CNPD

COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Rapport annuel 2013

CNPD

COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Rapport annuel 2013

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 consiste 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 à travers :

- 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.

1 Avant-propos 8

2 Les activités en 2013 12

2.1 Supervision de l'application de la loi 14
- *2.1.1 Formalités préalables* 14
- *2.1.2 Transferts de données hors Union européenne* 17
- *2.1.3 Les chargés de la protection des données* 19
- *2.1.4 Demandes de vérification de licéité et plaintes* 20
- *2.1.5 Contrôles et investigations* 25
- *2.1.6 Secteur des communications électroniques* 28

2.2 Avis et recommandations 30
- *2.2.1 Le statut, les modalités de désignation et les attributions du médecin-coordinateur* 31
- *2.2.2 Projet de loi n°6394 portant approbation de différents accords en matière de coopération transfrontalière* 33
- *2.2.3 La réforme de la législation sur la fonction publique* 34
- *2.2.4 L'organisation du Service de Renseignement de l'Etat* 35
- *2.2.5 La réforme de l'exécution des peines et de l'administration pénitentiaire* 37
- *2.2.6 Règlementation de l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales* 39
- *2.2.7 Echange transfrontalier d'informations sur les infractions en matière de sécurité routière* 40
- *2.2.8 Organisation du centre socio-éducatif de l'Etat* 41
- *2.2.9 Modalités du comptage de l'énergie électrique et du gaz naturel* 42
- *2.2.10 Règlement interne du Registre National du Cancer* 43

2.3 Information du public 45
- *2.3.1 Actions de sensibilisation du public* 45
- *2.3.2 Reflets de l'activité de la Commission nationale dans la presse* 46
- *2.3.3 Outil de communication : le site Internet* 47
- *2.3.4 Formations et conférences* 47

2.4 Conseil et guidance 50
- *2.4.1 Concertation avec les organisations représentatives sectorielles, les principaux acteurs économiques, l'Etat et les organismes publics* 50
- *2.4.2 Demandes de renseignements* 51

2.5 Recherche 53

Table des matières

2.6 Participation aux travaux européens 53
2.6.1 *Le groupe « Article 29 »* 54
2.6.2 *Comité consultatif de la Convention 108 du Conseil de l'Europe (T-PD)* 64
2.6.3 *Le « Groupe de Berlin »* 65
2.6.4 *Le séminaire européen « Case Handling Workshop »* 68
2.6.5 *Conférence Internationale des commissaires à la protection des données* 68
2.6.6 *Conférence de printemps des autorités européennes à la protection des données* 69
2.6.7 *Conférence de l'Association francophone des autorités à la protection des données* 70
2.6.8 *Révision des lignes directrices de l'OCDE sur la vie privée* 70
2.6.9 *La CNPD devient membre du Global Privacy Enforcement Network (GPEN)* 71

3 Les temps forts de 2013 72
3.1 Conférence de M. Dean Spielmann à l'occasion des 10 ans de la CNPD 72
3.2 Validation de la charte BCR du groupe « ArcelorMittal » 77
3.3 L'AFCDP s'adresse aux chargés de la protection des données 78
3.4 Analyse détaillée du contrat des services de Microsoft 80
3.5 Privacy Impact Assessment : accompagnement du GIE Luxmetering dans la mise en place des compteurs intelligents 80
3.6 Prospection électorale et protection des données 82

4 Perspectives 84

5 Ressources, structures et fonctionnement 88
5.1 Rapport de gestion relatif aux comptes de l'exercice 2013 88
5.2 Personnel et services 90
5.3 Organigramme de la Commission nationale 91

6 La Commission nationale en chiffres 92

7 Annexes
Avis et décisions
- Avis concernant le projet de règlement grand-ducal relatif au statut, aux modalités de désignation et aux attributions du médecin-coordinateur (Délibération n°28/2013 du 7 février 2013) 94

- Avis relatif au projet de loi n°6394 portant approbation : de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg, le Gouvernement du Royaume de Belgique, le Gouvernement de la République fédérale d'Allemagne et le Gouvernement de la

République française, concernant la mise en place et l'exploitation d'un centre commun de coopération policière et douanière dans la zone frontalière commune, signé à Luxembourg, le 24 octobre 2008 ; de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République française relatif à la coopération dans leurs zones frontalières entre les autorités de police et les autorités douanières, signé à Luxembourg, le 15 octobre 2001
(Délibération n°178/2013 du 19 avril 2013) 99

- Avis au sujet des projets de loi relatifs à la réforme dans la Fonction Publique en particulier des dispositions ayant trait à la protection des données comprises dans le projet de loi n°6457
(Délibération n°265/2013 du 14 juin 2013) 101

- Avis relatif à l'avant-projet de règlement grand-ducal pris en exécution de l'article 4 de la loi modifiée du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat et à l'avant-projet de règlement grand-ducal pris en exécution de l'article 23 de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité
(Délibération n°274/2013 du 28 juin 2013) 105

- Avis relatif au projet de loi n°6381 portant réforme de l'exécution des peines, au projet de loi n°6382 portant réforme de l'administration pénitentiaire et au projet de règlement grand-ducal portant organisation des régimes internes des établissements pénitentiaires
(Délibération n°302/2013 du 5 juillet 2013) 113

- Avis relatif à l'avant-projet de règlement grand-ducal portant création des traitements de données à caractère personnel nécessaires à l'exécution de l'article 32 de la loi du 2 septembre 2011 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu' à certaines professions libérales
(Délibération n°345/2013 du 12 juillet 2013) 117

- Avis relatif au projet de loi n°6566 facilitant l'échange transfrontalier d'informations concernant les infractions en matière de sécurité routière
(Délibération n°385/2013 du 25 juillet 2013) 121

