie privée. Certains prétendent qu'il sera impossible d'appliquer les règles de la protection des données à l'aube du Big Data et estiment que cette protection devrait être assurée par des entreprises qui sont transparentes dans leur gestion des données envers les personnes concernées. Toutefois, le Groupe de Berlin est d'avis que la protection de ces principes est plus importante que jamais et que ceux-ci garantissent que les citoyens ne feront pas l'objet d'un profilage extensif dans un large éventail de contextes nouveaux.

Selon le groupe, la protection de la vie privée dans un contexte de Big Data doit être basée sur les principes de limitation de la finalité, la pertinence et la minimisation des données, l'intégrité et la qualité des données, la transparence et l'accès à l'information.

L'objet de ce document de travail est de souligner les défis en matière de protection des données en relation avec le Big Data, particulièrement dans le domaine des télécommunications.

Le groupe a décrit d'abord en détail la « chaîne de valeur » en matière de Big Data qui comprend plusieurs étapes : la collecte de données, la conservation et l'agrégation des données, l'analyse des données et l'utilisation des résultats de l'analyse.

Ensuite ont été analysés les défis résultant de l'utilisation de Big Data. Le groupe a cité notamment :

- la réutilisation des données à de nouvelles fins ;
- la « maximisation des données » ;
- le manque de transparence ;
- la compilation des données, qui pourrait révéler des informations sensibles ;
- le risque de ré-identification ;
- les implications en matière de sécurité ;
- les données inexactes ;
- le déséquilibre de pouvoir entre les grandes entreprises et les consommateurs ;
- la discrimination sur base d'analyses statistiques.

Le Groupe de Berlin a finalement fait plusieurs recommandations sur la manière dont le Big Data peut être utilisé en respectant la vie privée des individus. Selon le groupe :

- Le consentement doit rester la pierre angulaire des lois sur la protection de la vie privée. Réduire l'importance de ce principe constituerait une diminution considérable du contrôle des individus sur leurs données.

- La procédure d'anonymisation doit être effective et irréversible.

- La transparence envers les personnes concernées et leur contrôle sur les données doivent être améliorés de la collecte jusqu'à l'utilisation des données.

- L'utilisation des technologies Big Data doit être basée sur les principes du « Privacy by design ».

- Les responsables du traitement doivent montrer qu'ils peuvent prendre des décisions responsables concernant l'utilisation de Big Data (« accountability »).

#### *2.6.3.2 Utilisation d'appareils privés dans des réseaux d'entreprise*

Le phénomène du « Bring Your Own Device » (en français : « apportez votre appareil personnel ») est de plus en plus répandu dans les environnements de travail. Il repose sur l'utilisation par un salarié de ses appareils technologiques privés (smartphones, tablettes, ordinateur portable etc.) dans le cadre professionnel.

Dans son document de travail, le Groupe de Berlin a analysé les risques en matière de sécurité et de la protection de la vie privée de cette pratique.

Selon le groupe, une organisation qui accepte l'utilisation d'appareils privés dans son réseau, doit prendre les mesures de sécurité nécessaires pour protéger les données de l'entreprise. En même temps, l'impact de ses mesures sur la vie privée des salariés doit être minimisé.

Il existe de nombreux risques potentiels liés à l'utilisation d'appareils privés dans le cadre professionnel :

- le risque de perte et de vol est augmenté pour ces appareils qui en principe sont petits et mobiles ;

- ces appareils sont capables de partager des données de l'entreprise par différentes applications en contournant les mesures de sécurité techniques ;

- il est difficile d'adapter le système d'exploitation sur des appareils privés pour réduire certaines fonctions et accroître la sécurité comme c'est souvent les cas avec les appareils mis à disposition par l'entreprise ;

- les appareils privés sont souvent connectés à des réseaux privés et publics (maison, aéroport, etc.) potentiellement moins sûrs que les réseaux situés dans les environnements de travail ;

- il est possible que l'infrastructure de réseau existante de l'entreprise n'ait pas été conçue avec une sécurité adéquate pour fournir un accès à partir de périphériques propres ;

# Les activités en 2014

- l'utilisation d'appareils privés n'est en principe pas limitée à une seule personne et s'étend souvent à la famille et au ménage du salarié ;

- des services comme la sauvegarde automatique ou d'autres logiciels tiers installés par l'utilisateur peuvent entraîner une utilisation inattendue ou non autorisée de services de cloud computing ;

- l'utilisateur peut être moins vigilant et prendre plus de risques de sécurité avec ses propres appareils qu'avec ceux de l'entreprise ;

- il est possible que les données personnelles ne soient pas supprimées de manière convenable avant l'élimination, la revente ou le recyclage de l'appareil.

À la lumière de ces risques en matière de sécurité et de la protection des données, le groupe de travail a recommandé aux organisations d'évaluer l'impact de l'utilisation d'appareils privés dans le contexte professionnel sur la vie privée des utilisateurs à l'aide d'un « Privacy Impact Assessment (PIA) ». Celui-ci conduit à évaluer la vraisemblance des risques d'atteinte à la vie privée et à documenter les mesures prises pour y faire face. Le Groupe de Berlin a énuméré de façon détaillée les mesures qui peuvent être prises dans son document de travail.

### 2.6.4 Le séminaire européen « Case Handling Workshop »

L'autorité de protection des données de la République de Macédoine a organisé le séminaire européen « Case Handling Workshop » à Skopje, les 6 et 7 octobre 2014.

Ce « workshop » a permis aux employés des autorités de protection des données européennes d'échanger leurs expériences pratiques en matière de traitement des plaintes.

En 2014, le séminaire a abordé les thèmes suivants :

- protection des données dans le domaine de la justice ;

- rétention des données ;

- collecte excessive de données ;

- équilibre entre protection des données et droit d'accès aux données publiques ;

- vidéosurveillance ;

- utilisation de « dashcams » ;

- copies des cartes d'identité dans les banques et autres institutions ;

- utilisation de données biométriques ;

- protection des données et marketing ;

- « mystery shopping » et protection des données ;

- transferts internationaux entre autorités publiques ;

- transferts de données vers les Etats-Unis.

### 2.6.5 Conférence internationale des commissaires de la protection des données

L'office de la protection des données personnelles de Maurice a organisé la 36ème Conférence internationale des commissaires de la protection des données et de la vie privée à Maurice du 13 au 16 octobre 2014. Le thème de la conférence était : « Un ordre mondial pour la protection des données : un rêve qui devient réalité ».

Le président de la CNPD a participé au panel « E-Health and data protection ». Sa présentation a porté sur le dossier électronique du patient au Luxembourg.

Des résolutions relatives aux thèmes suivants ont été adoptées :

- Internet des Objets ;

- Big Data ;

- coopération en matière répressive ;

- protection de la vie privée à l'ère numérique.

### 2.6.6 Conférence de printemps des autorités européennes à la protection des données

Le Conseil de l'Europe et la Commission Nationale de l'Informatique et des Libertés (CNIL) ont organisé conjointement la Conférence européenne des autorités de protection des données à Strasbourg le 5 juin 2014.

Le thème principal de cette « Spring conference » était la coopération entre autorités de protection des données. Pour l'édition de 2014, 90 experts de 30 différents pays s'étaient réunis autour de 3 sessions principales :

- Session 1 : État des lieux de la coopération européenne et internationale

- Session 2 : Attentes en termes de coopération européenne et internationale

- Session 3 : Perspectives et solutions pour une coopération renforcée

Le président de la CNPD est intervenu dans la première session et a présenté les cadres juridiques existants.

Des résolutions relatives à la révision de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108) et relative à l'accréditation de la Géorgie en tant que membre de la Conférence de printemps ont été adoptées.

### 2.6.7 Réunion de coordination annuelle du GPEN

Les 2 et 3 avril 2014 s'est tenue à Manchester la réunion de coordination annuelle du « Global Privacy Enforcement Network (GPEN) ». Cet événement a réuni les autorités de 34 pays de plusieurs continents, qui exercent toutes les prérogatives de vérification de la conformité du traitement de données à caractère personnel leur conférant des pouvoirs d'intervention et/ou de sanction en vue du respect de la protection de la vie privée.

La Commission nationale a adhéré en 2013 à ce réseau informel et de coopération dont elle attend un développement non négligeable de son expertise à travers les échanges d'expérience, de méthodologie et de capacité de réaction dans les dossiers concernant des activités transfrontalières, voire mondiales.

# 3 Les temps forts de 2014

**Les travaux de la Commission nationale ont été marqués par un certain nombre de dossiers, soit à l'ordre du jour 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 Évaluation de la sécurité et des risques sur la vie privée du dossier de soins partagé

Au Luxembourg, un dossier de soins partagés (ci-après DSP) sera prochainement créé automatiquement pour toute personne affiliée à la Sécurité Sociale. Ce dossier électronique, qui regroupera les informations de santé de chacun, devra contribuer à optimiser le flux des informations médicales qui circulent entre patients et professionnels de santé et permettre un meilleur suivi des soins des patients.

Si le DSP ne doit pas se révéler plus intrusif pour le citoyen 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 devront être contrebalancés par des règles protectrices rigoureuses et transparentes. Ces règles doivent être mises en œuvre au moyen de mesures techniques et organisationnelles aptes à faire respecter le droit à la vie privée des patients, en garantir sa protection et à assurer le respect du secret médical. Dans le cadre du traitement de données à caractère personnel, et particulièrement dans le domaine de la santé, il est donc primordial d'établir la confiance à travers la transparence et la sécurité.

L'objectif est de parvenir à une optimisation de la protection des données des patients tout en respectant les contraintes opérationnelles des prestataires de soins. Afin de concilier ces objectifs, la CNPD accompagne actuellement activement l'agence eSanté dans l'évaluation de leur plateforme d'échange de données. À cet effet, un groupe de travail commun a été mis en place par les deux entités. Les objectifs et les détails de l'évaluation que mène actuellement ce groupe de travail sont exposés ci-après.

### *Le Dossier de Soins Partagés (DSP) - De quoi s'agit-il ?*

Le gouvernement luxembourgeois a lancé fin 2006 le programme national dénommé « eSanté ». Les travaux préliminaires, menés en concertation avec les acteurs du secteur (hospitaliers et extrahospitaliers), ont pu souligner la nécessité de mettre en place une plateforme informatique

nationale permettant un échange et un partage des données de santé.

Pour faire suite aux travaux engagés, le gouvernement a décidé, dans le cadre de la loi du 17 décembre 2010 portant sur la réforme des soins des systèmes de santé, la création de l'agence eSanté dont une des missions clés consiste dans la réalisation, le déploiement et la gestion administrative et technique d'une plateforme électronique nationale d'échange et de partage de données de santé ainsi que des applications et des systèmes informatiques de santé à l'échelle nationale, à savoir le dossier de soins partagé (DSP). Le DSP regroupe les données médicales et autres informations utiles et pertinentes concernant le patient, afin de favoriser leur sécurité, la continuité et la coordination des soins, ainsi qu'une utilisation efficiente des services de soins de santé. Il peut notamment comporter :

- les comptes rendus des examens de radiologie,
- les images radiologiques ayant permis de faire le diagnostic et les images significatives permettant une relecture par un autre prestataire en cas de besoin,
- les résultats des analyses de laboratoire,
- les comptes rendus des interventions chirurgicales déjà réalisées,
- les rapports des endoscopies déjà réalisées,
- les prescriptions des médicaments,
- les antécédents de maladie,
- les informations relatives aux maladies chroniques comme par exemple le diabète,
- les lettres de transfert,
- les informations relatives aux allergies,
- les informations relatives aux vaccinations,
- les données administratives du patient,
- l'espace d'expression personnelle du patient.

Ces informations proviennent de diverses sources : médecins référents, médecins généralistes, médecins spécialistes, cabinets médicaux, hôpitaux, laboratoires d'analyses médicales, patients, etc.

# 3 Les temps forts de 2014


*Quelles sont les innovations introduites par le DSP ?*

Ce nouveau maillon dans la chaîne de soins est caractérisé par la multiplication des destinataires et par une ampleur inédite du traitement des données de santé.

Les données contenues dans le DSP sont des copies des documents qui se trouvent actuellement, entre autres, chez le médecin référent, le médecin généraliste, le médecin spécialiste, les hôpitaux, dans les laboratoires et les cabinets médicaux fréquentés par le patient. Une copie de ces informations sera stockée dans un entrepôt de données centralisé (une sorte de « cloud » localisé au Luxembourg). L'agence eSanté, en tant que responsable, a l'obligation de mettre en œuvre des mesures pour assurer une garantie de la sécurité des données et une haute disponibilité de l'infrastructure.

Avec le dossier de soins partagé, tout professionnel effectuant un suivi auprès du patient peut théoriquement accéder aux données spécifiques de son patient. Le partage des données entre les différents acteurs peut avoir un effet sur la relation classique qu'entretient le patient avec son médecin, le colloque singulier. Il peut être difficile de concilier ce partage d'informations avec le respect du secret médical par lequel chaque relation entre un patient et son médecin doit être scellée pour éviter d'éventuels abus.

La concentration quasi-exhaustive des informations relatives au parcours de santé d'un patient dans un dossier électronique global pourrait aussi susciter l'intérêt de tiers tel que, par exemple, l'employeur, les industries pharmaceutiques, les compagnies d'assurances, les autorités répressives, etc.

Il est aussi prévu que les autorités sanitaires et de sécurité sociale pourront réutiliser des données rendues anonymes (c'est-à-dire lorsque tous les traits identifiants d'une personne ont été enlevés) à des fins statistiques ou pour l'étude des épidémies (et des facteurs qui pourraient les causer) dans le respect des règles visant à garder l'anonymat des personnes. L'accès ne se fera pas sur les dossiers eux-mêmes, mais sur des bases de données tierces alimentées avec des données anonymisées.

### *Quelle est la légitimité du DSP ?*

Le DSP contribuera à la continuité des soins en participant à l'amélioration de la gestion des services de santé. Le pilotage national du système de soins de santé sera facilité grâce à une meilleure disponibilité des données médicales sous un même format.

Aujourd'hui, si un patient doit, par exemple, se rendre en urgence à l'hôpital pour un problème de santé, le médecin qui le prend en charge n'a pas forcément accès aux résultats de ses derniers examens (analyses, scanners, IRM, etc.). Très souvent, il sera dans l'obligation de faire des nouveaux examens. Le DSP permettra au médecin de voir les résultats des examens antérieurs du patient et ainsi d'éviter une redondance d'examens. De plus, la possibilité d'accéder très rapidement à une information sur l'état de santé antérieur du patient lui garantira potentiellement une meilleure prise en charge.

Ces finalités sont légitimes et nécessaires. Toutefois, elles nécessitent des garanties appropriées en matière de protection de la vie privée et des données à caractère personnel.

### *Quels sont les enjeux en matière de protection des données ?*

Les données de santé sont relatives aux corps humain et considérées comme des données particulièrement sensibles, qui relèvent de l'intimité de la vie privée. La centralisation et la mutualisation de ces données, résultant de la mise en œuvre du DSP, crée de nouveaux risques de violations de confidentialité et de la sécurité. Pour cette raison, des restrictions et des garanties fortes doivent être prévues.

L'enjeu de confiance des patients et du personnel de santé dans la sécurité des données est d'autant plus critique alors que le progrès scientifique nécessite davantage d'échanges et de partages de données par des intervenants successifs et équipes multidisciplinaires. Ce n'est que si les différents acteurs ont confiance dans la sécurité du système qu'ils seront prêts à en bénéficier.

L'objectif final est de parvenir à une optimisation de la protection des données des patients tout en respectant les contraintes opérationnelles des prestataires de soins.

Tous les volets et tous les risques doivent être passés en revue avant la mise en production du DSP. Une perte de confidentialité ou d'intégrité des informations aurait des répercussions très importantes sur la confiance et sur l'utilisation du DSP (tant par les patients que par le personnel de santé) et pourrait avoir des impacts graves sur la vie privée des individus (ex : perte d'emploi à cause de la révélation d'une maladie grave, refus inexpliqué d'obtention d'une assurance, isolement social…).

### *Comment peut se traduire l'autodétermination informationnelle du patient dans le cadre du DSP ?*

Une des garanties pour la protection de la vie privée est le respect de l'autodétermination informationnelle du patient. Chaque patient doit toujours

# Les temps forts de 2014

avoir le droit de décider par qui, quand et quelles données le concernant sont traitées. De même, chaque individu est libre d'apprécier et de décider du partage et de la perception de ses données. A cet effet, on constate que la technologie peut offrir des services facilitant la maîtrise, voir l'appropriation, par les individus, de l'autodétermination informationnelle lorsqu'elle est mise en œuvre en respectant les principes de « privacy by design ». En d'autres mots, les services doivent être conçus avec un paramétrage par défaut favorable au respect de la vie privée.

Un dossier électronique sera ouvert d'office pour chaque patient. Toutefois, le patient pourra s'opposer dès la création à l'alimentation de son DSP. Même si son consentement préalable n'est pas demandé, le patient garde tout de même un rôle actif lors de la création du DSP. Par ailleurs, le patient pourra demander la désactivation de son dossier. Cette possibilité d' « opt-out » reste valable pour toute la durée de vie du DSP. À partir de la désactivation du dossier, les prestataires de soins ne peuvent plus inscrire de nouvelles données dans le DSP, mais ceux qui y figuraient déjà restent inscrites et uniquement les auteurs des documents auront encore accès à leur propre document.

Le patient aura également la faculté d'attribuer un accès modulaire des informations qui le concernent selon le personnel de santé appelé à consulter son dossier et selon la nature des informations enregistrées. Cela permet 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 de ses données de santé. Il aura toujours la possibilité de masquer des documents à un ou à un ensemble de professionnels. Il peut aussi bloquer l'accès au dossier à un professionnel de santé particulier (par exemple un voisin qui serait médecin ou soignant).

À retenir que le patient aura lui-même aussi accès à un espace d'expression personnel, qui lui permettra de partager et de gérer dans son DSP les informations qu'il souhaite porter à la connaissance des prestataires de santé.

Le patient aura la possibilité de vérifier a posteriori les accès effectués à son dossier par la mise en place d'une journalisation. Cette dernière devra garantir une intégrité des informations qui y sont contenues : tous les accès sans exception seront enregistrés et des entrées du journal des accès ne doivent pas pouvoir être effacées.

*Comment sont évalués les risques sur la vie privée ?*

Dans le cadre de ce projet, la CNPD considère que le déploiement d'un « Privacy Impact Assessment » (PIA ou DPIA - Data Protection Impact Assessment) est une démarche adaptée pour faire une analyse des risques de l'impact sur la vie privée pour les personnes concernées et évaluer le respect des principes de protection des données à caractère personnel comme l'autodétermination informationnelle.

Bien que le nouveau projet de règlement européen sur la protection des données qui prescrira une telle évaluation préalable pour tous les nouveaux systèmes de traitement potentiellement intrusifs ou susceptibles de comporter des risques particuliers ne soit pas encore en vigueur, l'étendue et le degré de sensibilité du projet DSP justifient d'adopter d'ores et déjà une telle approche de protection des données dès la conception (« Privacy by design »).

Dans le cadre des activités de l'agence eSanté, le PIA évalue :

- les éléments de sécurité technique (ex : architecture de la plateforme, sécurité des transmissions des données, sécurité des données stockées…)
- les éléments de sécurité organisationnelle (ex : mise en œuvre d'une politique de sécurité du système d'information, politique de chiffrement…)
- les éléments inhérents à la protection des données à caractère personnel (ex : droit d'accès / rectification / suppression pour les patients, journalisation de tous les accès effectués pour chaque dossier patient, mise en œuvre d'une politique « vie privée », la définition de la matrice d'habilitations des accès aux DSP, techniques d'anonymisation…).

De manière plus détaillée, le PIA comporte, entre autres, les sections suivantes : responsabilisation des ressources humaines, organisation de la protection de la vie privée, gestion des risques sur la vie privée, politique de protection de la vie privée, intégration de la protection de la vie privée dans la mise en œuvre de nouveaux

projets (privacy by design), supervision de la protection de la vie privée, les exigences spécifiques relatives au respect des droits du patient et du personnel de santé ou encore les exigences spécifiques relatives à la protection des données à caractère personnel.

Dans le contexte de l'évaluation des risques sur la vie privée sont notamment identifiés les types de données collectées, les processus décisionnels liés à leurs usages et les accès autorisés pour les professionnels de santé. Par exemple, le dossier de soins partagé comprend une fonction « bris de glace » qui permet aux professionnels de soins de santé d'accéder aux données d'un patient en cas d'acte médical à pratiquer de toute urgence lorsque le patient (ou son représentant) est dans l'incapacité de consentir à temps. Pour cet exemple, l'évaluation consistera à analyser les processus décisionnels desquels découlent la possibilité d'activer le « bris de glace », les accès réels autorisés pour ce scénario, la journalisation des accès qui en résulte et la durée de validité de cet accès exceptionnel.

La totalité de l'évaluation de la plateforme permet également d'obtenir une transparence des activités en relation avec les données à caractère personnel par l'élaboration d'une cartographie des risques et, de ce fait, permettra à l'agence eSanté de choisir en connaissance de causes et de mettre en œuvre les mesures adéquates pour traiter les risques identifiés.

Finalement, le PIA n'est pas une analyse unique qui se déroule avant le lancement du dossier de soins partagés, mais il a vocation à faire partie intégrante de l'évolution de la plateforme eSanté et des changements futurs inhérents à ce dernier. En d'autres termes, toutes modifications ou nouvelles fonctionnalités ajoutées au sein de la plateforme feront l'objet d'une analyse des risques sur la vie privée afin que l'agence eSanté soit en mesure de continuellement garantir un haut niveau de sécurité pour les traitements de données de santé.

## 3.2 Publication de la brochure « La surveillance sur le lieu de travail »

Le domaine des nouvelles technologies connaît de nos jours un développement fulgurant. L'utilisation de ces nouvelles technologies est à l'origine d'une mutation profonde et inexorable au sein de notre société dans son ensemble. Alors que leurs apports bénéfiques sont incontestables, le constat inévitable est que ces technologies deviennent également de plus en plus envahissantes et intrusives à notre

CHAMBRE DES SALARIES
LUXEMBOURG

N° 4 - OCTOBRE 2014

# dialogue

THÉMATIQUE

## LA SURVEILLANCE SUR LE LIEU DE TRAVAIL
## DIE ÜBERWACHUNG AM ARBEITSPLATZ

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

www.csl.lu

# Les temps forts de 2014

égard. Et ce développement inquiétant touche aussi bien la sphère privée des individus que leur environnement professionnel.

Le milieu du travail n'est pas épargné par les dernières avancées réalisées dans le domaine de la technologie. Dans un contexte où l'employeur cherche à gérer efficacement et à rentabiliser au maximum son entreprise, celui-ci entend aussi mettre à son profit les nouvelles technologies. Or, celles-ci permettent de suivre l'activité des salariés avec un niveau de détail impensable il y a quelques années.

Qu'il s'agisse des derniers développements en matière de géolocalisation, de vidéosurveillance, de biométrie ou de systèmes informatiques permettant une surveillance minutieuse de l'usage des outils informatiques, le contrôle des activités des salariés à l'aide de ces nouvelles technologies s'est extrêmement diversifié au cours des dernières années. Le développement du concept BYOD (« bring your own device ») suscite lui aussi la controverse entre les droits et intérêts de l'employeur et le respect de la vie privée des salariés.

Tous ces dispositifs enregistrent évidemment de nombreuses données à caractère personnel relatives aux salariés. Leur utilisation est dès lors susceptible de porter gravement atteinte aux droits des salariés et au respect de leur vie privée sur le lieu de travail, droit qui a été consacré par la jurisprudence européenne : « Il paraît, en outre, n'y avoir aucune raison de principe de considérer cette manière de comprendre la notion de vie privée comme excluant les activités professionnelles ou commerciales : après tout, c'est dans leur travail que la majorité des gens ont beaucoup, voire le maximum d'occasions de resserrer leurs liens avec le monde extérieur.[8]» .

Pour contrecarrer toute dérive potentielle, le législateur luxembourgeois a mis en place un régime juridique spécifique applicable aux traitements de données à des fins de surveillance, qui traduit en quelque sorte une mise en balance des intérêts divergents qui sont, d'une part pour l'employeur, le droit de veiller au bon fonctionnement de son entreprise, et d'autre part pour les salariés, le droit de bénéficier du respect de leur vie privée sur leur lieu de travail.

Comment concilier les droits de chacun lors de la mise en place d'une surveillance sur le lieu de travail ? Quelles sont les dispositions légales à respecter ? Quelles peuvent être les raisons amenant un employeur à mettre en œuvre une surveillance ? Quelles mesures doivent-ils

[8] CEDH, Niemietz c. Allemagne, 16 décembre 1992. Voir en ce même sens : CEDH, Halford c. Royaume-Uni, 27 juillet 1997 ; CEDH, Copland c. Royaume-Uni,3 avril 2007 ; CEDH, Peev c. Bulgarie, 26 juillet 2007.

adopter pour se conformer à la loi ? De quels droits disposent les salariés ? Comment sont-ils protégés ?

La nouvelle publication de la CNPD et de la Chambre des Salariés (CSL) relative à la surveillance sur le lieu de travail a pour objet d'apporter des réponses à toutes ces questions et d'éclairer le lecteur sur les droits et obligations du salarié et de l'employeur en la matière.

Dans un premier temps, la brochure expose les deux régimes applicables au traitement de données à caractère personnel à des fins de surveillance :

- les traitements à des fins de surveillance des tiers (régime général),
- les traitements à des fins de surveillance des salariés sur le lieu de travail (régime spécifique).

Dans un deuxième temps, elle analyse les différentes formes de surveillance qui sont utilisées sur le lieu de travail telles que :

- la vidéosurveillance,
- le contrôle de l'utilisation des outils informatiques,
- l'enregistrement des conversations téléphoniques,
- les systèmes de reconnaissance biométrique,
- les dispositifs de géolocalisation et
- les systèmes de surveillance des accès et des horaires de travail.

Pour chaque forme de surveillance, les auteurs ont essayé, dans la mesure du possible, de donner des exemples concrets illustrés par des jurisprudences et cas pratiques.

## 3.3 Table ronde à l'occasion de la journée de la protection des données : « Les défis en matière de protection de la vie privée dans un monde interconnecté »

A la veille de la Journée européenne de la protection des données, la CNPD et le Centre Interdisciplinaire pour la Sécurité, la Fiabilité et la Confiance (SnT) de l'Université du Luxembourg ont organisé une table ronde intitulée « Les défis en matière de protection de la vie privée dans un monde interconnecté ».

L'événement a réuni des experts dans le domaine du droit, de l'industrie et de la régulation pour explorer le défi de protéger la vie privée dans un monde numérique de plus en plus interconnecté. Les participants étaient :

- Prof. Dr. Stefan Braum (Doyen de la Faculté de Droit, d'Économie et de Finance de l'Université du Luxembourg)
- M. Gérard Lommel (Président, Commission nationale pour la protection des données, CNPD)
- M. Michael Hofmann (Partner, Information Risk Management, KPMG Luxembourg)
- RA Prof. Dr. Stephan Ory (Avocat et professeur honoraire à l'Université du Saarland)

Avec les développements récents autour de la collecte des données de la NSA, la possibilité de localiser et de profiler les utilisateurs à l'aide d'applications mobiles, avec la perspective que Google et d'autres entreprises entrent dans nos chambres à coucher via la technologie du smart metering, réveils ou autres dispositifs dans l'ère de l'Internet des objets, il est devenu évident que les règles existantes en matière de protection des données doivent être modernisées pour que le droit à l'autodétermination informationnelle reste pertinent.

# 3 Les temps forts de 2014


*De gauche à droite : Michael Hofmann, Stephan Ory, Stephan Braum, Gérard Lommel, Björn Ottersten et Mark Cole*

Alors que les débats au niveau de l'Union européenne concernant le nouveau règlement général continuent, les intervenants se sont prononcés sur les sujets suivants :

- Comment donner davantage de pouvoirs aux citoyens afin qu'ils puissent prendre des décisions concernant leurs données et qu'ils aient plus de contrôle sur la collecte et l'utilisation de leurs données.

- Comment le nouveau règlement peut donner plus de droits aux citoyens comme le droit à l'effacement, la portabilité des données, un accès élargi et plus simplifié et comment ces droits peuvent être conçus pour être plus faciles à faire appliquer.

- Comment il peut être garanti que l'implémentation des règles en matière de protection des données dans les 28 États Membres et leur application pratique se fait de manière unifiée et si cela est une réponse appropriée aux attentes des citoyens, consommateurs, entreprises et développements dans d'autres parties du monde.


*Table ronde « Les défis en matière de protection de la vie privée dans un monde interconnecté ».*

# 4 Perspectives

En 2014, la Cour de justice de l'Union européenne (CJUE) a adopté plusieurs arrêts relatifs à la protection des données à caractère personnel et à la protection de la vie privée. Il s'agit de :

- l'arrêt du 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12 (Digital Rights Ireland et Seitlinger e.a.) qui invalide la directive sur la conservation des données ;

- l'arrêt du 13 mai 2014 dans l'affaire C-131/12 (Google Spain SL, Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González) qui consacre un « droit à l'oubli » pour les moteurs de recherche et

- l'arrêt du 11 décembre 2014 dans l'affaire C-212/13 (František Ryneš / Úřad pro ochranu osobních údajů) qui confirme que la directive sur la protection des données s'applique à la vidéosurveillance au domicile d'un particulier si la caméra est dirigée vers la voie publique.

Dans la suite, nous allons passer en revue les trois arrêts et en décrire les conséquences.

### *La Cour de Justice de l'UE a déclaré la directive sur la conservation des données invalide*

La directive européenne 2006/24/CE du 15 mars 2006 sur la conservation des données a été invalidée par la Cour de justice de l'Union européenne qui l'a déclarée disproportionnée et trop intrusive. La Cour a estimé dans son arrêt du 8 avril 2014 que *« la directive comporte une ingérence d'une vaste ampleur et d'une gravité particulière dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel sans que cette ingérence soit limitée au strict nécessaire ».*

La directive précise les obligations des fournisseurs de services de communications électroniques, qui doivent conserver les données relatives au trafic, de localisation ainsi que les données nécessaire pour identifier l'utilisateur à des fins de prévention, de recherche, de détection et de poursuite des infractions graves. Selon la Cour, ces données *« prises dans leur ensemble, sont susceptibles de fournir des indications très précises sur la vie privée des personnes dont les données sont conservées, comme les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales et les milieux sociaux fréquentés ».*

*« La conservation des données en vue de leur transmission éventuelle aux autorités nationales compétentes répond effectivement à un objectif d'intérêt général, à savoir la lutte contre la criminalité grave ainsi que, en définitive, la*

*sécurité publique », a poursuivi la Cour. « Toutefois, la Cour estime qu'en adoptant la directive sur la conservation des données, le législateur de l'Union a excédé les limites qu'impose le respect du principe de proportionnalité ».*

L'arrêt ne s'est pas prononcé sur la validité des législations nationales qui ont transposé la directive et qui restent donc en place et continuent à lier les opérateurs du secteur des communications électroniques. Même si la directive 2006/24/CE n'existe plus, les opérateurs luxembourgeois sont à l'heure actuelle toujours obligés à retenir ces données (articles 5 et 9 de la loi du 30 mai 2005) et les juges d'instruction continuent à y avoir accès (article 67-1 du Code d'instruction criminelle relatif au « repérage »).

La CNPD a publié un avis sur l'arrêt en juin 2014[9] et a analysé en détail les conditions de validité qui devront être remplies par les lois nationales pour encadrer l'obligation de conservation d'une part et l'accès aux données par les autorités d'autre part. La CNPD a recommandé l'élaboration d'un projet de loi visant à amender les dispositions actuelles sur plusieurs points parmi lesquels la redéfinition de la condition correspondant à l'objectif de lutte contre la criminalité grave et organisée et le terrorisme par un critère plus approprié de qualification et d'incrimination des faits qui font l'objet de l'enquête.