- Avis relatif au projet de loi n°6593 portant modification de la loi du 16 juin 2004 portant réorganisation du centre socio-éducatif de l'Etat et de diverses autres lois et au projet de règlement grand-ducal portant organisation de l'unité de sécurité du centre socio-éducatif de l'Etat
(Délibération n°385/2013 du 25 juillet 2013) 125

Table des matières

- Avis relatif au projet de règlement grand-ducal relatif aux modalités du comptage de l'énergie électrique et du gaz naturel (Délibération n°566/2013 du 13 décembre 2013) 130

- Avis relatif au règlement interne du Registre National du Cancer (Délibération n°606/2013 du 23 décembre 2013) 135

Participations aux travaux internationaux

- Documents adoptés par le groupe de travail européen « Article 29 » en 2013 140

- Groupe de travail européen « Article 29 »: Document de travail 02/2013 énonçant des lignes directrices sur le recueil du consentement pour le dépôt de cookies 141

- Groupe de travail européen « Article 29 » : Avis 01/2013 apportant une contribution supplémentaire aux discussions sur la proposition de directive relative à la protection des données traitées dans les domaines de la police et de la justice pénale 147

- International Working Group on Data Protection in Telecommunications: Working Paper on Privacy and Aerial Surveillance 154

- International Working Group Data Protection in Telecommunications: Working Paper on the Human Right to Telecommunications Secrecy 159

- International Working Group Data Protection in Telecommunications: Working Paper on Web Tracking and Privacy 160

Discours

- La protection des données dans la jurisprudence de la Cour européenne des droits de l'homme - Discours du Président Dean Spielmann (Cour européenne des droits de l'homme) prononcé lors de la célébration du 10e anniversaire de la Commission nationale pour la protection des données à Esch/Belval le 28 janvier 2013 169

Factory A
Factory B
Factory C

1 Avant-propos

Le collège :
Pierre WEIMERSKIRCH, Gérard LOMMEL, Thierry LALLEMANG

Au cours des dernières années, la sensibilité des citoyens européens aux questions de protection des données s'est nettement accrue : 74% des Européens considèrent que la communication d'informations personnelles prend une part de plus en plus grande dans la vie moderne. Le Luxembourg n'est pas une exception. Cette évolution se manifeste non seulement dans les travaux de la CNPD, mais se retrouve aussi au niveau du gouvernement et de l'opinion publique.

L'augmentation considérable des plaintes (+33% par rapport à 2012) et des demandes de renseignement (+22% par rapport à 2012) adressées à la CNPD témoigne de l'intérêt croissant des citoyens pour la protection de leur sphère privée. Les nombreuses réunions avec les acteurs des secteurs privé et public reflètent leur besoin d'être accompagnés

dans leurs démarches de mise en conformité.

Les questions relatives à la protection de la vie privée sont évoquées de manière détaillée dans le programme gouvernemental. Le phénomène du « Big Data », la conservation des données (« Vorratsdatenspeicherung »), E-Santé et le dossier de soins partagé, le cloud computing ou encore la cyber security y ont été abordés. L'avis de la CNPD est par ailleurs de plus en plus demandé dans le contexte des projets de loi ou mesures réglementaires. En 2013, elle a notamment pris position par rapport aux sujets suivants : l'organisation du Service de Renseignement de l'Etat, le statut, les modalités de désignation et les attributions du médecin-coordinateur, la réforme de la fonction publique, la réforme de l'exécution des peines et de l'administration pénitentiaire, l'échange transfrontalier d'informations concernant les infractions en matière de sécurité routière et le registre national du cancer.

Au niveau européen, la directive 1995/46/CE sur la protection des données est en cours de révision depuis janvier 2012 : il s'agit de conférer au cadre juridique européen l'effectivité nécessaire et de tenir compte de l'émergence des nouvelles technologies et de la globalisation, qui ont modifié en profondeur la manière dont les données sont collectées et utilisées. Même si les dispositions du projet de règlement européen, qui remplacera cette directive, subiront encore certaines modifications plus ou moins profondes, les points centraux de la réforme ne manqueront pas d'exiger de la part de tous les acteurs un effort d'adaptation non négligeable face à la nouvelle approche moins bureaucratique, mais plus exigeante pour tous les acteurs.

Ceci vaut tant pour les entreprises et organisations du secteur privé que pour les organismes publics, qui devraient se préparer au cours des deux prochaines années à cette conduite préventive et responsable qu'on attend dorénavant des « data controllers » et que ces derniers doivent adopter à l'égard des données à caractère personnel qu'ils collectent, sauvegardent dans des fichiers, utilisent et transmettent le cas échéant à des tiers.

« Accountability » signifiera pour eux bien davantage que de s'acquitter des formalités déclaratives et de respecter leurs obligations légales ainsi que les restrictions prévues le cas échéant dans les autorisations émises par la CNPD pour les traitements susceptibles d'engendrer des risques particuliers.

Le fait de devoir fournir la preuve que les mesures requises en interne pour assurer le respect des droits des individus dont ils traitent les données dans une optique de « Privacy by design » ont été prises, nécessitera une méthodologie d'analyse et d'évaluation des risques et une compétence d'identification des solutions reconnues conformes aux exigences de la protection des données, dont l'expérience manque encore largement aux acteurs.

Pouvoir les conseiller et les orienter dans cette délicate démarche est ce qu'ils demanderont légitimement à l'autorité de surveillance. C'est donc à un développement de l'activité de guidance que notre équipe entend se préparer dans les prochains mois, tout comme à l'extension de sa capacité d'investigation et de contrôle.

Les outils et mécanismes innovateurs qui seront introduits par le futur règlement européen (PIA, codes de conduite sectoriels, BCR, certificats de conformité etc.) accompagneront l'évolution vers un comportement autoresponsabe des acteurs.