Le Ministre de la Justice a annoncé qu'il faut adapter dans les meilleurs délais – et sans attendre une initiative de la Commission européenne – la législation luxembourgeoise aux exigences de l'arrêt de la CJUE. Selon le ministre, les points suivants sont les plus importants :

- préciser les conditions d'accès aux données retenues en remplaçant le seuil de peine (actuellement un an, art. 67-1 Code d'instruction criminelle) par une liste limitative d'infractions pour lesquelles les juge d'instruction peuvent ordonner l'accès aux données ;

- introduire une obligation de destruction irrémédiable des données retenues après l'expiration du délai de rétention sans aucune possibilité de les conserver, même sous forme anonymisée ;

- renforcer la sécurité de la rétention des données auprès des opérateurs télécom en prévoyant des mesures techniques, matérielles et organisationnelles très strictes à mettre en œuvre dans le but de garantir un niveau de protection élevé des données pendant le délai de rétention et lors de leur traitement par les opérateurs et leurs salariés.

À défaut d'initiative de la part de la Commission européenne, le gouvernement s'est engagé à clarifier sous Présidence luxembourgeoise la question du maintien ou de l'abandon du principe même de la rétention des données au niveau européen.

### *« Droit à l'oubli » : l'exploitant d'un moteur de recherche sur Internet est responsable du traitement qu'il effectue des données à caractère personnel qui apparaissent sur des pages web publiées par des tiers*

Dans l'affaire opposant Google à l'autorité espagnole de la protection des données, la Cour de justice européenne a rendu un arrêt reconnaissant un « droit à l'oubli » ou du moins une conséquence concrète de celui-ci : selon cet arrêt, tout citoyen européen peut demander à ce que ses données à caractère personnel n'apparaissent plus dans les résultats de moteurs de recherche en ligne si celles-ci sont erronées ou ne sont plus pertinentes. Les juges ont précisé cependant que cette possibilité ne devait pas être systématique. L'appréciation des requêtes devait se faire au cas par cas et au regard de l'information en question et sa sensibilité pour la vie privée de la personne concernée, ainsi que de l'intérêt public à recevoir cette information.

Le point de départ de cette affaire était une plainte d'un citoyen auprès de l'autorité espagnole. En tapant son nom dans le moteur de recherche, il a remarqué que plusieurs résultats renvoyaient vers un article de

[9] Voir partie 2.2.2.

# 4 Perspectives

presse de 1998 relatant la mise en vente aux enchères forcée de sa maison. Après cette découverte, il voulait que ces résultats soient retirés du moteur de recherche au motif que ces derniers n'étaient plus d'actualité, ce que la société américaine a refusé. Saisie en appel, la justice espagnole a demandé à la CJUE de se prononcer sur ce point.

Dans son arrêt, la Cour a conclu que Google, et de manière générale tous les moteurs de recherche, sont des responsables du traitement au sens de la directive 1995/46/CE sur la protection des données. Les obligations classiques du droit européen en matière de gestion, protection et de suppression des données à caractère personnel s'appliquent donc aussi à eux.

Concrètement, lorsqu'à la suite d'une recherche effectuée à partir du nom d'une personne, la liste de résultats affiche un lien vers une page web qui contient des informations sur la personne en question, la personne concernée peut s'adresser directement à l'exploitant ou, lorsque celui-ci ne donne pas suite à sa demande, saisir les autorités compétentes pour obtenir, sous certaines conditions, la suppression de ce lien de la liste de résultats.

Quelques semaines après l'arrêt de la Cour, les principaux moteurs de recherche comme ceux de Google (Search) et de Microsoft (Bing) ont mis en ligne un formulaire permettant aux citoyens européens de demander la suppression de résultats de recherche qu'ils jugent inappropriés. Lors de l'évaluation de chaque demande, le moteur de recherche vérifie si les résultats comprennent des informations obsolètes sur la vie privée du requérant. Il cherche également à déterminer si ces informations dans les résultats de recherche présentent un intérêt public, par exemple, si elles concernent des escroqueries financières, une négligence politique, des condamnations pénales ou la conduite publique de responsables politiques.

Si un requérant est convaincu d'avoir donné une raison légitime de faire supprimer ses données mais que sa demande a été refusée, il peut contacter l'autorité nationale compétente et/ou s'adresser au tribunal. Dans tous les cas, il doit d'abord demander la suppression de ses données et respecter à cet effet la procédure de la loi sur la protection des données avant que l'autorité nationale ou le tribunal puissent intervenir.

Jusqu'à présent, la compétence de la CNPD se limite à intervenir en tant que médiateur. Elle peut donc uniquement évaluer si, à son avis, le refus est fondé. Dans la négative, elle peut faire pression sur le gestionnaire du site Internet concerné pour faire supprimer les données du requérant, sans pour autant

pouvoir l'imposer. Pour cela, le requérant doit s'adresser au tribunal. Le requérant peut également choisir de ne pas solliciter la CNPD et de s'adresser directement au tribunal.

*La directive sur la protection des données s'applique à la vidéosurveillance au domicile d'un particulier si la caméra est dirigée vers la voie publique*

Selon la Cour de justice de l'Union européenne, la directive sur la protection des données à caractère personnel (Directive 95/46/CE) s'applique à l'enregistrement vidéo réalisé à l'aide d'une caméra de surveillance installée par une personne sur sa maison familiale et dirigée vers la voie publique. Au Luxembourg, cette directive est transposée par la loi modifiée du 2 août 2002.

La directive permet, en principe, de traiter de telles données que si la personne concernée a donné son accord. Néanmoins, elle ne s'applique pas au traitement de données effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques. La Cour a constaté que cette exemption doit être interprétée de manière stricte. Ainsi, une vidéosurveillance qui s'étend à l'espace public et qui, de ce fait, est dirigée en dehors de la sphère privée de la personne traitant les données ne peut pas être considérée comme « une activité exclusivement personnelle ou domestique ».

Dans cette affaire originaire de la République tchèque, un particulier avait installé sur sa maison familiale une caméra de surveillance qui filmait l'entrée de celle-ci, la voie publique ainsi que l'entrée de la maison d'en face. Lorsqu'une fenêtre fut brisée, les enregistrements de la caméra ont permis d'identifier deux suspects. L'un d'eux a toutefois contesté auprès de l'Office tchèque pour la protection des données la légalité de ce traitement des données. L'Office a constaté que le particulier avait effectivement violé les règles en matière de protection des données et lui a infligé une amende. À cet égard, l'Office a relevé, entre autres, que les données du suspect avaient été enregistrées sans son consentement alors qu'il était sur la voie publique, c'est-à-dire dans la portion de la rue située devant la maison.

La directive permet néanmoins d'apprécier l'intérêt légitime de cette personne à protéger ses biens, sa santé et sa vie, ainsi que ceux de sa famille. En particulier, premièrement, le traitement de données à caractère personnel peut être effectué sans le consentement de la personne concernée, notamment lorsqu'il est nécessaire à la réalisation de l'intérêt légitime du responsable du traitement. Deuxièmement, une personne ne doit pas être informée du traitement de ses données, si l'information de celle-ci se révèle impossible ou implique des efforts disproportionnés. Troisièmement, les États membres peuvent limiter la portée des obligations et des droits prévus par la directive lorsqu'une telle limitation est nécessaire pour la prévention, la recherche, la détection et la poursuite d'infractions pénales ou la protection des droits et libertés d'autrui.

# 5 Ressources, structures et fonctionnement

## 5.1 Rapport de gestion relatif aux comptes de l'exercice 2014

*Dépenses*

Le total des frais de fonctionnement de l'établissement public au cours de l'exercice 2014 s'élève à 1.709.863,21 €. Ce chiffre représente une augmentation de 2,69% par rapport à l'exercice précédent et dépasse les prévisions budgétaires.

Les charges relatives au personnel permanent correspondent aux prévisions budgétaires de 1.450.000 €, alors que cet article avait été adapté aux dépenses des années précédentes. Or, entretemps, un poste vacant a été pourvu.

Les dépenses d'honoraires et frais d'experts et de prestataires externes de 85.000 € dépassent de 47% les prévisions budgétaires. Parmi ces dépenses figurent également les honoraires d'avocats et de la fiduciaire qui tient la comptabilité et établit le bilan de l'établissement public. Le montant principal était toutefois absorbé par l'étude d'impact réalisée dans la cadre du dossier de soins partagé.

Après le déménagement de la CNPD dans ses nouveaux locaux à Esch-Belval, seul le montant des charges locatives de 35.700,81 € a été porté en compte, puisqu'il n'y a plus de frais de loyer à supporter.

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

Les frais de déplacement et de séjour à l'étranger se chiffrent à 30.065,81 €, et dépassent ainsi légèrement les prévisions tout en restant 26,38% en dessous du montant de l'année précédente. Les frais de voyage sont dans une large mesure incompressibles, puisqu'ils se rapportent à la participation des membres effectifs et des collaborateurs de la Commission nationale aux réunions, séances de travail et conférences organisées sur le plan européen dans le domaine de la protection des données, où l'autorité luxembourgeoise ne peut pas faire la politique de la chaise vide et se doit d'être représentée.

Les dépenses pour l'information du public et la communication de 9.875,17 € restent largement en dessous des prévisions budgétaires, étant donné que certains des projets prévus sont restés en suspens.

A défaut de disposer des ressources spécialisées nécessaires en interne pour la maintenance des systèmes et réseaux informatiques, les frais correspondants aux prévisions budgétaires n'ont pas pu être diminués en 2014. Vu l'état suranné de certains équipement informatiques, des efforts d'investissement ont été effectués pour remplacer ces derniers, de sorte que le total de la dépense s'élève à 75.888,38 €, ce qui constitue une augmentation de 347% par rapport à l'année précédente.

Les amortissements comptabilisés en 2014 atteignent un montant total de 5.723,36 €. 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'élève à 115.168 € et dépasse dès lors les prévisions de 15.168 €.

En outre, des produits financiers (intérêts créditeurs) ont été enregistrés à hauteur de 1.014,33 €.

### *Résultat d'exploitation*

Compte tenu de la dotation annuelle de 1.665.000 € dont la Commission nationale a bénéficiée en 2014 de la part de l'Etat en application de l'article 37 paragraphe (4) de la loi, le résultat d'exploitation de l'établissement public s'élève à - 44.863,21€ au 31 décembre 2014. Ce déficit a pu être comblé par l'excédent d'exercices antérieurs.

# 5 Ressources, structures et fonctionnement

## 5.2 Personnel et services

*Collège*
Tine A. LARSEN,
présidente
Thierry LALLEMANG,
membre effectif
Georges WANTZ,
membre effectif

*Membres suppléants*
Josiane PAULY,
Ministère du Développement durable et des Infrastructures (Département des transports), direction de la circulation et de la sécurité routières
Marc HEMMERLING,
Association des Banques et Banquiers Luxembourg (ABBL), membre du comité de direction
François THILL,
Ministère de l'Économie, direction du commerce électronique et de la sécurité de l'information

*Service juridique*
Georges WEILAND,
attaché de direction 1er en rang
Michel SINNER,
attaché de direction 1er en rang
Christian WELTER,
attaché de direction 1er en rang
Laurent MAGNUS,
employé public
Arnaud HABRAN,
employé public

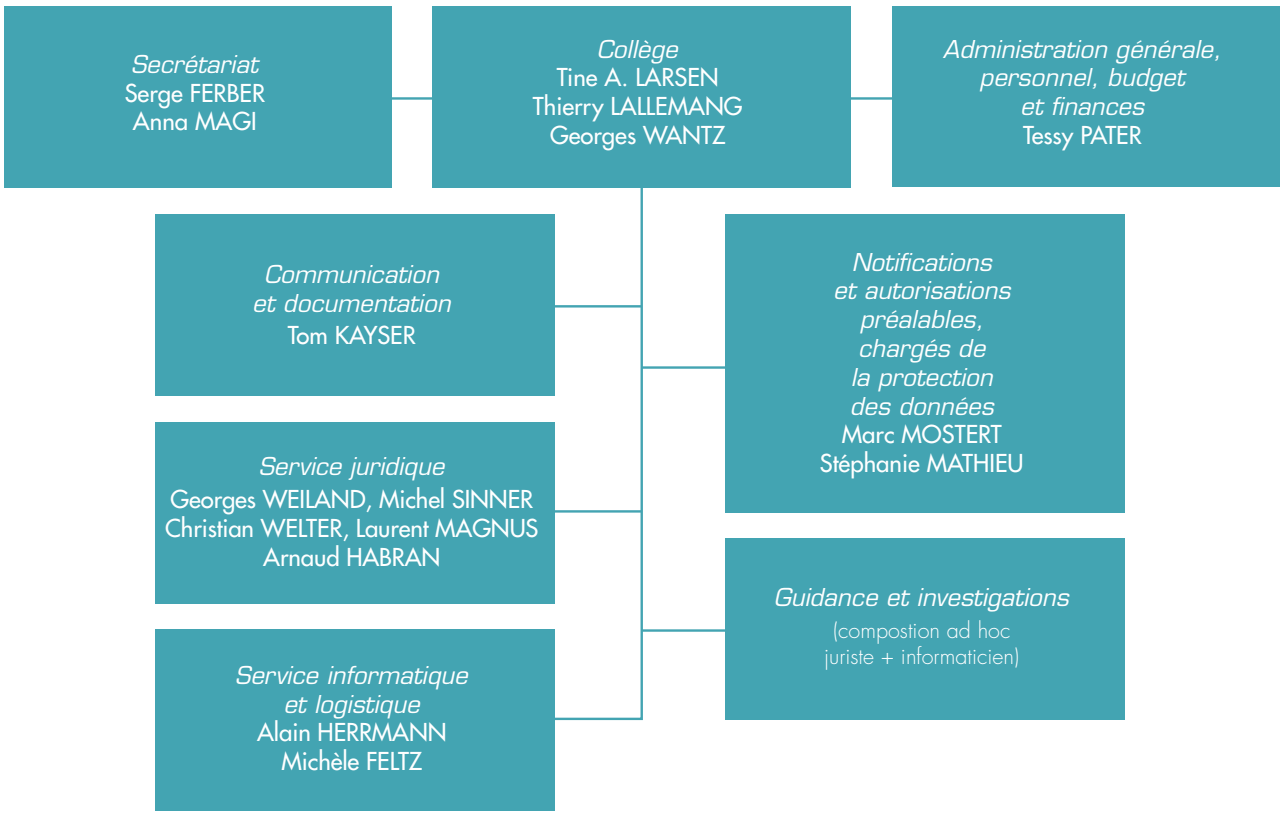
*Tenue du registre public et prise en charge administrative des notifications et demandes d'autorisation*
Marc MOSTERT,
chef de bureau adjoint
Stéphanie MATHIEU,
rédacteur

*Service informatique et de la logistique*
Alain HERRMANN,
attaché de direction
Michèle FELTZ,
employée de l'Etat

*Secrétariat, administration générale et finances*
Tessy PATER,
rédacteur
Serge FERBER,
employé de l'Etat
Anna MAGI,
employée de l'Etat

*Service communication et documentation*
Tom KAYSER,
attaché de direction 1er en rang

## 5.3 Organigramme de la Commission nationale



# 6 La Commission nationale en chiffres

## *Formalités préalables*

| | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| a) Notifications | | | | | | | | | | | TOTAL 2003-2014 |
| Notifications ordinaires | 500 | 250 | 760 | 385 | 345 | 295 | 355 | 437 | 421 | 564 | 7.808 |
| Notifications simplifiées | 720 | 890 | 537 | - | - | - | - | - | - | - | 3.797 |
| Engagements de conformité | - | - | - | 942 | 227 | 15 | 46 | 149 | 651 | 45 | 2.075 |
| (Total a) | 1.220 | 1.140 | 1.297 | 1.327 | 572 | 310 | 401 | 586 | 1.072 | 609 | 13.680 |
| b) Autorisations préalables | | | | | | | | | | | TOTAL 2003-2014 |
| Demandes d'autorisation | 317 | 295 | 392 | 606 | 542 | 607 | 604 | 706 | 833 | 914 | 6.987 |
| Engagements de conformité | 17 | 19 | 151 | 220 | 70 | 92 | 49 | 70 | 149 | 85 | 1.654 |
| (Total b 2003-2014) | 334 | 314 | 543 | 826 | 612 | 699 | 653 | 776 | 982 | 999 | 8.641 |
| (Total général a + b 2003-2014) | 1.554 | 1.454 | 1.840 | 2.153 | 1.184 | 1.009 | 1.054 | 1.362 | 2.054 | 1.608 | 22.321 |
| Déclarants (responsables ayant accompli des formalités) | 2.850 | 3.300 | 3.754 | 4.357 | 4.772 | 5.110 | 5.399 | 5.821 | 6.559 | 6.993 | |

## *Demandes de renseignements*

| | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 |
|---|---|---|---|---|---|---|---|---|---|---|
| a) Demandes de renseignements par écrit | | | | | | | | | | |
| (Total a) | 117 | 150 | 148 | 138 | 138 | 213 | 173 | 273 | 274 | 416 |
| b) Demandes de renseignements par téléphone | | | | | | | | | | |
| (Total b) | 1.550 | 1.930 | 1.870 | 1.586 | 1.407 | 1.405 | 1.634 | 1.424 | 1.803 | 1.776 |
| (Total général a + b) | 1.667 | 2.080 | 2.018 | 1.724 | 1.545 | 1.618 | 1.807 | 1.697 | 2.077 | 2.192 |

## *Plaintes*

| | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 |
|---|---|---|---|---|---|---|---|---|---|---|
| Plaintes, demandes de vérification de licéité et investigations | 40 | 30 | 34 | 63 | 133 | 145 | 115 | 133 | 177 | 207 |

### *Séances de délibération*

| | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 |
|---|---|---|---|---|---|---|---|---|---|---|
| | 36 | 39 | 40 | 40 | 37 | 38 | 35 | 27 | 31 | 20 |

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

| | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 |
|---|---|---|---|---|---|---|---|---|---|---|
| | 33 | 23 | 22 | 22 | 32 | 40 | 37 | 43 | 39 | 40 |

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

| | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 |
|---|---|---|---|---|---|---|---|---|---|---|
| Secteur public | 62 | 32 | 56 | 52 | 54 | 56 | 69 | 71 | 102 | 92 |
| Secteur privé | 38 | 12 | 40 | 44 | 52 | 54 | 71 | 61 | 75 | 77 |
| **(Total)** | **100** | **44** | **96** | **96** | **106** | **110** | **140** | **132** | **177** | **169** |

### *Séances d'information, conférences, exposés*

| | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 |
|---|---|---|---|---|---|---|---|---|---|---|
| | 10 | 11 | 14 | 11 | 23 | 21 | 15 | 10 | 18 | 22 |

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

| | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 |
|---|---|---|---|---|---|---|---|---|---|---|
| Articles et interviews parus dans | | | | | | | | | | |
| - les quotidiens | 16 | 67 | 127 | 59 | 104 | 202 | 105 | 94 | 139 | 162 |
| - les hebdomadaires | 6 | 4 | 9 | 11 | 10 | 30 | 22 | 12 | 21 | 29 |
| - les mensuels | 7 | 5 | 4 | 2 | 1 | 5 | 4 | 1 | 3 | 10 |
| - les médias audiovisuels | 3 | 3 | 3 | 16 | 13 | 21 | 7 | 17 | 24 | 18 |
| - Internet | | | | | | 49 | 36 | 51 | 52 | 58 |
| **(Total)** | **32** | **79** | **143** | **88** | **128** | **307** | **174** | **175** | **239** | **277** |

# 7 Annexes

## *Avis à l'égard du projet de loi n°6612 relatif 1) au titre d'artiste, 2) aux mesures sociales au bénéfice des artistes professionnels indépendants et des intermittents du spectacle, 3) à la promotion de la création artistique*

Délibération n°69/2014
du 24 mars 2014

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 Madame la Ministre de la Culture en date du 29 octobre 2013, la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet du projet de loi n°6612 relatif 1) au titre d'artiste, 2) aux mesures sociales au bénéfice des artistes professionnels indépendants et des intermittents du spectacle, 3) à la promotion de la création artistique, déposé à la Chambre des Députés comme projet de loi n°6612 en date du 12 septembre 2013.

La Commission nationale limite ses observations aux questions traitant des aspects portant sur la protection des données, soulevées plus particulièrement par l'article 15 du projet de loi sous examen.

L'objectif principal du projet de loi est d'adapter aux réalités vécues par les artistes et intermittents du spectacle, la loi modifiée du 30 juillet 1999 concernant a) le statut de l'artiste professionnel indépendant et l'intermittent du spectacle, b) la promotion de la création artistique. En particulier, il est suggéré d'adopter des modifications de cette loi à cinq niveaux : l'introduction d'un titre d'artiste, l'introduction de règles spécifiques en faveur des jeunes artistes diplômés, la modification des conditions de résidence et de lieu de travail pour les artistes professionnels indépendants respectivement les intermittents du spectacle, des mesures en faveur de la professionnalisation des artistes professionnels indépendants, et enfin la prise en compte des congés de maladie, de maternité et parental.

Dans le cadre du traitement des demandes d'admission au titre d'artiste (article 5), au bénéfice des aides à caractère social en faveur des artistes professionnels indépendants (article 6), ou au bénéfice d'une indemnisation en cas d'inactivité involontaire


des intermittents du spectacle (article 7), l'article 15 du projet de loi sous objet prévoit que le Ministre de la Culture et les agents de son département ministériel nommément désignés par lui ont accès direct, par un système informatique, (1) au registre général des personnes physiques et morales créé par la loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales, (2) au fichier relatif aux affiliations des salariés, des indépendants et des employeurs géré par le Centre commun de la sécurité sociale sur base de l'article 413 du Code de la sécurité sociale, à l'exclusion de toutes données relatives à la santé, et (3) au fichier relatif aux demandeurs d'emploi inscrits et relatif aux bénéficiaires du revenu minimum garanti.

Suivant le commentaire des articles joint au projet de loi, l'accès direct à ces différents fichiers répond à un double objectif. D'un côté, le ministre doit pouvoir exercer un contrôle effectif concernant les demandes lui adressées au titre du projet de loi sous objet. De l'autre côté, il sera possible de répondre rapidement aux demandes relatives au titre d'artiste, des aides en faveur des artistes professionnels indépendants et des indemnités journalières des intermittents du spectacle.

Selon le principe de proportionnalité et de nécessité, tout traitement de données à caractère personnel doit être proportionné aux finalités à atteindre, compte tenu du risque que le traitement fait peser pour la vie privée des personnes concernées. Dans le cadre de l'analyse des principes de la nécessité et de la proportionnalité d'un traitement de données, la Commission nationale se doit de vérifier s'il n'existe pas de moyens alternatifs, moins intrusifs et moins attentatoires à la vie privée des personnes concernées, mais permettant d'arriver aux mêmes finalités. Cette vérification des moyens alternatifs résulte notamment de la jurisprudence de la Cour de Justice de l'Union Européenne qui exige que « *les moyens mis en œuvre (…) soient aptes à réaliser l'objectif visé et n'aillent pas au-delà de ce qui est nécessaire pour l'atteindre* »[1].

Il s'agit en effet d'éviter une prolifération des accès d'une administration aux fichiers d'une autre administration, si ces accès n'apparaissent pas comme proportionnés et nécessaires par rapport aux intérêts publics distincts qu'elles poursuivent.

Dans sa rédaction actuelle, l'article 15 du projet de loi sous objet permet l'accès par le Ministre de la culture et les agents de son département ministériel à des fichiers et registres d'autres administrations (en l'occurrence, le Centre des technologies de l'information de l'Etat, le Centre commun de la sécurité sociale, l'Administration de l'emploi et le Fonds national de solidarité) dont les missions publiques ne présentent a priori pas de lien direct avec celles du Ministre de la culture.

La Commission nationale comprend que cet accès direct du ministère de la culture aux fichiers ou registres d'autres administrations pourrait permettre d'atteindre la finalité envisagée par les auteurs du projet de loi, à savoir le double objectif de contrôle effectif et de réponse rapide des demandes. Cependant, un accès direct à un fichier d'une administration par une administration tierce laisse toujours courir un risque pour la vie privée des personnes concernées. Dans un souci de confidentialité et de sécurité des données au sens des articles 21 à 23 de la loi du 2 août 2002, il convient d'éviter tout risque d'abus ou de détournement de finalité.

Un des critères à prendre en compte en outre dans l'analyse du principe de proportionnalité et de nécessité est la proportion du nombre de personnes concernées par la mesure (les artistes et intermittents du spectacle) par rapport au nombre de personnes non concernées, mais dont les données seraient consultables par l'administration via un accès informatique.

En l'espèce, le nombre de personnes concernées par le

[1] Arrêt du 9 novembre 2010, Schecke et al., C-92/09 et C-93/09, point 74 et jurisprudence citée.

dispositif envisagé demeure très restreint, comme en attestent les chiffres mentionnés dans le rapport annuel du Ministère de la culture, par ailleurs évoqués dans l'avis du Conseil d'Etat[2]. L'article 15 du projet de loi sous objet, dans sa rédaction actuelle, permettrait un accès aux données contenues dans des fichiers ou registres concernant au contraire une partie très importante de la population (à savoir l'ensemble des salariés, indépendants et employeurs, ainsi que les bénéficiaires du revenu minimum garanti) voire l'ensemble de la population (dans le cas du registre général des personnes physiques et morales).

La Commission nationale estime dès lors que le principe de proportionnalité et de nécessité n'est pas respecté au regard des finalités envisagées.

Toutefois, la Commission nationale est à se demander s'il n'est pas envisageable d'adapter le mécanisme de l'accès prévu à l'article 15 du projet de loi sous objet, en prévoyant la mise en place d'une solution technique qui permettrait de garantir, d'un point de vue informatique, que les agents du ministère de la culture puissent seulement accéder aux données concernant les personnes qui ont introduit une demande au titre de l'article 5, 6 ou 7 du projet de loi sous objet, à l'exclusion des données relatives au reste de la population. En d'autres termes, seule l'ouverture d'un dossier administratif à l'occasion de l'introduction d'une telle demande ouvrirait aussi le droit pour ledit ministère d'accéder aux fichiers visés à l'article 15 et auxquels il n'aurait pas accès en l'absence de dossier.

La CNPD considère par ailleurs nécessaire d'insérer une mention informant la personne qui introduit sa demande au titre de l'article 5, 6 ou 7 du projet de loi sous objet que le ministère de la culture pourra accéder à des données la concernant figurant dans des fichiers d'autres administrations, et que la personne concernée dispose de la possibilité de s'opposer à un tel accès, auquel cas le ministère en question conservera toujours la possibilité de demander au requérant des certificats émanant des administrations concernées.

Ce n'est que sous ces conditions décrites ci-avant que la Commission nationale estime que le principe de proportionnalité et de nécessité serait respecté, et qu'elle ne verrait pas d'objection à ce que le ministère de la culture puisse accéder aux fichiers d'autres administrations.

Si par contre, cette solution n'apparaît pas techniquement envisageable ou nécessiterait des moyens déraisonnables pour pouvoir être mise en œuvre, la Commission nationale se rallie à la position du Conseil d'Etat. Celui-ci estime

[2] En 2012, 48 artistes, 135 intermittents du spectacle et 46 boursiers ont ainsi reçu une aide financière du Ministère de la culture.


qu' « *il convient d'éviter au maximum les interconnexions entre des bases de données personnelles établies par les administrations étatiques. Ceci pourrait se faire en demandant aux requérants d'aide d'inclure à leurs demandes, des certificats émanant de l'Administration de l'emploi, du Fonds national de solidarité et du Centre commun de la sécurité sociale* ». Cette solution éliminerait en effet les risques potentiels posés par un accès direct aux fichiers et registres d'autres administrations.

En tout état de cause, les finalités justifiant l'accès ou la consultation des fichiers et registres devront être suffisamment déterminées, explicites et légitimes, conformément à l'article 4 (1) (a) de la loi du 2 août 2002.

De même, les données devront être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées ultérieurement par le Ministère de la culture, au titre de l'article 4 (1) (b) de la même loi. Comme elle a déjà eu l'occasion de l'expliquer dans d'autres avis lui sollicités, la Commission nationale ne voit pas de problème particulier à ce que la loi, en l'occurrence le paragraphe (2) de l'article 15 du projet de loi sous objet, prévoie que les données soient davantage précisées dans un règlement grand-ducal. Cependant, ne disposant pas du projet dudit règlement grand-ducal, il lui est impossible d'apprécier et d'identifier les catégories de données en question.

Enfin, la Commission nationale propose de modifier la référence, au point 1 de l'article 15 (1) du projet de loi sous objet, à la loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales, au regard de l'adoption de la nouvelle loi du 19 juin 2013 relative à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité, aux registres communaux des personnes physiques.

Ainsi décidé à Esch-sur-Alzette en date du 24 mars 2014.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

## *Avis quant à la conformité de la loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection des personnes à l'égard du traitement des données dans le secteur des communications électroniques et des articles 67-1, 88-2 et 88-4 du Code d'instruction criminelle avec les exigences posées par l'arrêt du 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12 pour 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*

Délibération n°214/2014
du 13 mai 2014

Conformément à l'article 32 paragraphe (3) lettre (e) et (f) 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 de présenter au gouvernement toutes suggestions susceptibles d'améliorer le cadre légal et 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* ».

# 7 Annexes

Par lettre du 9 avril 2014, Monsieur le Ministre de la Justice a saisi la Commission nationale d'une demande d'examen de la conformité de la législation luxembourgeoise avec les exigences posées par la Cour de Justice de l'Union Européenne dans son arrêt du 8 avril dernier par lequel elle a invalidé la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données modifiant la directive 2002/58/CE.

Il y a lieu de rappeler en introduction que l'obligation de conservation des données de trafic et de localisation relatives aux communications électroniques a été introduite dans notre législation par la loi du 30 mai 2005 sur base de l'article 15 § 1er de la directive 2002/58/CE du 12 juillet 2002 qui permettait aux Etats membres d'introduire une telle mesure lorsqu'une telle limitation des principes prévus aux articles 5, 6, 8 et 9 constitue une mesure nécessaire appropriée et proportionnée au sein d'une société démocratique pour sauvegarder la sûreté de l'Etat, la défense et la sécurité publique. Il s'agit là d'une référence explicitée au 2ième paragraphe de l'article 8 de la Convention européenne de sauvegarde des Droits de l'Homme de 1950 et donc indirectement d'une réserve des droits fondamentaux prévus par la Charte, en particulier ceux visés par les articles 7 (vie privée) et 8 (données personnelles).

Après avoir ramené à 6 mois le délai de conservation initialement fixé à 12 mois (loi du 27 juillet 2007), le législateur a transposé la directive 2006/24/CE en modifiant la loi du 30 mai 2005 par les dispositions de la loi du 24 juillet 2010 assorties par ailleurs d'un règlement grand-ducal du même jour qui en a réglé les modalités d'application (déterminant les catégories de données visées).

Les modalités d'accès aux données font l'objet des dispositions des articles 67-1 (loi du 29 juillet 2010) et des articles 88-1 à 88-5 (loi du 30 mai 2005) du Code d'instruction criminelle.

La Commission nationale avait exprimé son appréciation et ses recommandations dans un avis relatif au projet de loi 6113 (n°85/2010) le 26 avril 2010.

L'analyse de l'arrêt du 8 avril 2014 fait apparaître avec force l'attachement de la haute juridiction aux principes consacrés par la Charte des droits fondamentaux de l'Union européenne, en particulier ses articles 7 et 8 qui prennent leur racine dans l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales [CEDH signée à Rome le 4 novembre 1950].


Le paragraphe 2 de l'article en question ci-dessus prévoit qu'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, entre autres, à la sécurité nationale, à la sûreté publique, à la défense l'ordre et à la prévention des infractions pénales, ou à la protection des droits et libertés d'autrui ».