C'est dans une optique d'anticipation de la future approche légale que la CNPD a décidé d'accompagner l'analyse des enjeux de protection de

la vie privée face aux futurs compteurs d'énergie intelligents (« smart metering ») à travers un dialogue avec les responsables des ministères compétents, fournisseurs et exploitants de réseau (gaz et électricité). Un exercice semblable sera mené en collaboration avec l'agence eSanté au sujet du futur dossier électronique (dossier de soins partagé) du patient, en collaboration avec le Ministère de la Santé et la CNS.

Le facteur décisif de progrès résidera néanmoins dans le développement d'une culture de la protection des données au sein même des entreprises et organisations privées ainsi que des organismes publics. Un rôle prépondérant reviendra à cet égard aux dirigeants et aux juristes, « compliance officer », responsables des systèmes informatiques et technologies de communication et aux consultants et avocats qui les conseillent.

A cet égard la Commission nationale se félicite particulièrement de la constitution fin 2013 de l'Association pour la protection des données au Luxembourg et du succès rencontré par ses premières activités. Comme les chargés de la protection des données, ces professionnels avisés joueront un rôle indispensable pour permettre aux organisations de se préparer à satisfaire aux attentes de la future législation.

La confiance des utilisateurs s'en trouvera renforcée et représentera un atout de compétitivité non négligeable pour des secteurs de pointe de notre économie.

La nouvelle approche régulatrice apportera aussi son lot de transformations dans l'activité de la CNPD qui est consciente qu'elle devra être à la hauteur de l'attente des citoyens et ne devra pas ménager ses efforts d'information du public au sujet des règles de la protection des données. Un rapport récent de l'Agence des droits fondamentaux de l'Union européenne encourage la Commission à miser sur un renforcement du rôle des autorités de contrôle, une clarification des droits individuels et une facilitation des voies de recours pour permettre aux citoyens d'invoquer et, si nécessaire, de faire respecter leurs droits fondamentaux de protection des données.

La modernisation du cadre légal vient à point nommé pour que ces droits ne soient pas perçus comme purement théoriques et inadaptés à l'ère numérique et à notre vie connectée, à l'aube de « l'Internet des objets » et du Big Data. Réussir la modernisation de la protection des données est essentiel pour

Le siège de la CNPD à Belval

le futur marché unique du numérique, pour la compétitivité et la capacité d'innovation des entreprises européennes. Elle devra rétablir la confiance du public ébranlée par PRISM et les nouvelles répétées concernant des pannes de sécurité et d'accès aux données personnelles à l'insu ou contre la volonté des concernés.

Luxembourg, le 25 avril 2014

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

2

Les activités en 2013

L'année 2013 en un coup d'œil

Janvier
28 - La CNPD participe à la Journée de la protection des données et fête son 10e anniversaire avec une conférence de M. Dean Spielmann, Président de la Cour Européenne des Droits de l'Homme

Février
1 - La CNPD valide la charte « BCR » du groupe ArcelorMittal en tant qu'autorité chef de file
7 - La CNPD émet son avis sur le projet de règlement grand-ducal relatif au statut, aux modalités de désignation et aux attributions du médecin-coordinateur
7 - La CNPD participe à la table ronde *„Wéi ass meng Foto hei geland?"* dans le cadre du Safer Internet Day

Mars
12 - Les chargés de la protection des données se réunissent à Luxembourg à l'occasion d'une conférence de l'AFCDP

Avril
19 - La CNPD émet son avis sur le projet de loi n°6394 portant approbation de différents accords en matière de coopération transfrontalière
25 - La CNPD intervient à la conférence ISACA avec le thème *« Accountability for Data Protection »*

Mai
16-17 - La CNPD participe à la conférence de printemps des autorités européennes à la protection des données à Lisbonne

Juin
14 - La CNPD émet son avis au sujet des projets de loi relatifs aux réformes dans la fonction publique
28 - La CNPD se prononce sur l'organisation du Service de Renseignement de l'Etat

Juillet
5 - La CNPD émet son avis sur le projet de loi n°6381 portant réforme de l'exécution des peines et sur le projet de loi n°6382 portant réforme de l'administration pénitentiaire
11 - L'OCDE présente une version révisée de ses lignes directrices sur la protection de la vie privée et les flux transfrontières de données à caractère personnel
12 - La CNPD émet son avis sur l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales
26 - La CNPD émet son avis sur le projet de loi n°6566 sur l'échange transfrontalier d'informations concernant les infractions en matière de sécurité routière dans lequel elle appelle à une transposition adéquate de la décision-cadre 2008/977/JAI relative à la protection des données traitées dans le cadre de la coopération policière et judiciaire en matière pénale
26 - La CNPD émet son avis sur la réorganisation du centre socio-éducatif de l'Etat et sur l'organisation de l'unité de sécurité du centre en question

DELIBERATIONS

606
Délibérations adoptées
(+63% par rapport à 2012)

10
Avis relatifs à des projets ou propositions de loi ou mesures réglementaires

20
Agréments pour les chargés de la protection des données

FORMALITES PREALABLES

1072
Notifications reçues

833
Demandes d'autorisation

6559
Déclarants (depuis 2002)

DEMANDES DE RENSEIGNEMENT

2077
Demandes
(+22% par rapport à 2012)

PLAINTES ET INVESTIGATIONS

177
Plaintes
(+33% par rapport à 2012)

26
Investigations

VIOLATIONS DE DONNEES (COMMUNICATIONS ELECTRONIQUES)

1
Notification

Août

11 - L'Uruguay devient le premier Etat non européen à adhérer à la « Convention 108 » pour la protection des données à caractère personnel

Septembre

11 - La CNPD participe à une table ronde, organisée par l'Université du Luxembourg en coopération avec la Ville d'Esch, intitulée « *Prism - lutte antiterroriste, sauvegarde de la sphère privée et protection des intérêts économiques sont-ils compatibles ?* »

19 - La CNPD participe à la conférence « *Classification des banques de données de l'Etat* » du Cyber Security Board

23-26 - La CNPD participe à la conférence internationale des commissaires à la protection des données et de la vie privée à Varsovie

Octobre

2-3 - La CNPD participe au 25e Case Handling Workshop à Sarajevo

Novembre

18-21 - La CNPD participe à une formation sur la sécurité de l'information dans la commune de Differdange, organisée par CASES

Décembre

1 - La CNPD devient membre du Global Privacy Enforcement Network (GPEN)

13 - La CNPD émet son avis sur le projet de règlement grand-ducal relatif aux modalités de comptage de l'énergie électrique et du gaz naturel

23 - La CNPD émet son avis relatif au règlement interne du Registre National du Cancer

2 Les activités en 2013

Le travail de la Commission nationale pendant l'année 2013 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 20.713. En tout, 6.559 déclarants/responsables se sont ainsi conformés aux devoirs de déclaration imposés par la loi.