Les juridictions nationales autrichiennes et irlandaises ont posé dans leurs décisions respectives la question préjudicielle de la validité de la directive 2006/24 à la lumière des articles 7 (« respect de la vie privée »), 8 (« protection des données à caractère personnel ») et 11 (« liberté d'expression ») de la Charte des droits fondamentaux de l'Union européenne.

La Cour retient en premier lieu la vaste ampleur et le caractère intrusif de l'ingérence dans l'exercice de ces droits fondamentaux que comporte l'obligation faite aux fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communication de conserver les données de trafic et de localisation des utilisateurs par la directive incriminée.

Nous n'estimons pas nécessaire d'évoquer plus amplement les motifs afférents retenus (couverture générale de toutes personnes et tous moyens de communication, sensibilité des données, sentiment de la population de surveillance massive et indépendante de toute suspicion, …) mais nous nous attachons dans la suite à examiner les conséquences que la Cour en a tiré.

Nous passerons dès lors en revue une à une les conditions de compatibilité exigées selon l'arrêt de la Cour pour une conformité avec le régime des droits fondamentaux de la Charte.

La CJUE a invalidé la directive mais non le principe même d'une rétention de données rendue obligatoire par des législations nationales. L'accent est mis dans ce cas sur un encadrement suffisamment restrictif de façon à limiter l'ingérence au minimum nécessaire et des conditions et modalités aptes à prévenir des abus.

Un écueil dans l'interprétation du sens de l'arrêt consisterait à notre avis à ne pas distinguer la validité de l'instrument juridique communautaire de celle d'une disposition nationale mettant en œuvre une « Vorratsdatenspeicherung ».

Certes notre législation nationale, comme celle des plus de 20 Etats membres disposant d'un régime de conservation de données de communications obligatoire pendant une durée limitée en vue de garantir l'accès aux autorités chargées des missions afférentes dans la prévention d'atteintes à la sécurité publique, sûreté de l'Etat et la répression de la criminalité grave, ne saurait être reconnue respectueuse des valeurs fondamentales de la Charte, si elle(s) ne prévoient pas les restrictions, précautions et garanties reconnues nécessaires dans les motifs de l'arrêt, mais il nous semble que les conditions dégagées dans l'examen de la validité de la directive ne s'appliquent pas toutes et cumulativement à une législation nationale donnée de la même façon que la Cour les a estimé nécessaires pour qu'une directive imposant la rétention des données dans toute l'Union soit reconnue valide (cf. 30[3]).

C'est la seule lecture qui permette à notre avis de ne pas voir une contradiction dans les développements relevant que la rétention des données s'applique à toutes personnes et tous moyens de communication sans différenciation suivant la probabilité d'un lien avec des infractions graves avec ceux mettant en évidence que la rétention obligatoire des données peut être considérée comme apte à réaliser l'objectif poursuivi (9, 50) reconnu comme intérêt général suffisamment fondamental pour justifier la mesure (44, 51), à condition que celle-ci soit précisément encadrée et s'opère dans les limites du strict nécessaire (46, 52), et avec

[3] Les numéros référencés entre parenthèses renvoient aux différents points de l'arrêt de la Cour commenté.

# Annexes

toutes les garanties qui l'entourent (54). La directive est invalidée compte tenu de la portée de l'ingérence dans les droits fondamentaux des personnes et l'absence de proportionnalité et de règles claires et suffisantes imposant des limites et mesures de sauvegarde.

Il convient donc de noter que la CJUE « a interdit d'obliger dans les conditions de la directive 2006/24 sans pour autant obliger l'Union à interdire aux Etats membres d'obliger à la rétention des données ».

Voyons donc une à une les conditions de validité qui devront être remplies par les lois nationales. Pour cela, il y a lieu de distinguer les conditions et garanties exigées pour encadrer l'obligation de conservation (A) d'une part, de celle nécessaire au niveau de l'accès aux données par les autorités d'autre part (B).

## A. Obligation de rétention des données

1) La constatation de la Cour que la directive ne fait aucune différenciation en fonction de l'objectif de lutte contre les infractions graves dans la définition de son champ d'application (qui couvre toutes personnes et tous moyens de communication (57)) sans requérir par ailleurs aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique (59) ne doit à notre avis être seulement comprise comme une critique de l'étendue excessive de la directive.

Si ces aspects devraient être considérés comme critères d'exclusion dans le contexte d'un régime légal national, le modèle de la rétention de données conservatoire devrait être considéré en soi comme répudié par la Cour et seul un schéma du type « quick freeze » serait conforme à son arrêt, ce qui n'est, dans l'interprétation communément admise, pas le cas.

Quant aux avantages et inconvénients respectifs de ces deux modèles alternatifs envisageables pour permettre aux autorités judiciaires et de sécurité publique d'avoir recours aux données générées dans le cadre des communications électroniques, nous aimerions donner à considérer que les données faisant l'objet de l'obligation de conservation actuellement en place au Luxembourg (catégories reprises au règlement grand-ducal du 24 juillet 2010) sont générées et traitées de toute façon dans les systèmes des fournisseurs de services et opérateurs de réseaux. Le Code d'instruction criminelle en permet l'accès aux autorités judiciaires sous réserve du respect des conditions afférentes.

Les données de trafic peuvent en effet être conservées sous


certaines conditions pendant une durée maximale de 6 mois par les fournisseurs de service pour leur servir aux besoins de la facturation, de l'établissement des décomptes de paiement d'interconnexion entre réseaux, des poursuites engagées en cas de non-paiement, des litiges et contestations non encore vidés, et des besoins techniques et de gestion du trafic (article 5 § 3 à 5 de la loi modifiée du 30 mai 2005).

Ce ne serait donc que pour des données que les opérateurs seraient amenés à effacer le cas échéant plus rapidement que la période de 6 mois d'obligation de conservation généralisée prévue aux articles 5 § 1 et 9 § 1 de ladite loi du 30 mai 2005 se révélerait plus attentatoire aux droits des personnes concernées qu'un système de quick freeze qui n'affecterait de façon ciblée que les données ponctuellement jugées nécessaires par le juge. Il appartiendrait dans cette hypothèse au gouvernement d'arbitrer entre ces deux systèmes en tenant encore compte d'autres facteurs non analysés ici.

Alors que la durée de conservation obligatoire en vue de la mise à disposition des données des autorités judiciaires n'est pas plus longue que celle pendant laquelle les opérateurs peuvent les conserver pour les besoins de la facturation, les risques engendrés par le régime légal luxembourgeois nous semblent proportionnés aux objectifs d'intérêt public poursuivis.

Par ailleurs la législation luxembourgeoise entoure l'obligation de conservation et l'accès aux données d'un certain nombre de restrictions et garanties qu'il nous semble plus important d'examiner une à une au niveau de leur conformité aux exigences de l'arrêt de la CJUE et de l'opportunité d'y apporter encore des améliorations.

2) Durée de conservation imposée par la loi

La Cour fédérale constitutionnelle allemande, dans son arrêt du 2 mars 2010, avait considéré qu'une durée de conservation non excessive au regard de la gravité de l'ingérence d'une rétention de données de communication devrait être inférieure à un an et qu'une durée de 6 mois pourrait être justifiée dans le respect du principe de proportionnalité.

Sur ce point la CJUE s'exprime moins clairement que la plus haute juridiction allemande parce qu'elle avait à statuer par rapport aux dispositions de la directive communautaire et non d'une législation nationale individuelle. Elle critique la fourchette prévue par le législateur communautaire (6 mois à 2 ans) et relève l'absence de critères objectifs et notamment d'une quelconque différenciation entre les catégories de données (63) ou selon les moyens de communications utilisés.

La Commission nationale estime en revanche qu'en appliquant une durée unitaire de 6 mois à l'ensemble des données faisant l'objet de l'obligation de conservation et des moyens de communication concernés, le législateur a efficacement minimisé les risques d'atteinte au respect de la vie privée et des données personnelles.

3) Défaut d'exceptions pour les personnes dont les communications sont soumises au secret professionnel

La loi luxembourgeoise ne prévoit pas d'exceptions en faveur de personnes dont le secret des communications bénéficierait d'une protection renforcée.

Il est à signaler toutefois que l'article 88-2 du Code d'instruction criminelle dispose à son paragraphe (5) que « les communications avec des personnes liées par le secret professionnel au sens de l'article 458 du Code pénal et non suspectées d'avoir elles-mêmes commis l'infraction, ou d'y avoir participé, ne pourront être utilisées. Leur enregistrement et leur transcription seront immédiatement détruits par le juge d'instruction. »

L'article 88-4 contient un paragraphe (3) d'une teneur

similaire applicable aux cas de surveillance des communications et correspondances à opérer pour le Service de renseignement de l'Etat.

Certes il s'agit dans un de ces cas d'une surveillance concernant également le contenu des communications et correspondances et non seulement des données de trafic (et de localisation) mais l'ajout d'une disposition analogue à l'article 67-1 serait sans doute de nature à répondre à l'exigence reflétée dans l'arrêt de la CJUE examiné d'exempter les données relatives aux communications de ces personnes.

La Commission nationale s'interroge en outre sur le point de savoir s'il ne faudrait pas étendre l'effet de cette exception aux communications des journalistes lorsque cela est nécessaire pour éviter une atteinte à la protection des sources dont ils bénéficient de par la loi dans l'exercice de leur activité professionnelle.

Nous sommes conscients que les mesures préconisées ci-dessus ne reviennent pas rigoureusement à exempter ces personnes de la conservation légalement obligatoire de leurs données de communication mais se limiteraient à en exclure l'accès et l'utilisation.

La Commission nationale estime pourtant que cette voie - bien plus facilement praticable - reviendrait à réduire de façon équivalente les conséquences pour la vie privée résultant de l'ingérence dans le secret de leurs communications électroniques des personnes visées par la CJUE au regard de la protection spéciale dont ils bénéficient dans les activités considérées.

4) Obligation de destruction à l'expiration de la durée de conservation légale

L'arrêt mentionne l'exigence que la législation impose la destruction irrémédiable des données à caractère personnel à la fin de la période de conservation obligatoire.

L'article 5, paragraphe 1er (b) de la loi modifiée du 30 mai 2005 prévoit effectivement « qu'après la période de conservation, le fournisseur de services ou l'opérateur est obligé d'effacer les données relatives au trafic concernant les abonnés et utilisateurs, ou les rendre anonymes ».

On peut donc à notre avis conclure que la législation luxembourgeoise est conforme sur ce point. Certes on pourrait s'interroger sur le point de savoir si la préservation des données permise en cas d'anonymisation ne constitue pas une entorse à l'exigence en question. Tout est ici une question d'interprétation du terme « anonymisation » (pour davantage de développements sur la distinction entre


pseudonymisation, données dépersonnalisées et données anonymes, cf. WP 05/2014 du Groupe de l'Art. 29, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf).

Des données rendues irréversiblement anonymes sont en effet à considérer comme en dehors du champ d'application de la protection des données selon la directive 95/46/CE (cf. aussi considérant 26 : données conservées sous une forme ne permettant plus l'identification de la personne concernée).

Au cas où le gouvernement voudrait néanmoins se prémunir de tout malentendu sur ce point, il conviendrait de proposer la suppression du bout de phrase « ou les rendre anonymes » dans les articles 5 et 9 de la loi modifiée du 30 mai 2005.

5) Obligation de conserver les données sur le territoire de l'Union européenne

La législation luxembourgeoise ne prévoit aucune limitation de la sorte. Le responsable du traitement pourrait donc théoriquement avoir recours à des moyens de traitements ou à des sous-traitants situés sur le territoire de pays-tiers reconnus offrir un niveau de protection adéquate ou les transmettre en dehors de l'UE dans les autres circonstances prévues à l'article 26 de la directive faisant échec au principe général d'interdiction de transfert de données personnelles de l'article 25. L'arrêt motive cette exigence (plus rigoureuse que celle prévue aux articles 25 et 26 de la directive 95/46/CE) par la nécessité de voir soumettre le traitement et la conservation de ces vastes quantités de données sensibles par une autorité de contrôle indépendante mettant en œuvre le droit européen de protection des libertés et droits fondamentaux. Il conviendrait donc de rajouter une limitation afférente aux articles 5-1 et 9-2 de la loi modifiée du 30 mai 2005 visée ci-haut.

6) Mesures techniques et d'organisation destinées à assurer la confidentialité et la sécurité des données conservées

L'article 5-1 de la loi du 30 mai 2005 renvoie aux articles 22 à 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 quant aux mesures de sécurité.

La CJUE pose des exigences plus strictes dans son arrêt du 8 avril.

La Commission nationale avait déjà dans son avis du 26 avril 2010 plaidé pour l'inscription dans la loi de l'obligation pour les fournisseurs de service et opérateurs de réseaux de prendre des mesures de protection spécifiques pour les données faisant l'objet de la rétention obligatoire et avait mentionné les mesures envisageables suivantes :

- 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.

7) Sanction des abus

La loi luxembourgeoise prévoit des sanctions pénales en cas d'accès non autorisé aux données retenues par les fournisseurs de service et opérateurs de réseaux. La CNPD avait suggéré dans son avis de 2010 sur le projet de loi 6113 d'inscrire en outre expressément dans le Code d'instruction criminelle la nullité de la preuve

obtenue moyennant un accès illicite ou un abus des données en question.

### B. Conditions d'accès aux données par les autorités

C'est à ce niveau que se situe à notre avis la nécessité la plus importante de modification de la législation luxembourgeoise pour la rendre conforme avec les exigences dégagées par la Cour en application des principes de proportionnalité et pour réduire l'ingérence dans l'exercice des droits individuels au strict minimum nécessaire.

1) Le seuil définissant les incriminations des faits pour lesquels l'article 67-1 du Code d'instruction criminelle (premier alinéa) permet l'accès aux données nous est déjà apparu en 2010 comme sensiblement trop bas pour correspondre à l'objectif fixé de prévention et poursuite de la criminalité grave et de la lutte contre le terrorisme et la criminalité internationale organisée (cf. point B.1. de l'avis de la CNPD du 26 avril 2010 sur le projet de loi 6113).

Elle préconise aussi de privilégier la voie de détermination d'un catalogue d'infractions plutôt que d'un seuil de peine d'emprisonnement prévu.

2) En revanche la législation luxembourgeoise prévoit d'ores et déjà un accès subordonné à une autorisation préalable du juge d'instruction (art. 67-1) et n'a pas à être modifiée et apparaît exemplaire en Europe à cet égard.

### Conclusion

Les autorités de protection des données européennes ont unanimement salué l'arrêt de la Cour de Justice de l'Union européenne, ce qui n'est pas étonnant puisque le G29 au sein duquel elles se coordonnent avait exprimé clairement l'appréciation dans son rapport sur les mises en œuvre nationales de la directive 2006/24[4] que la directive invalidée ne répondait pas à l'ensemble des exigences du droit européen de la protection des données. Une étude détaillée des textes de transposition nationale et de leur application pratique a mis en lumière une grande diversité de situations nationales, au niveau des durées de conservation prescrites, des services et données concrètes soumis à l'obligation de conservation, des autorités bénéficiant de l'accès à ces données et des conditions, modalités, de ces accès et du contrôle de la justification de ces accès et finalement des garanties établies en vue de la sécurité et confidentialité des données conservées ainsi que de la prévention et de la sanction d'éventuels abus.

Dans leurs réactions, nos collègues ne s'expriment

[4] WP 172/2010 Rapport sur le respect au niveau national par les fournisseurs de services de télécommunication et de services Internet des obligations découlant de la législation nationale sur la conservation des données de trafic http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf


guère quant à l'expectative de l'élaboration d'une réédition de la directive comportant des dispositions intégralement conformes aux exigences de l'arrêt par la Commission européenne. Il nous semble pourtant qu'une harmonisation serait souhaitable dans ce domaine, moins pour imposer une conservation obligatoire des données, mais pour que les conditions de celles-ci prévues dans les législations nationales soient conformes aux standards dégagés par la Cour et conformément à la Charte des droits fondamentaux de l'Union européenne.

La plupart des autorités nationales de protection des données sont engagées, pour ce qui les concerne, dans un travail d'analyse de la conformité de leur législation nationale, ou accompagnent un passage en revue initié par leurs autorités gouvernementales, en vue d'établir les modifications nécessaires à apporter aux règles nationales en place.

Aussi nous félicitons-nous d'avoir été consultés par le gouvernement et recommandons-nous vivement l'élaboration d'un projet de loi visant à amender les dispositions actuellement en vigueur sur les points évoqués ci-dessus, parmi lesquels la redéfinition de la condition correspondant à l'objectif de lutte contre la criminalité grave et organisée et le terrorisme par un critère plus approprié de qualification et d'incrimination des faits qui font l'objet de l'enquête, nous semble la plus importante.

Ainsi décidé à Esch-sur-Alzette en date du 13 mai 2014.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

### *Avis complémentaire relatif au projet de loi n°6566 facilitant l'échange transfrontalier d'informations concernant les infractions en matière de sécurité routière*

Délibération n°324/2014
du 14 juillet 2014

Conformément à l'article 32 paragraphe (3) lettre (e) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après désignée « la loi modifiée du 2 août 2002 »), la Commission nationale pour la protection des données 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 du Développement durable et des Infrastructures en date du 6 mai 2014, lui demandant d'aviser les amendements adoptés par la Commission parlementaire compétente au sujet du projet de loi n°6566, la Commission nationale expose ci-après ses réflexions et commentaires au sujet des amendements en question.

La CNPD a émis son premier avis relatif au projet de loi en question

en date du 25 juillet 2013. Elle limite dans le présent avis ses observations aux questions traitant des aspects portant sur la protection des données, soulevées plus particulièrement par l'amendement 6 portant sur l'article 7 initial (nouvel article 6).

Quant à la question de la suppression de toute référence à la décision-cadre 2008/977 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 et l'introduction d'un renvoi aux articles 24 à 32 de la décision 2008/615/JAI relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière, la CNPD se rapporte à prudence du Conseil d'Etat et plus particulièrement à son avis du 3 juin 2014.

Pour ce qui est de l'exercice du droit d'accès des personnes concernées auquel a trait le paragraphe 2 du nouvel article 6 en projet, la CNPD ne partage pas les arguments et explications fournis dans le commentaire de l'amendement 6 pour les raisons indiquées ci-après et maintient à cet égard ses propositions formulées dans son avis du 25 juillet 2013, à savoir l'organisation d'un accès direct en faveur des personnes concernées qui s'exerce directement auprès de la Police grand-ducale.

La solution envisagée par l'amendement sous examen maintient un droit d'accès indirect à exercer par l'intermédiaire de l'autorité de contrôle instituée par l'article 17 (2) de la loi modifiée du 2 août 2002. Comme nous l'avions déjà souligné dans notre premier avis du 25 juillet 2013, par exception au principe d'un droit d'accès direct tel que prévu à l'article 28 de la loi modifiée du 2 août 2002, dans le cadre d'un système d'accès indirect, la personne concernée ne reçoit pas de détail relatif à ses données, mais reçoit seulement l'information sommaire de la part de l'autorité de contrôle « article 17 » que les données personnelles traitées à son égard ne sont pas contraires à la loi.

Or, l'amendement sous examen prévoit bien, conformément à l'article 7 paragraphe 3 de la directive 2011/82/UE, que la personne concernée a le droit d'obtenir des informations détaillées sur le traitement de ses données. L'amendement introduit donc en réalité un droit d'accès direct, sauf que les informations relatives aux données traitées ne sont pas transmises à la personne concernée par la Police grand-ducale mais par l'autorité de contrôle « Article 17 ». Suivant le texte en projet, les demandes d'accès doivent être introduites auprès de l'autorité de contrôle « Article 17 » qui les continue à la Police grand-ducale ; cette dernière transmet ensuite les informations relatives aux


données traitées à l'autorité de contrôle qui les transmet à son tour à la personne concernée. L'autorité de contrôle servirait ainsi en quelque comme « boîte aux lettres » et « facteur ». La CNPD est à se demander quel est l'intérêt ou l'utilité de ce mécanisme bureaucratique qui n'apporte pas de valeur ajoutée et ne fait que rallonger le délai endéans lequel la personne concernée reçoit une réponse.

La CNPD donne par ailleurs à considérer que l'autorité de contrôle « Article 17 » risque fort probablement d'être confrontée au traitement d'un grand nombre de demande d'accès de ce type. Dans ce contexte, nous voudrions relever que l'autorité de contrôle, actuellement composée par le délégué du Procureur général d'Etat, à savoir le Procureur général d'Etat adjoint et par deux membres de la CNPD, ne dispose pas de ressources propres, ni financières, ni en personnel, de même que le règlement grand-ducal pourtant prévu à l'article 17 de la loi modifiée du 2 août 2002 n'a jamais été adopté. La rapport annuel portant sur l'année 2013 précise à ce sujet ce qui suit : *« Dans ses rapports antérieurs, l'autorité de contrôle avait considéré que « compte tenu de la charge croissante de travail, au niveau européen, mais aussi au niveau national avec l'entrée en vigueur de nouvelles réglementations en matière policière, … il serait indiqué d'adopter ce règlement à l'effet de créer un secrétariat à rattacher soit à la CNPD, soit au Parquet général, chargé des tâches administratives ». L'autorité de contrôle maintient ces considérations. Les demandes individuelles d'accès aux fichiers du service de renseignement dont l'autorité a été saisie depuis fin 2012 ont été gérées, pour l'essentiel, par le président avec l'assistance du secrétariat du parquet général. L'autorité a signalé, dans ses rapports antérieurs, que le Comité d'évaluation Schengen qui avait procédé au cours de la période fin 2008 – début 2009 à un contrôle du Luxembourg, avait souligné, dans son rapport du 7 mai 2009, la nécessité de doter l'autorité de contrôle des moyens financiers et en personnel nécessaires pour exécuter ses missions et d'adopter le règlement grand-ducal prévu à l'article 17 paragraphe (2) de la loi modifiée du 2 août 2002. Aucune suite n'a été réservée à cette recommandation du comité européen que l'autorité de contrôle a régulièrement rappelée dans ses rapports successifs. Une nouvelle évaluation Schengen est en cours ; les évaluateurs posent, encore, la question des moyens financiers et humains de l'autorité de contrôle ».* (voir rapport annuel de l'autorité de contrôle spécifique « Article 17 », point III., pages 4 et 5).

Quant à l'argument que le traitement des données tombant dans le champ d'application de la directive 2011/82/UE serait ainsi le pour lequel un accès direct serait organisé, la CNPD voudrait relever qu'une loi spéciale peut déroger à la loi générale.

Enfin, la Commission nationale réitère également sa proposition formulée dans son avis du 25 juillet 2013, à savoir de *« conférer au droit d'accès un certain automatisme en prévoyant notamment une information automatique à l'adresse des personnes concernées dès que la Police grand-ducale transmet des données à un autre Etat membre. Un tel mécanisme permettrait aux personnes concernées une transparence effective et un meilleur contrôle de leurs données et garantirait qu'un autre Etat membre ne puisse éventuellement abuser du système d'échange de données ».*

Ainsi décidé à Esch-sur-Alzette en date du 14 juillet 2014.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

# 7 Annexes

## *Avis à l'égard du projet de règlement grand-ducal déterminant les modèles de cartes d'identité pour les membres des Corps diplomatique et consulaire résident et les agents de l'Union européenne et des Organisations internationales ayant leur siège au Luxembourg*

Délibération n°325/2014
du 14 juillet 2014

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

Par courriel du 18 février 2014, la Direction du Protocole et de la Chancellerie du Ministère des Affaires étrangères et européennes, a invité la Commission nationale à aviser le projet de règlement grand-ducal déterminant les modèles de cartes d'identité pour les membres des Corps diplomatique et consulaire résidents et les agents de l'Union européenne et des Organisations internationales ayant leur siège au Luxembourg.

La Commission nationale limite ses observations aux questions traitant des aspects portant sur la protection des données, soulevées plus particulièrement par les articles ci-après dénommés pour les besoins du présent avis « 2A » et « 2B », alors que le projet de règlement grand-ducal sous examen contient deux articles portant le chiffre « 2 ».

L'un des objectifs principaux du projet de règlement grand-ducal consiste à préciser les données traitées par le Ministère des Affaires étrangères et appelées à figurer sur les cartes diplomatiques, de légitimation et consulaires (ci-après : « les cartes »), ainsi que dans un registre des cartes diplomatiques, de légitimation et consulaires, en application de la loi du 7 août 2012 relative à la carte d'identité pour les membres des Corps diplomatique et consulaire résident et les agents de l'Union européenne et des Organisations internationales ayant leur siège au Luxembourg (ci-après : « la loi du 7 août 2012 »).

Il convient de noter que la Commission nationale a accordé une autorisation en date du 13 décembre 2013 au Ministère des Affaires étrangères, Direction du Protocole, sur base de l'article 14 de la loi du 2 août 2002. Cette autorisation portait sur un traitement de données, y compris biométriques, ayant pour finalité la confection, la vérification technique et la délivrance de


cartes diplomatiques, de cartes de légitimation et de cartes consulaires, ainsi que la gestion administrative y afférente.

Le Ministère des Affaires étrangères désire poursuivre un tel traitement en inscrivant les conditions et modalités du traitement des données à caractère personnel dans un règlement grand-ducal.

Dans sa version actuelle, l'article 2A du projet de règlement grand-ducal sous objet détermine les catégories de données à caractère personnel contenues sur les cartes, alors que l'article 2B établi un registre des cartes qui contient certaines données présentes sur les cartes ainsi que des données supplémentaires.

La Commission nationale est à se demander s'il ne serait pas préférable de définir dans un premier article les finalités du traitement, les catégories des données traitées par le Ministère ainsi que les autres caractéristiques de traitement de données, pour ensuite indiquer dans un second article quelles sont parmi ces données collectées et utilisées celles qui sont appelées à être inscrites sur les cartes. En effet, le fichier (registre) qui sera créé servira de base pour la gestion des demandes de cartes ainsi que la confection des cartes.

Les finalités du traitement de données à caractère personnel sont définies à l'article 2B paragraphe (1) du projet de règlement grand-ducal. Il apparaît toutefois à la Commission nationale que les termes utilisés dans cet article se réfèrent davantage à des opérations de traitement plutôt qu'à des finalités au sens de la loi du 2 août 2002.

Il ressort en effet du projet de règlement grand-ducal sous examen que les finalités pour lesquelles le Ministère traite les données visées dans ledit projet sont, d'une part, la gestion des demandes ces cartes diplomatiques, des cartes de légitimation et des cartes consulaires, et d'autre part la confection et la délivrance de ces mêmes cartes.

Après avoir déterminé les finalités du traitement envisagé, la Commission nationale suggère d'énumérer l'ensemble des catégories de données contenues dans le fichier. Celles-ci se retrouvent déjà d'une part à l'article 2A, paragraphe (1), points 1 et 2, et à l'article 2B, paragraphe (1), alinéa 2, d'autre part.

Il peut être utile, comme c'est le cas dans la version actuelle du projet de règlement grand-ducal sous examen, de distinguer les données traitées selon leur provenance : certaines proviennent du registre national des personnes physiques, tandis que d'autres sont fournies par le demandeur.

La Commission nationale propose ainsi le libellé qui pourrait avoir la teneur suivante : « *Le Ministre ayant les Affaires étrangères et européennes dans ses attributions met en œuvre un traitement de données relatif à la carte d'identité pour les membres des Corps diplomatique et consulaire résident et les agents de l'Union européenne et des Organisations internationales ayant leur siège au Luxembourg. Le ministre a la qualité de responsable du traitement au sens de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.*

*Le traitement de données a pour finalités :*

- *la gestion administrative des demandes des cartes diplomatiques, des cartes de légitimation et des cartes consulaires,*

- *la confection, la vérification technique et la délivrance de ces cartes,*

- *de répertorier les cartes émises.*

*A cet effet, il est créé un fichier qui contient les données suivantes :*

- *en provenance du registre national des personnes physiques :*
*(…)*

- *fournies par le demandeur :*
*(…) ».*

# 7 Annexes

La catégorie de données visée sous le point d) du deuxième alinéa de l'article 2 paragraphe (1), *« des informations déclaratives supplémentaires provenant de la demande d'enrôlement »,* n'apparaît pas très précise : il pourrait être utile de détailler un peu plus le type d'informations collectées.

En ce qui concerne la date de validation de la carte pour ce qui concerne les cartes consulaires (article 2 paragraphe (2) alinéa 2 point e)), la Commission nationale se demande pourquoi cette information concerne seulement les cartes consulaires et non pas aussi les cartes diplomatiques et de légitimation.

Une autre disposition pourrait ensuite spécifier parmi les données contenues dans le fichier (registre) celles qui figurent sur les cartes. Ces informations apparaissent dans le projet de règlement grand-ducal sous objet, à l'article 2A paragraphe (1), respectivement à l'article 2B paragraphe (1) alinéa 2.

La Commission nationale suggère par ailleurs, pour des raisons de cohérence de terminologie avec la loi du 2 août 2002, de parler de « fichier » plutôt que de « registre » des cartes, la notion de « fichier de données à caractère personnel » étant définie à l'article 2 lettre (h) de la loi du 2 août 2002.

Concernant la durée de conservation des données à caractère personnel traitées par le Ministère, la CNPD note avec satisfaction que le paragraphe (3) de l'article 2A du projet de règlement grand-ducal sous objet précise que les données biométriques ne sont conservées que pendant une durée de deux mois après la délivrance d'une carte diplomatique, de légitimation ou consulaire et sont, à l'expiration de ce délai, automatiquement et irréversiblement supprimées. Cette durée correspond en effet à celle préconisée par la Commission nationale concernant les données biométriques dans son autorisation du 13 décembre 2013. Le renvoi aux lettres (i) et (j) de l'article 2 paragraphe (1) semble toutefois erroné, puisque la donnée biométrique concernée est la photographie numérisée du titulaire, listée à la lettre (h) du même paragraphe.

Par ailleurs, il pourrait être utile d'indiquer les durées de conservation des données à caractère personnel autres que biométriques. D'une manière générale, les données ne peuvent être conservées indéfiniment, selon l'article 4 paragraphe (1) lettre (d) de la loi du 2 août 2002. D'après cet article, les données ne doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des


finalités pour lesquelles elles sont collectées et traitées, dans ce cas la gestion des demandes, la confection et la délivrance des cartes diplomatiques, des cartes de légitimation et des cartes consulaires. La Commission nationale est d'avis que les données devraient être supprimées après un certain délai suivant le moment où les personnes concernées quittent la fonction qui leur donne droit à l'une de ces cartes.

Enfin, elle recommande de préciser davantage les modalités d'accès aux données présentes dans le fichier. En particulier, il est important que seules les personnes qui en ont besoin dans l'exercice de leur mission légale soient habilitées par le Ministre à y avoir accès.

Dans ce contexte, la CNPD estime également nécessaire de prévoir un système de journalisation des accès, ce qui constitue une garantie appropriée contre les risques d'abus. Ainsi, à l'instar d'autres lois ou règlements grand-ducaux pour lesquels l'avis de la Commission nationale avait été demandé, il conviendrait de rajouter une disposition qui pourrait avoir la teneur suivante : « *Le système informatique par lequel l'accès au fichier est opéré doit être aménagé de sorte que les informations relatives à la personne ayant procédé à la consultation, les informations consultées, la date, l'heure et la référence du dossier dans le cadre duquel la consultation a été effectuée, ainsi que le motif précis de la consultation puissent être retracés. Les données de journalisation doivent être conservées pendant un délai de trois ans à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle.* »

Ainsi décidé à Esch-sur-Alzette en date du 14 juillet 2014.

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°6410 portant modification de la loi du 4 juillet 2008 sur la jeunesse*

Délibération n°338/2014 du 21 juillet 2014

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 29 juillet 2013, le Ministère de la Famille et de l'Intégration a invité la Commission nationale à aviser le projet de loi n°6410 portant modification de la loi modifiée du 4 juillet 2008 sur la jeunesse.

La Commission nationale limite ses observations aux questions traitant des aspects portant sur la protection des données, soulevées plus particulièrement par l'article 29 du texte coordonné (comprenant les amendements gouvernementaux) du projet de loi sous objet.