Le projet de règlement européen sur la protection des données, présenté par la Commission européenne le 25 janvier 2012, 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.

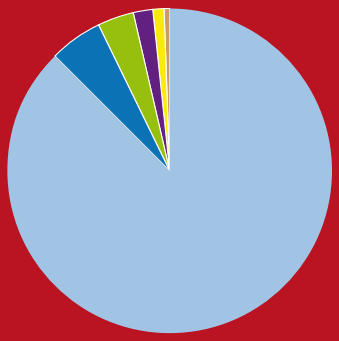
En 2013, 1.072 traitements ont été notifiés à la Commission nationale, ce qui représente une augmentation importante par rapport à l'année précédente. La raison principale de cette augmentation est le nombre important d'engagements formels de conformité que la CNPD a reçus dans le contexte des élections sociales de 2013. Au total, elle en a reçu 651.

En effet, la loi prévoit, à côté des notifications ordinaires, une forme simplifiée de notification (« notification unique »). Cette

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

Catégories des demandes d'autorisation



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 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 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.

Parmi les 421 notifications ordinaires, 75% proviennent d'acteurs du secteur privé. Les finalités déclarées le plus souvent dans ces notifications étaient l'administration du personnel et la gestion des ressources humaines. 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.

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.

2 Les activités en 2013

Le registre public

La loi prescrit la tenue d'un registre public par la CNPD. 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
- ceux qui, soumis à autorisation préalable, n'ont pas été autorisés.

La CNPD a reçu 833 demandes d'autorisation en 2013 (contre 706 en 2012). Elle n'a jamais reçu autant de demandes en une année depuis sa création.

Plus de 70% des demandes concernent l'exploitation de caméras de surveillance.
Les demandes concernant la géolocalisation de véhicules et de personnes continuent à augmenter, tandis que celles concernant la surveillance des conversations téléphoniques et des outils restent à un niveau constant.

En plus des demandes d'autorisation, la Commission nationale a reçu 149 engagements formels de conformité en 2013.
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 en dehors 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 95/46/CE ou disposant d'une législation propre reconnue adéquate), elle devra demander une autorisation préalable à la CNPD.

Mais, il existe 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[1] : 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 2013, la Commission nationale a été saisie de 85 demandes d'autorisation en vue du transfert de données vers des pays tiers. Ce chiffre représente une nette augmentation 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 et l'Inde.

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 spectaculaire 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

[1] 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 2013

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. 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.

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 « 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 ».

En 2013, la charte du groupe ArcelorMittal a été validée par les 25 autres autorités impliquées des Etats membres où le groupe est implanté[2]. La CNPD avait passé en revue de façon approfondie cette charte en tant qu'autorité chef de file (« lead authority »). En 2009, elle avait déjà gagné de l'expérience dans ce domaine en prenant le rôle de chef de file dans l'examen de la charte « BCR » du groupe eBay. Actuellement, elle est en train d'analyser la charte d'un autre groupe international avec siège à Luxembourg.

La Commission nationale a par ailleurs analysé et approuvé les règles d'entreprise contraignantes concernant 19 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, le 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 de ses 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, 81 entreprises, associations et organismes publics ont désigné un chargé de la protection des données. A la fin de l'année 2013, 105 personnes physiques ou morales étaient agréées pour exercer l'activité de chargé de la protection des données.

[2] Voir partie 3.2.

Les activités en 2013

2.1.4 Demandes de vérification de licéité et plaintes

Le nombre de citoyens faisant appel à la CNPD lorsqu'ils estiment qu'il y a violation de la loi ou entrave à l'exercice de leurs droits continue à augmenter. En 2013, la Commission nationale a reçu un nombre record de 177 plaintes et demandes de vérification de licéité.

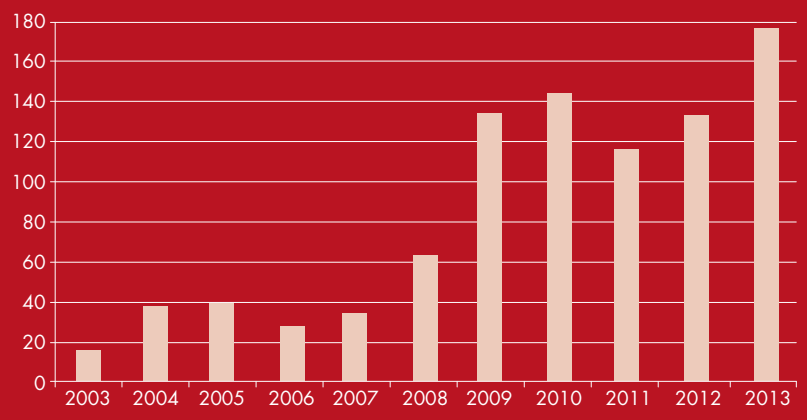
Dans les deux tiers des cas, les plaintes proviennent d'autres Etats membres de l'Union européenne, soit par l'intermédiaire des autorités de protection des données qui agissent au nom de leurs propres citoyens, soit directement par les ressortissants étrangers. Cela est notamment dû à la présence de nombreuses sociétés multinationales ayant choisi d'établir leur siège européen à Luxembourg (eBay, PayPal, Skype, Microsoft, Amazon …) et pour lesquelles la CNPD est l'autorité compétente pour assurer le respect de la législation nationale en matière de protection des données. Dans 62% des cas, les entreprises visées par les plaintes sont celles offrant des services sur Internet.

Un quart des plaintes concerne des demandes d'effacement ou de rectification de données qui n'ont pas été respectées. Cela inclut toutes les plaintes relatives à des demandes de clôture de comptes auprès des commerces ou des services en ligne, à des demandes d'effacement de données (données clients, données de candidature, données bancaires, etc.) ou encore les cas dans lesquels les plaignants demandent l'assistance de la CNPD pour rectifier leurs données après une transmission erronée de données à des tiers (contrats, livraisons, documents, etc.).

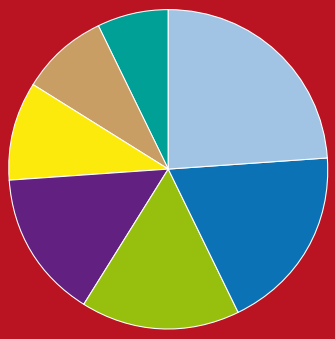
Dans beaucoup de cas (19%), les plaignants ont demandé à la CNPD de vérifier la licéité de certaines pratiques administratives ou commerciales. En dehors des nombreuses demandes qui remettent en cause les conditions générales de certains commerces, d'autres cas de figure de l'année 2013 concernaient par exemple : la collecte disproportionnée de données par un garagiste, la collecte des copies des titres d'identité par un service en ligne ou encore la publication d'une brochure par une commune avec des informations personnelles des résidents (voir encadré page 22).

Un autre motif souvent invoqué par les plaignants est le refus qui leur est opposé, l'absence de réponse ou l'insuffisance des informations en matière d'accès à leurs données (17%). Dans ces cas, la Commission nationale a dû intervenir pour faire valoir leurs droits auprès des différents responsables du traitement. A ce titre, les fermetures respectivement

Evolution du nombre de plaintes



Motif des plaintes



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'ils ne comprennent pas toujours les raisons pour lesquelles le statut de leur compte a changé.

Fait également l'objet de plaintes récurrentes la transmission de données à des tiers non autorisés (15%). En effet, comme tous les ans, la Commission nationale a été saisie de nombreuses plaintes concernant la publication de données sur Internet (voir encadré page 23).

Reviennent aussi régulièrement les plaintes concernant l'envoi de courriels confidentiels, mais distribués de façon collective et visible à tous les destinataires (« CC » au lieu de « BCC »).

L'année 2013 était par ailleurs marquée par le scandale NSA/PRISM, qui a fait l'objet de plusieurs demandes auprès de la CNPD (voir encadré page 23).

Par ailleurs, la Commission nationale est régulièrement saisie par des citoyens ayant des difficultés à faire valoir leur droit d'opposition à la prospection ou qui estiment n'avoir jamais consenti à voir leur données utilisées pour être prospectés via des communications électroniques. La Commission nationale a dû intervenir notamment 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 pour prospecter lesdits plaignants.

Les activités en 2013

Distribution d'une brochure avec des informations personnelles des résidents

La Commission nationale a été saisie de plusieurs plaintes concernant la distribution, par une administration communale, d'une brochure destinée à l'entièreté des ménages qui contenait en effet une liste des différentes localités de la commune, les noms des rues, les codes postaux et les numéros des maisons avec les noms et prénoms des résidents afférents.

La loi ne permet pas à un responsable du traitement de communiquer des données à caractère personnel à un tiers non autorisé et encore moins de divulguer ces données à un large public. En l'espèce, la Commission nationale a estimé que l'utilisation du fichier de la population pour communiquer et divulguer les noms et adresses de tous ses résidents indistinctement à toute la population de la commune est incompatible avec la finalité pour laquelle les données ont été collectées initialement par la commune, à savoir la tenue du fichier permettant d'administrer la population de la commune.

Elle a donc demandé à la commune en question de cesser cette pratique pour l'avenir alors qu'elle n'était pas conforme à la loi sur la protection des données. Par ailleurs, elle a suggéré aux administrations communales de prendre connaissance de la décision n°2/2010 du 15 janvier 2010 dans laquelle elle a défini les modalités des traitements de données à caractère personnel mises en œuvre par les communes du Grand-Duché de Luxembourg dans le cadre de l'exercice des missions qui leur sont conférées.

Cette décision énumère, entre autres, les destinataires ou catégories de destinataires auxquels les données détenues par les communes peuvent être communiquées.

Effacement de groupes sur Facebook après intervention de la CNPD

La Commission nationale a reçu plusieurs plaintes concernant deux groupes luxembourgeois sur Facebook, par l'intermédiaire desquels les membres publiaient des photos de voitures mal stationnées ou en stationnement interdit. Or, sur la plupart des photos, les plaques d'immatriculation des voitures n'étaient pas floutées ou masquées.

La CNPD a informé les administrateurs et les utilisateurs de ces groupes que les plaques d'immatriculation sont considérées par la loi comme étant des données à caractère personnel et qu'une telle publication est interdite.

Les utilisateurs des deux groupes ayant continué à publier des photos de voitures avec des plaques d'immatriculation non floutées, la CNPD a décidé de s'adresser directement à la société Facebook en lui demandant de fermer les groupes en question et d'exiger de la part des administrateurs de ne plus ouvrir de groupes similaires à l'avenir.

La société Facebook a fait droit à la demande de la CNPD et a fermé les pages des groupes. Par ailleurs, une nouvelle violation par les administrateurs résultera dans la désactivation définitive de leurs comptes.