# Annexes

Cet article a pour objet la création et l'exploitation d'un fichier de données à caractère personnel relatif à la gestion des demandes et du contrôle des paiements des chèques-service accueil dans le cadre de la loi du 4 juillet 2008 sur la jeunesse, appelée à être modifiée.

## 1) L'origine des données

La Commission nationale souhaite tout d'abord relever que la version actuelle de l'article 29 du projet de loi ne précise pas l'origine des données. Se pose en effet la question de savoir si toutes les données sont fournies par la personne qui introduit une demande de chèque-service accueil, ou si toutes les données sont fournies par d'autres administrations au Ministère de la Famille et de l'Intégration, ou bien si certaines données sont fournies par le demandeur et d'autres par des administrations.

Or, d'une part l'origine des données constitue un élément devant figurer obligatoirement dans toute demande d'autorisation préalable auprès de la Commission nationale, aux termes de l'article 14 paragraphe (2) lettre (d) de la loi du 2 août 2002. D'autre part, l'article 12 paragraphe (3) lettre (j) de cette même loi précise que pour être exempté de notification, les traitements de données à caractère personnel effectués par des autorités administratives doivent être « *soumis à des réglementations particulières adoptées par ou en vertu de la loi et réglementant l'accès aux données traitées ainsi que leur utilisation et leur obtention* ».
A cet égard, il conviendrait à notre avis que le texte sous avis précise l'origine des différentes catégories de données.

Dans l'hypothèse où les données seraient transmises par d'autres administrations, en l'occurrence via un accès aux fichiers de ces administrations par le ministère de la famille et de l'intégration, la Commission nationale estime nécessaire, à l'instar d'autres textes légaux pour lesquels son avis a été demandé, que soit prévue la mise en place d'une solution technique permettant de garantir, d'un point de vue informatique, que les agents du ministère de la famille puissent seulement accéder aux données concernant les personnes qui ont introduit une demande de chèques-service accueil, à l'exclusion des données relatives au reste de la population. En d'autres termes, seule l'ouverture d'un dossier administratif à l'occasion de l'introduction d'une telle demande ouvrirait aussi le droit pour ledit ministère d'accéder au fichier visé à l'article 29 paragraphe (2) et auquel il n'aurait pas accès en l'absence de dossier.

## 2) Les finalités du traitement des données

Pour ce qui est des finalités du traitement des données, la CNPD suggère à l'endroit de l'article


29 paragraphe (1) la formulation suivante : « en vue de la gestion et du suivi administratif, ainsi que du contrôle financier des dossiers de demandes de chèques-service accueil » (sous réserve d'autres finalités pour lesquelles un traitement du ministère pourrait avoir lieu, cf. infra, point 4, notre remarque concernant les catégories de données relatives au prestataire).

3) La présence réelle de l'enfant bénéficiaire dans la structure

En ce qui concerne l'article 29, paragraphe (2), lettre (e), comme le soulève également le Conseil d'Etat, la CNPD se pose la question de la nécessité pour le ministère de connaître la présence réelle de l'enfant bénéficiaire dans la structure. Il semble que cette information permette, le cas échéant, de constater d'éventuels abus. Si tel est le cas, il serait utile de le préciser, afin de pouvoir apprécier la nécessité et le caractère adéquat de cette information.

4) Les catégories de données relatives au prestataire

L'article 29 paragraphe (2), lettres (f) à (h), liste les catégories de données relatives aux prestataires, c'est-à-dire aux assistants parentaux, responsables du service d'accueil pour enfants, et personnel encadrant.

La Commission nationale comprend tout-à-fait que les données listées sous les lettres (f) à (h) puissent apparaître utiles et nécessaires au ministère de la famille et de l'intégration dans ses relations avec le prestataire. Elle se demande cependant quel est le lien de la collecte de ces données avec la finalité invoquée au paragraphe (1) de l'article 29, à savoir la gestion des demandes introduites dans le cadre du chèque-service accueil et du contrôle des paiements.

En ce sens, il y aurait lieu de rajouter une finalité supplémentaire au paragraphe (1), du type « gestion des prestataires des services d'accueil ».

En tout état de cause, la Commission nationale estime que la photo du personnel encadrant ne peut pas être collectée. La CNPD s'aligne à cet égard sur les commentaires du Conseil d'Etat dans son avis complémentaire du 6 mai 2014. La publication de photos paraît excessive et inadéquate au regard de la finalité invoquée, à savoir la gestion des demandes introduites et du contrôle des paiements, respectivement de la gestion des prestataires des services d'accueil (si une telle finalité était ajoutée au texte du projet de loi). Dans le même sens, la CNPD renvoie également à son avis du 26 juillet 2010 et à son avis complémentaire du 15 juin 2012 relatif au projet de loi n°6284 portant sur l'exploitation d'une base de données à caractère personnel relative aux élèves (délibération n°156/2012 du 15 juin 2012).

A l'exception de la photo, le traitement des catégories de données sous (f) à (h) se justifierait pour les besoins de gestion interne du ministère (ses relations avec les prestataires, etc.).

Or, le dernier alinéa du paragraphe (2) prévoit que les données visées sous les lettres (f) à (h) sont publiées dans un portail édité par le ministre. La CNPD ne voit pas en quoi une telle publication s'avère nécessaire aux fins de la gestion administrative et du suivi des dossiers de demandes des chèques-service accueil, respectivement de la gestion des prestataires des services d'accueil. S'il s'agit le cas échéant d'une nouvelle finalité, à savoir la gestion d'un portail internet à caractère informatif par le ministère, il y aurait lieu de le préciser également dans le texte de loi en projet.

Cependant, alors que la « qualification professionnelle » et la « langue parlée du personnel » pourraient se justifier dans le cadre des relations entre le ministère et les prestataires de services d'accueil, la CNPD se pose la question de la proportionnalité et de la nécessité de publier sur un portail accessible au grand public de telles données. Faut-il vraiment dévoiler au grand public quel

salarié de tel ou tel prestataire de service d'accueil dispose de quelle qualification et parle quelles langues ?

5) L'accès aux données

L'article 29 paragraphe (4) prévoit que « *l'accès [aux] données [par] des tiers ne peut avoir lieu que pour les besoins de la gestion, de la tenue, de la maintenance de la base des données (…)* ». La CNPD souhaite relever qu'au sens de l'article 2 (q) de la loi du 2 août 2002, le responsable du traitement (en l'espèce, le ministère), le sous-traitant (le SIGI respectivement les communes concernées) et les personnes qui, placés sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilités à traiter des données, ne sont pas à considérer comme des tiers. Or, en principe, ce sont ces acteurs qui interviennent dans le traitement des données visées à l'article 29 paragraphe (2) pour les besoins de la gestion, la tenue et la maintenance de la base des données.

De manière générale, les données ne peuvent pas être communiquées à des tiers ou accédées par des tiers. La Commission nationale ne comprend dès lors pas la raison d'être de la disposition selon laquelle « *la transmission de données à des tiers ne peut avoir lieu qu'avec l'accord du responsable du traitement et à la demande motivée adressée par le tiers au responsable du traitement* ». En effet, elle se demande pour quelle raison des tiers non autorisés pourraient recevoir communication des données, à moins que les auteurs du projet de loi précisent les finalités et les catégories de données pour lesquels une communication de données serait nécessaire.

Pour ce qui est de l'accès aux données par les agents du Ministère de la Famille et de l'Intégration, la Commission nationale recommande de préciser davantage les modalités d'accès aux données présentes dans le fichier. En particulier, il est important que seules les personnes qui en ont besoin dans l'exercice de leur fonction et de leurs tâches professionnelles soient habilitées par le Ministre à y avoir accès.

6) Traçage des accès

Dans ce contexte, la CNPD estime également nécessaire de prévoir un système de journalisation des accès, ce qui constitue une garantie appropriée contre les risques d'abus. Ainsi, à l'instar d'autres lois ou règlements grand-ducaux, il conviendrait de rajouter une disposition qui pourrait avoir la teneur suivante : « Le système informatique par lequel l'accès au fichier est opéré doit être aménagé de sorte que les informations relatives à la


personne ayant procédé à la consultation, les informations consultées, la date, l'heure et la référence du dossier dans le cadre duquel la consultation a été effectuée, ainsi que le motif précis de la consultation puissent être retracés. Les données de journalisation doivent être conservées pendant un délai de trois ans à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle».

7) La durée de conservation des données

En ce qui concerne la durée de conservation indiquée à l'article 29 paragraphe (5), la CNPD estime, à l'instar de l'avis complémentaire du Conseil d'Etat du 6 mai 2014, que celle-ci paraît excessivement longue par rapport aux finalités des traitements des données concernées. En effet, l'article 4 de la loi du 2 août 2002 prévoit que « *le responsable du traitement doit s'assurer que (…) [les] données sont (…) 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 (…)* ». Dès lors, il y aurait lieu de réduire cette durée de manière conséquente, ou à tout le moins de justifier la nécessité de conserver les données pour une durée aussi longue.

Ainsi décidé à Esch-sur-Alzette en date du 21 juillet 2014.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

*Avis à l'égard du projet de loi n°6542 portant introduction d'une subvention de loyer et modifiant la loi modifiée du 25 février 1979 concernant l'aide au logement*

Délibération n°339/2014
du 21 juillet 2014

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 du Logement en date du 8 février 2013, la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet du projet de loi « portant introduction d'une subvention de loyer et modifiant la loi modifiée du 25 février 1979 concernant l'aide au logement », déposé à la Chambre des Députés comme projet de loi n°6542 en date du 12 février 2013.

La Commission nationale limite ses observations aux questions

traitant des aspects portant sur la protection des données, soulevées plus particulièrement par l'article 14sexies du projet de loi sous examen.

L'objectif principal du projet de loi est l'introduction d'une subvention de loyer en faveur de ménages à faible revenu, afin de leur faciliter l'accessibilité à un logement du marché locatif privé ainsi que d'améliorer leurs conditions de logement. Il est proposé d'introduire cette nouvelle subvention en rajoutant deux nouveaux articles aux dispositions de la loi modifiée du 25 février 1979 concernant l'aide au logement. Alors que l'article 14*quinquies* retient le principe d'une telle subvention et précise sa formule de calcul et tous les critères, conditions et modalités relatifs à son obtention, l'article 14*sexies* prévoit un accès des agents du ministère du logement à certains fichiers d'autres administrations dans le cadre de demandes de subvention de loyer.

A la lecture de l'article 14sexies du projet de loi, il résulte que celui-ci prévoit également de manière implicite la création d'un fichier en vue de la gestion et du suivi administratif des dossiers des demandeurs d'une subvention de loyer.

La Commission nationale pour la protection des données estime que le principe de la tenue d'un tel fichier devrait aussi être précisé dans le texte du projet de loi, tandis que les modalités et conditions d'utilisation (catégories de données traitées, leur utilisation et leur obtention, etc.) pourraient être précisées dans un règlement grand-ducal.

Suivant le commentaire des articles du projet de loi, l'accès par l'administration du ministère du Logement à différents fichiers d'autres administrations est promu au vu de la simplification administrative substantielle et du gain de temps qu'il représente au profit de la population cible, mais aussi pour les services d'aide au logement.

Selon le principe de proportionnalité et de nécessité, tout traitement de données à caractère personnel doit être proportionné aux finalités à atteindre, compte tenu du risque que le traitement fait peser pour la vie privée des personnes concernées. Dans le cadre de l'analyse des principes de la nécessité et de la proportionnalité d'un traitement de données, la Commission nationale se doit de vérifier s'il n'existe pas de moyens alternatifs, moins intrusifs et moins attentatoires à la vie privée des personnes concernées, mais permettant d'arriver aux mêmes finalités. Cette vérification des moyens alternatifs résulte notamment de la jurisprudence de la Cour de Justice de l'Union Européenne qui exige que « les moyens mis en œuvre (…) soient aptes à réaliser l'objectif visé et


n'aillent pas au-delà de ce qui est nécessaire pour l'atteindre »[5].

Il s'agit en effet d'éviter une prolifération des accès d'une administration aux fichiers d'une autre administration, si ces accès n'apparaissent pas comme proportionnés et nécessaires par rapport aux intérêts publics distincts qu'elles poursuivent.

Dans sa rédaction actuelle, l'article 14*sexies* du projet de loi sous objet permet l'accès par le ou les gestionnaires du dossier du ministère du Logement aux fichiers issus du Centre commun de la sécurité sociale, de l'Administration des contributions directes et du Fonds national de sécurité, dont les missions publiques ne présentent a priori pas de lien direct avec celles du ministère du Logement.

La Commission nationale comprend que cet accès du ministère du Logement aux fichiers ou registres d'autres administrations pourrait permettre d'atteindre la finalité envisagée, à savoir l'objectif de simplification administrative et de gain de temps pour la population cible et pour les services d'aide au logement.

Cependant, cet objectif de simplification administrative doit être mis en balance avec le droit pour les personnes concernées à la protection de leur vie privée. Ce dernier élément constitue un droit fondamental consacré notamment par l'article 11 (3) de la Constitution, par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne ainsi que par l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales. Il s'agit donc de vérifier si cette balance des intérêts penche en faveur du droit fondamental au respect de la vie privée, qui protège l'intérêt des citoyens, ou en faveur de l'intérêt légitime de l'administration à la simplification de ses procédures, en tenant compte du critère de proportionnalité et de nécessité.

Un accès à un fichier d'une administration par une administration tierce laisse toujours courir un risque pour la vie privée des personnes concernées. Dans un souci de confidentialité et de sécurité des données au sens des articles 21 à 23 de la loi du 2 août 2002, il convient d'éviter tout risque d'abus ou de détournement de finalité.

Un des critères à prendre en compte en outre dans l'analyse du principe de proportionnalité et de nécessité est la proportion du nombre de personnes concernées par la mesure (les personnes bénéficiant de la subvention de loyer) par rapport au nombre de personnes non concernées, mais dont les données seraient consultables par l'administration via un accès aux fichiers d'autres administration en cas d'un réexamen du dossier.

En l'espèce, le nombre de personnes concernées par le dispositif envisagé en cas d'un réexamen du dossier demeure relativement restreint, puisqu'il s'agit des ménages qui présentent de façon cumulative les 3 caractéristiques suivantes : ils possèdent un faible revenu (ce qui est le cas d'environ 12440 ménages au Luxembourg selon les critères retenus par les auteurs de projet de loi), ils louent un logement sur le marché privé national, et leur taux d'effort consacré au paiement du loyer est supérieur à 33% de leur revenu net disponible.

L'article 14*sexies* du projet de loi sous objet, dans sa rédaction actuelle, permettrait un accès aux données contenues dans des fichiers concernant au contraire une partie très importante de la population (à savoir l'ensemble des salariés, indépendants et employeurs, ainsi que les bénéficiaires du revenu minimum garanti), voire toute la population (dans le cas du fichier de l'Administration des contributions directes)

La Commission nationale estime dès lors que le principe de proportionnalité et de nécessité n'est pas respecté au regard de la finalité envisagée.

Toutefois, la Commission nationale est à se demander s'il n'est pas envisageable d'adapter le mécanisme de l'accès prévu à l'article 14*sexies* du projet de loi

[5] Arrêt du 9 novembre 2010, Schecke et al., C-92/09 et C-93/09, point 74 et jurisprudence citée.

sous objet, en prévoyant la mise en place d'une solution technique qui permettrait de garantir, d'un point de vue informatique, que le ou les gestionnaires du dossier du ministère du Logement puissent seulement accéder aux données concernant les personnes qui ont introduit une demande au titre de l'article 14*quinquies* du projet de loi sous objet, à l'exclusion des données relatives au reste de la population. En d'autres termes, seule l'ouverture d'un dossier administratif à l'occasion de l'introduction d'une telle demande ouvrirait aussi le droit pour le ministère du Logement d'accéder aux fichiers visés à l'article 14sexies et auxquels il n'aurait pas accès en l'absence de dossier.

Ce n'est que sous cette condition que la Commission nationale estime que le principe de proportionnalité et de nécessité serait respecté, et qu'elle ne verrait pas d'objection à ce que le ministère du Logement puisse accéder aux fichiers d'autres administrations.