Affaire « PRISM » : pas de violation constatée en matière de protection des données de la part de Skype et Microsoft au Luxembourg

Plusieurs entreprises, parmi lesquelles Google, Yahoo, Microsoft, Apple et AOL, ont été soupçonnées en juin 2013 d'avoir ouvert leurs serveurs informatiques à la National Security Agency (NSA), l'une des principales agences américaines de renseignements, facilitant la surveillance d'e-mails, de chats, de photos, vidéos et d'autres données stockées par des millions d'internautes dans le monde. Deux enquêtes simultanées publiées dans les journaux Guardian et Washington Post ont révélé ces accusations d'espionnage massif des communications sur Internet. Si les autorités américaines ont déjà reconnu l'existence de ce programme appelé « Prism », les sociétés concernées ont fermement rejeté les accusations de collaboration active, sauf celle requise par la législation en vigueur.

Cette affaire a d'ailleurs mené au dépôt de deux demandes de vérification de licéité auprès de la CNPD qui visaient les sociétés Skype Communications s.à r.l. et Microsoft Luxembourg s.à r.l. En date du 15 novembre 2013, la CNPD a informé les requérants des résultats de l'examen de leurs demandes relatives au respect de leurs droits et libertés fondamentaux à l'égard de traitements de données par lesdites sociétés.

A l'issue de son enquête et recherche sur les faits conduite à partir de juillet 2013 et de son analyse détaillée subséquente, la CNPD a statué ne disposer d'aucun élément permettant de conclure à un transfert massif de données de la part des deux entreprises basées au Luxembourg à la National Security Agency (NSA). Par ailleurs, il s'est avéré que le transfert de certaines catégories de données vers les entreprises affiliées aux Etats-Unis, tel qu'il est établi dans les politiques de confidentialité des services en ligne des deux entreprises mises en cause, s'opérait légalement, conformément aux clauses contractuelles acceptées par leurs utilisateurs et aux règles applicables de la décision d'adéquation 2000/520/CE de la Commission européenne mettant en œuvre l'accord « Safe Harbor » conclu entre l'Union Européenne et les Etats-Unis d'Amérique.

Par conséquent, la CNPD n'a pas pu constater de violation des dispositions de la législation sur la protection des données à caractère personnel, ni par Skype Communications s.à r.l., ni par Microsoft Luxembourg s.à r.l.

Par ailleurs, dans une deuxième lettre du 29 novembre 2013, la CNPD a fourni aux requérants des clarifications complémentaires quant à la portée de ses constatations.

En réponse à la question de savoir si la CNPD est parvenue à confirmer ou infirmer l'existence du programme PRISM et l'accès par la NSA aux données personnelles des utilisateurs de Skype et d'autres services en ligne de Microsoft, la Commission nationale a expliqué qu'en tant qu'autorité de contrôle, elle surveille le respect de la protection des données au Grand-Duché et que le périmètre de sa recherche se limitait donc forcément aux activités de Skype Communications s.à r.l. et de Microsoft Luxembourg s.à r.l.. En dehors de sa juridiction, il n'appartient pas à la CNPD d'enquêter, de sorte que ses conclusions ne sont pas de nature à confirmer ou réfuter l'existence des programmes de surveillance massive d'Internet de la part des services secrets comme PRISM, ni à exclure que les systèmes de Microsoft ou de Skype puissent avoir été accédés dans ce contexte, notamment aux Etats-Unis. Toutefois, la Commission nationale n'a décelé aucun indice dont on aurait pu déduire que Skype ou Microsoft concédaient un accès aux données personnelles des utilisateurs de leurs services en ligne, ou fournissaient des données en dehors des injonctions ponctuelles leur soumises conformément aux législations nationales applicables dans le domaine répressif et de la sécurité publique.

La CNPD a donc estimé que les sociétés sous investigation n'auraient pu être frappées de sanctions qu'en présence d'éléments concrets indiquant une violation de leurs obligations légales, et qu'une suspension des transferts de données vers les Etats-Unis basés sur le dispositif Safe Harbor était inconcevable en l'absence de preuves matérielles ou d'indices constatés laissant présumer un transfert massif de données.

En outre, la Commission nationale a estimé que les exceptions prévues pour l'accès par les autorités répressives et de sécurité nationale stipulées dans l'accord « Safe Harbor » passé en 2000 entre la Commission européenne et les autorités américaines, ne légitimaient pas en soi une surveillance massive des communications et du trafic Internet.

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 et d'intervention 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 »).

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 dans un but de prévention. Elle a effectué un total de 26 contrôles et investigations en 2013, que ce soit dans le cadre de la vidéosurveillance, de la surveillance sur le lieu du travail ou encore lorsqu'elle a pris connaissance (par elle-même ou par une notification) d'une attaque informatique ou d'une faille de sécurité.

Outre les tractations menées avec Microsoft dans le cadre du passage en revue décidé par le G29 et opéré conjointement avec nos collègues de la CNIL française concernant les questions de protection de données des utilisateurs européens des services en ligne du groupe en application de son contrat de services (voir partie 3.4), les investigations auprès d'Amazon portant sur l'organisation et le déroulement effectif des différents traitements de données personnelles effectués par le groupe en Europe et chez Skype dans le contexte des plaintes reçues en juin 2013 (voir partie 2.1.4.), les cas suivants illustrent les investigations opérées par la CNPD.

2.1.5.1 Prise d'images panoramiques à des fins de mesurage

La Commission nationale avait été saisie de plaintes de résidents préoccupés concernant la prise d'images panoramiques, par des voitures spécialement équipées à cet effet, à l'intérieur de plusieurs communes luxembourgeoises. Dans le cadre de sa mission de vérifier s'il y a effectivement eu atteinte à la vie privée des résidents, la CNPD a été informée que ces images géoréférencées sont proposées et vendues par une société néerlandaise à certaines communes du Grand-Duché qui s'en serviront à des fins de mesurage/gestion du territoire, etc. et que, dans aucun cas, l'accès à ces images ne sera mis à la disposition du public. Les visages des personnes se trouvant sur les photos et les plaques d'immatriculation des voitures sont masqués par défaut par ladite société.

La Commission nationale a informé les responsables des communes concernées que l'utilisation de ces photos pour la réalisation des finalités susmentionnées constitue un traitement de données à caractère personnel et a donc demandé aux communes de vérifier si la finalité envisagée du traitement de données rentre dans le cadre des traitements de données à caractère personnel mis en œuvre par les communes du Grand-Duché de Luxembourg, énumérés par la Commission nationale dans sa décision du 15 janvier 2010 (délibération n°2/2010). Par ailleurs, afin de respecter les droits que la loi confère aux citoyens, elle a rappelé aux communes d'informer leurs résidents du traitement envisagé, conformément à l'article 26 de la loi (p.ex. affichage au « *Reider* », publication dans le « *Buet* », etc.).

Comme le traitement de données de cette entreprise tombe sous la législation d'un autre pays européen, la CNPD a également contacté l'autorité de contrôle de ce pays notamment pour être informé des mesures de sécurité implémentées par ladite entreprise en ce qui concerne les résidents luxembourgeois.

2.1.5.2 Faille de sécurité d'une société offrant des services de télévision payante

L'autorité de protection des données tchèque avait reçu une plainte selon laquelle les données à caractère personnel

(noms, prénoms, adresses, adresses e-mail) de nombreux clients tchèques d'une entreprise établie au Luxembourg offrant des services de télévision payante ont pu être accédées par des tiers. Celle-ci a immédiatement signalé cette importante faille de sécurité à la Commission nationale. La Commission nationale a demandé à l'entreprise de procéder d'urgence à la vérification de son système informatique et de prendre dans les meilleurs délais toutes les mesures nécessaires, afin de rendre impossible un accès non autorisé aux données personnelles et d'assurer la sécurité et la confidentialité des données clients.

L'entreprise en cause a implémenté immédiatement les mesures de sécurité nécessaires, et elle a envoyé un rapport détaillé de l'incident à la CNPD.

2.1.5.3 Faille technique sur le site « ekb.lu »

La Commission nationale avait appris par les médias qu'un élève avait pu accéder, via le site Internet « ekb.lu », à l'ensemble des noms, prénoms, matricules et identifiants de tous les élèves et professeurs de son école.

Alors que cet incident semble avoir traduit des insuffisances quant au respect des mesures de sécurité et de confidentialité des données prévues aux articles 22 et 23 de la loi modifiée du 2 août 2002, la Commission nationale a noté avec satisfaction que des mesures appropriées ont immédiatement été prises afin d'y remédier. Ceci étant, elle a demandé au Ministère de l'Education Nationale et de la Formation Professionnelle de l'informer des raisons exactes de cet incident et des mesures de sécurité en vigueur.

Dans le cadre de cette enquête, la Commission nationale a constaté plusieurs manquements. Elle a notamment demandé à ne pas mettre en ligne un service dont la structure technique et les mesures de sécurité afférentes sont encore en phase de développement. Par ailleurs, elle a demandé au prédit Ministère de mettre en œuvre une authentification forte avant la mise à disposition du service. Etant donné que des données concernant les absences/présences, les excuses, les remarques et les sanctions disciplinaires des élèves y sont traitées, la divulgation de telles informations ou un accès non autorisé à ces données pourrait entraîner un préjudice important pour les personnes concernées. Pour cette raison, la Commission nationale a considéré qu'une authentification de type identifiant/mot de passe est insuffisante d'un point de vue sécurité pour ce type de dossier.

Finalement, la CNPD a demandé au Ministère de mettre en œuvre un audit de sécurité incluant

un test de pénétration effectué par une entité spécialisée et indépendante et, le cas échéant, les actions correctrices nécessaires avant la mise en ligne du service.

2.1.5.4 Attaque informatique sur un site Internet dédié à une étude scientifique

La presse ayant relaté une attaque informatique par déni de service sur le site Internet d'un centre de recherche dédié à une étude à laquelle participait un panel de 80.000 personnes, la CNPD a demandé des éclaircissements aux responsables.

La CNPD a notamment demandé des précisions quant aux mesures de sécurité prises par le centre de recherche pour éviter l'accès non autorisé à des données personnelles et assurer la confidentialité de la transmission sur Internet des informations personnelles des citoyens concernés.

Après analyse du CIRCL, le centre de recherche a pu confirmer qu'il ne s'agissait pas d'une attaque telle qu'évoquée par la presse et qu'aucune donnée à caractère personnel n'a été perdue. Il a par ailleurs répondu de manière satisfaisante aux questions de la CNPD.

2.1.5.5 Vidéosurveillance

Caméras filmant les propriétés avoisinantes ou la voie publique

En raison des quelques 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 de son 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, mais 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 suggère, de façon générale, de dénoncer ces installations de vidéosurveillance à la police ou au Parquet. En effet, contrairement à la CNPD, les autorités judiciaires ont la possibilité de procéder à des perquisitions.

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

Violation de sécurité de Numéricable

Le 25 juillet 2013, la Commission nationale a prononcé un avertissement à l'encontre de la société Coditel (Numéricable). En effet, ladite société a failli, conformément à l'article 3 paragraphe (3) alinéa 1 de la loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques, de notifier « sans retard » une violation de données à caractère personnel à la Commission nationale.

En l'espèce, la base de données des prospects (dont certains sont devenus clients) traitée par Numéricable a été la cible d'un piratage informatique. Par la suite, les auteurs dudit piratage ont publié les données à caractère personnel des personnes concernées sur Internet. Dès qu'elle a eu connaissance de l'affaire, la Commission nationale a demandé une prompte prise de position de la société Numéricable et la remise d'une notification de violation des données à caractère personnel.