Si par contre, cette solution n'apparaît pas techniquement envisageable ou nécessiterait des moyens déraisonnables pour pouvoir être mise en œuvre, la Commission nationale se rallie à la position du Conseil d'Etat. Celui-ci estime que « *ces informations pourront être fournies par les ménages eux-mêmes, nul besoin n'existant pour instaurer un droit d'accès aux fichiers de diverses administrations au profit du service du ministère du Logement. (…) Si les auteurs entendent éviter des abus ou le risque de ne pas se voir remettre les renseignements demandés, il serait plus facile de demander aux personnes concernées de fournir les réponses dans un certain délai et de les informer que, faute d'obtention de ces renseignements, le versement de l'aide sera arrêtée jusqu'à obtention des renseignements utiles* ». Cette solution éliminerait en effet les risques potentiels posés par un accès aux fichiers d'autres administrations.

Dans l'hypothèse où un accès aux fichiers d'autres administrations serait mis en œuvre et sous réserve des observations ci-contre, la Commission nationale recommande de préciser davantage les modalités suivant lesquelles les agents du ministère du logement ont accès aux données. En particulier, il est important que seules les personnes qui en ont besoin dans l'exercice de leur fonction et de leurs tâches professionnelles soient habilitées par le Ministre à y avoir accès.

Dans ce contexte, la CNPD estime également nécessaire de prévoir un système de journalisation des accès, ce qui constitue une garantie appropriée contre les risques d'abus. Ainsi, à l'instar d'autres lois ou règlements grand-ducaux pour lesquels l'avis de la Commission nationale avait


été demandé, il conviendrait de rajouter une disposition qui pourrait avoir la teneur suivante : « Le système informatique par lequel l'accès au fichier est opéré doit être aménagé de sorte que les informations relatives à la personne ayant procédé à la consultation, les informations consultées, la date, l'heure et la référence du dossier dans le cadre duquel la consultation a été effectuée, ainsi que le motif précis de la consultation puissent être retracés. Les données de journalisation doivent être conservées pendant un délai de trois ans à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle».

Ainsi décidé à Esch-sur-Alzette en date du 21 juillet 2014.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

*Avis concernant le projet de loi n°6604 relatif au classement des établissements d'hébergement touristique*

Délibération n°352/2014 du 31 juillet 2014

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 » ou « la CNPD ») 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 11 juin 2013, le Ministère des Classes moyennes et du Tourisme a invité la Commission nationale à se prononcer au sujet des avant-projets (entretemps devenus projets) de loi et de règlement grand-ducal relatifs au classement des établissements d'hébergement touristique.

L'objectif du projet de loi et de règlement grand-ducal consiste à définir les différents types d'établissements d'hébergement touristique, à établir un système de classification ainsi qu'à détailler les modalités de classement voire de sanction de ces établissements.

A ces fins, le ministre tient un registre des établissements d'hébergement touristique. La tenue de ce registre ainsi que les possibilités pour le ministre de recourir à certaines catégories de données font l'objet d'un chapitre dédié du projet de loi *(« Chapitre 3 - Traitement de données nominatives »)*, qui comporte un article 13.

La Commission nationale limite ainsi ses observations aux questions traitant des aspects portant sur la protection des données, soulevées plus particulièrement par ledit article 13.

L'article 1er du texte sous examen précise que la loi en projet s'applique aux établissements d'hébergement touristique. De tels établissements sont pour la plus grande partie constitués sous forme de personne morale. Or, depuis la loi modificatrice du 27 juillet 2007, les données concernant des personnes morales ne tombent plus sous le champ d'application de la loi du 2 août 2002. L'application des dispositions légales en matière de protection des données se limite dès lors aux établissements exploités en nom personnel, ainsi qu'aux personnes physiques (gérantes d'établissements d'hébergement touristique par exemple) dont des données

personnelles seraient également traitées dans le cadre du projet de loi.

D'une manière générale, la Commission nationale suggère d'aligner la terminologie utilisée dans le cadre de l'article 13 du projet de loi sur les termes définis dans la loi du 2 août 2002. Dans cette optique, « traitement des données nominatives » deviendrait « traitement de données à caractère personnel », et « registre » deviendrait « fichier » ou « fichier de données à caractère personnel ».

La CNPD est à se demander s'il ne serait pas également préférable, pour des raisons de cohérence avec la loi du 2 août 2002, d'indiquer qu'un traitement de données à caractère personnel est mis en œuvre, et d'en définir le responsable du traitement (le ministre), les finalités (qui sont déjà reprises dans la version actuelle de l'article 13), les catégories de données à caractère personnel traitées ainsi que l'origine de ces dernières (qu'il y aurait lieu de préciser).

La Commission nationale propose ainsi le libellé qui pourrait avoir la teneur suivante : *« Le ministre met en œuvre un traitement de données relatif aux établissements d'hébergement touristique. Le ministre a la qualité de responsable du traitement au sens de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.*

*Le traitement de données a pour finalités :*

- *le traitement et le suivi de l'évaluation et du classement des établissements d'hébergement touristiques,*

- *la prise des décisions de classement, d'avertissement, de reclassement, de suspension, de refus ou de retrait du classement.*

*A cet effet, il est créé un fichier qui contient les données à caractère personnel suivantes :*

*(...) ».*

En ce qui concerne les catégories de données à caractère personnel traitées, les termes *« Dans ce registre figurent toutes les données qui sont nécessaires (...) »* de l'article 13 paragraphe (1) alinéa 2 ainsi que ceux utilisés à l'endroit du paragraphe (2) *« le ministre peut s'entourer de toutes les informations requises (...) »* sont beaucoup trop imprécis et ne permettent pas d'apprécier la nécessité et le caractère adéquat des données à caractère personnel traitées. La Commission nationale estime donc nécessaire de préciser dans le texte en projet les catégories de données collectées et utilisées.


La CNPD suggère également d'indiquer l'origine des données à caractère personnel traitées par le ministre. Il y aurait lieu de préciser si celles-ci proviennent des personnes concernées (gestionnaires d'établissements d'hébergement touristique) qui les fournissent au ministre sur demande, ou si le ministère a, le cas échéant, accès à certaines données des personnes concernées figurant dans des fichiers d'autres administrations.

Si ce dernier cas était envisagé, d'autres questions relatives à la protection des données se poseront, que la CNPD pourra apprécier le cas échéant lors d'éventuels amendements au projet de loi sous objet.

Enfin, il serait utile de prévoir une disposition réglant la durée de conservation des données à caractère personnel. Selon l'article 4 paragraphe (1) lettre (d) de la loi du 2 août 2002, celles-ci peuvent en effet seulement être « *conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées (…)* ».

Pour le surplus, la Commission nationale n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 31 juillet 2014.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

## *Avis à l'égard du projet de loi n°6675 1) portant organisation du Service de Renseignement de l'Etat; 2) modifiant certaines lois 3) abrogeant la loi du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat*

Délibération n°353/2014
du 31 juillet 2014

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 d'Etat en date du 2 avril 2014, la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet du projet de loi n°6675 1) portant organisation du Service de Renseignement de l'Etat; 2) modifiant la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'Etat, la loi du 31 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, le Code d'Instruction criminelle, la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, et la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité; 3) abrogeant la loi du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat. Ledit projet de loi a été déposé à la Chambre des Députés comme projet de loi n°6675 en date du 2 avril 2014.

La Commission nationale entend limiter ses observations aux questions traitant des aspects portant sur la protection des données, et plus particulièrement aux articles 3,4 et 5 du projet de loi.

Ad article 3

D'un côté, il est important de décrire les missions du SRE - et par là les finalités des traitements de données à caractère personnel qu'il effectue - de manière assez précise. En effet, plus les missions sont formulées de manière précise, plus le cercle des personnes susceptibles d'être concernées par les traitements de données effectués par le service de renseignement sera restreint. D'un autre côté, au regard de l'évolution des menaces que le SRE doit tenter d'anticiper et prévenir, une telle description ne peut pas être trop détaillée non plus. Dès lors, le bon fonctionnement des mécanismes de contrôle tels que prévus par le projet de loi joue un rôle d'autant plus crucial afin d'éviter des abus tels que constatés dans le passé récent.

En ce qui concerne plus particulièrement la notion d'« ingérence » (paragraphe (2) lettre a) ), la CNPD préférerait que le texte contienne une définition à l'image de l'article 8 de la *loi organique des services de renseignement et de sécurité* belge du 30 novembre 1998[6], texte qui a inspiré l'article 3 du projet de loi. Par ailleurs, la loi belge prend soin de définir toute une série de termes en vue de l'application de la loi. Ces définitions procurent une sécurité juridique à la loi permettant ainsi aux instances compétentes de contrôler les activités des services de renseignement de manière plus efficace. Dans cette optique de sécurité juridique, la CNPD est à se demander s'il ne serait pas utile que le législateur luxembourgeois définisse lui aussi certains termes de l'article 3.

Ad article 4

L'article 4 prévoit la coopération et la communication d'informations entre le SRE et d'autres autorités et institutions.

La Commission nationale estime que les communications

[6] http://www.ejustice.just.fgov.be/cgi_loi/loi_a1.pl?language=fr&la=F&cn=1998113032&table_name=loi&&caller=list&F&fromtab=loi&tri=dd+AS+RANK&rech=1&numero=1&sql=%28text+contains+%28%27%27%29%29#LNK0003


d'informations du SRE à certaines autorités et institutions sont inhérentes aux finalités mêmes d'un service de renseignement. Tel est le cas pour les communications de données à des autorités publiques dont les compétences coïncident avec les intérêts à protéger par le service de renseignement en vertu de l'article 3 du projet de loi.

En toute hypothèse, les communications de données à caractère personnel ne peuvent avoir lieu qu'à condition que le principe de proportionnalité soit respecté.

En ce qui concerne l'échange de données avec des autorités et services de renseignements étrangers et notamment avec ceux situés dans des pays qui ne sont pas membres de l'Union européenne, on peut se référer aux explications données par le groupe de travail « article 29 »[7] dans son « *Avis 04/2014 sur la surveillance des communications électroniques à des fins de renseignement et de sécurité nationale* »[8].

Sur la question de l'applicabilité du droit communautaire et des exceptions à cette applicabilité prévues en matière de questions relevant de la sécurité nationale, le groupe de travail a relevé ainsi ce qui suit : « *En fait, la dérogation au titre de la sécurité nationale susmentionnée ne s'applique qu'à la sécurité nationale d'un État membre de l'Union, et non à la sécurité nationale d'un pays tiers.* » (page 7)

Il recommande par ailleurs de « *veiller à ce que le cadre juridique national comporte des règles claires en matière de coopération et d'échange de données à caractère personnel avec les autorités répressives en vue de prévenir, de combattre et de poursuivre les infractions, y compris au niveau du transfert de ces données aux autorités d'autres États membres de l'Union et de pays tiers* ». (page 14)

Enfin, le groupe de travail estime que « *les accords de coopération secrets conclus entre les États membres et/ou des pays tiers ne satisfont pas aux critères de la Cour européenne des droits de l'homme définissant une base juridique claire et accessible.* » (page 17)

Ad article 5

L'article 5 paragraphe (1) alinéa 2 prévoit que les conditions et modalités du traitement des données à caractère personnel du SRE doivent être précisées dans un règlement grand-ducal. L'adoption de ce texte réglementaire est d'une importance cruciale d'un point de vue protection des données et sécurité juridique. Dès lors, il aurait été judicieux de joindre en même temps un projet de projet de règlement grand-ducal au projet de loi sous examen, d'autant plus qu'un tel règlement grand-ducal n'a jamais vu le jour sous l'empire de la loi actuelle du 15 juin 2004.

Il convient toutefois de relever qu'un avant-projet de règlement grand-ducal basé sur l'article 4 de la loi du 15 juin 2004 avait été soumis à la CNPD pour avis en date du 16 mai 2013 et avisé par elle en date du 28 juin 2013. Au moment du présent avis, elle ignore le stade procédural actuel de ce projet de texte, elle se demande cependant si cet avant-projet servira le cas échéant de base pour le futur règlement grand-ducal.

La CNPD note avec satisfaction que l'on s'est inspiré de l'article 48-24 du Code d'Instruction criminelle en ce qui concerne la traçabilité des accès prévue par le paragraphe (3) de l'article 5 du projet. En effet, une traçabilité des accès aux fichiers d'autres administrations permet d'éviter des abus, des accès trop nombreux ou sans raison valable et contribue ainsi au respect de l'obligation de n'accéder aux bases de données énumérées au paragraphe (2) que pour un motif précis, obligation prévue au paragraphe (3) alinéa 2 lettre a). La CNPD considère cependant que la loi devrait également prévoir que le système informatique par lequel l'accès direct est opéré doit être aménagé de sorte que le motif de la consultation puisse être retracé c'est-à-dire documenté

[7] Le groupe de travail a été établi en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 14 de la directive 97/66/CE.

[8] WP 215 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_fr.pdf

dans le système informatique, à l'instar de ce qui est prévu pour les procureurs, les membres des parquets et les membres du personnel de l'administration judiciaire par l'article 48-24 paragraphe (4) lettre (b) du Code d'Instruction criminelle et pour les officiers et agents de police judiciaire par l'article 34-1 de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la police.

Le système informatique de la Police mis en place pour effectuer les accès directs à certaines bases de données de l'Etat pourrait d'ailleurs servir d'exemple pour la mise en œuvre des exigences de la loi.

Pour le surplus, la CNPD n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 31 juillet 2014.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif


*Travail au niveau international*

*Documents adoptés par le groupe de travail « Article 29 » en 2014*

| Document | Date d'adoption | Référence |
|---|---|---|
| Working Document on surveillance of electronic communications for intelligence and national security purposes | 05.12.2014 | WP 228 |
| Déclaration commune des autorités européennes de protection des données au sein du Groupe de l'Article 29 | 26.11.2014 | WP 227 |
| Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on "Contractual clauses" Considered as compliant with the EC Model Clauses | 26.11.2014 | WP 226 |
| Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" c-131/121 | 26.11.2014 | WP 225 |
| Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting | 25.11.2014 | WP 224 |
| Opinion 8/2014 on the Recent Developments on the Internet of Things | 16.09.2014 | WP 223 |
| Statement on the results of the last JHS meeting | 17.09.2014 | WP 222 |
| Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU | 16.09.2014 | WP 221 |
| Statement on the ruling of the Court of Justice of the European Union (CJEU) which invalidates the Data Retention Directive | 01.08.2014 | WP 220 |
| Opinion 7/2014 on the protection of personal data in Quebec | 05.06.2014 | WP 219 |
| Statement on the role of a risk-based approach in data protection legal frameworks | 30.05.2014 | WP 218 |
| Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC | 09.04.2014 | WP 217 |
| Avis 05/2014 sur les Techniques d'anonymisation | 10.04.2014 | WP 216 |
| Avis 04/2014 sur la surveillance des communications électroniques à des fins de renseignement et de sécurité nationale | 10.04.2014 | WP 215 |
| Document de travail 01/2014 relatif au projet de clauses contractuelles ad hoc « sous-traitant établi dans l'UE à sous-traitant ultérieur établi hors de l'UE » | 21.03.2014 | WP 214 |
| Avis 03/2014 sur la notification des violations de données à caractère personnel | 25.03.2014 | WP 213 |
| Avis 02/2014 relatif à un référentiel des exigences pour les règles d'entreprise contraignantes soumises aux autorités nationales responsables de la protection des données dans l'UE et les règles transfrontalières de protection de la vie privée soumises aux agents de responsabilisation de l'APEC en matière de RTPVP | 27.02.2014 | WP 212 |
| Avis 01/2014 sur l'application des notions de nécessité et de proportionnalité et la protection des données dans le secteur répressif | 27.02.2014 | WP 211 |

Tous les documents de travail du groupe de travail « Article 29 » peuvent être téléchargés sur Internet[9].

[9] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/

CNPD

COMMISSION
NATIONALE
POUR LA
PROTECTION
DES DONNÉES

1, avenue du Rock'n'Roll - L-4361 Esch-sur-Alzette
Téléphone : +352 26 10 60-1 - Fax : +352 26 10 60-29
www.cnpd.lu