Il résulte de ladite notification que la société Coditel a :

- mis en œuvre des mesures techniques pour corriger

le problème et protéger les données à caractère personnel,

- informé les personnes concernées par la violation de données à caractère personnel.

La Commission nationale a soulevé par ailleurs qu'en cas de manquement répété, elle peut prononcer une amende d'ordre qui ne peut excéder 50.000 euros.

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. 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 transfèrent 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 2013, des informations ont été transmises aux autorités compétentes (Police judiciaire et Justice) dans 1445 cas. Dans 800 cas, les demandes de données n'ont pas pu être satisfaites. Au total, les autorités compétentes ont fait 2245 demandes auprès des opérateurs. Ce chiffre reste stable par rapport à l'année 2012, où 2346 demandes ont été faites.

Les activités en 2013

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 2013, la Commission nationale a émis 10 avis dans le cadre de projets de loi ou de règlements grand-ducaux :

1. Avis concernant le projet de règlement grand-ducal relatif au statut, aux modalités de désignation et aux attributions du médecin-coordinateur (Délibération n°28/2013 du 7 février 2013) ;

2. Avis relatif au projet de loi n°6394 portant approbation : de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg, le Gouvernement du Royaume de Belgique, le Gouvernement de la République fédérale d'Allemagne et le Gouvernement de la République française, concernant la mise en place et l'exploitation d'un centre commun de coopération policière et douanière dans la zone frontalière commune, signé à Luxembourg, le 24 octobre 2008; de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République française relatif à la coopération dans leurs zones frontalières entre les autorités de police et les autorités douanières, signé à Luxembourg, le 15 octobre 2001 (Délibération n°178/2013 du 19 avril 2013) ;

3. Avis au sujet des projets de loi relatifs à la réforme dans la Fonction Publique en particulier des dispositions ayant trait à la protection des données comprises dans le projet de loi n°6457 (Délibération n°265/2013 du 14 juin 2013) ;

4. Avis relatif à l'avant-projet de règlement grand-ducal pris en exécution de l'article 4 de la loi modifiée du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat et à l'avant-projet de règlement grand-ducal pris en exécution de l'article 23 de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité (Délibération n°274/2013 du 28 juin 2013) ;

Les séances de délibération de la Commission nationale

Les membres de la Commission nationale se réunissent 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. En 2013, la Commission nationale a adopté au cours de 31 séances 606 délibérations, dont notamment :

- 539 autorisations ;
- 10 avis relatifs à des projets ou propositions de loi et mesures réglementaires ;
- 20 agréments pour les chargés de la protection des données ;
- 19 approbations de règles d'entreprise contraignantes ;
- 1 avertissement.

5. Avis relatif au projet de loi n°6381 portant réforme de l'exécution des peines, au projet de loi n°6382 portant réforme de l'administration pénitentiaire et au projet de règlement grand-ducal portant organisation des régimes internes des établissements pénitentiaires (Délibération n°302/2013 du 05 juillet 2013) ;

6. Avis relatif à l'avant-projet de règlement grand-ducal portant création des traitements de données à caractère personnel nécessaires à l'exécution de l'article 32 de la loi du 2 septembre 2011 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales (Délibération n°345/2013 du 12 juillet 2013) ;

7. Avis relatif au projet de loi n°6566 facilitant l'échange transfrontalier d'informations concernant les infractions en matière de sécurité routière (Délibération n°385/2013 du 25 juillet 2013) ;

8. Avis relatif au projet de loi n°6593 portant modification de la loi du 16 juin 2004 portant réorganisation du centre socio-éducatif de l'Etat et de diverses autres lois et au projet de règlement grand-ducal portant organisation de l'unité de sécurité du centre socio-éducatif de l'Etat (Délibération n°386/2013 du 25 juillet 2013) ;

9. Avis relatif au projet de règlement grand-ducal relatif aux modalités du comptage de l'énergie électrique et du gaz naturel (Délibération n°566/2013 du 13 décembre 2013) ;

10. Avis relatif au règlement interne du Registre National du Cancer (Délibération n°606/2013 du 23 décembre 2013).

2.2.1 Le statut, les modalités de désignation et les attributions du médecin-coordinateur

La Commission nationale s'est exprimée au sujet du projet de règlement grand-ducal relatif au statut, aux modalités de désignation et aux attributions du médecin-coordinateur.
La fonction du médecin-coordinateur a été créée par la loi du 17 décembre 2010 portant réforme du système de soins de santé et modifiant notamment l'article 29 de la loi du 28 août 1998 sur les établissements hospitaliers.

La CNPD a limité ses observations aux questions de protection des données, soulevées plus particulièrement par l'article 5 du projet de règlement grand-ducal. Celui-ci dispose notamment que « *pour les besoins de sa mission, le*

Les activités en 2013

médecin-coordinateur a accès aux dossiers individuels visés à l'article 36 de la loi modifiée du 28 août 1998 des patients qui sont pris en charge par son service ou groupement de services ».

Absence du lien thérapeutique entre le médecin-coordinateur et le patient

Dans son avis, la Commission nationale a estimé que l'introduction du rôle de médecin coordinateur dans notre législation est de nature à contribuer à améliorer la qualité de notre système de soins. En particulier, elle n'a pas mis en doute que, pour l'exercice et dans les limites de ses missions légales et réglementaires, le médecin-coordinateur devrait avoir accès aux dossiers individuels des patients pris en charge par son service ou groupement de services. Elle a cependant été d'avis que cet accès devra être encadré par certaines garanties.

La CNPD a attiré l'attention sur le fait que les missions du médecin-coordinateur, aussi légitimes et précieuses qu'elles soient, ne s'inscrivent pas dans un lien thérapeutique, mais bien dans une démarche d'amélioration de la qualité des soins. Il n'existe donc pas a priori de lien thérapeutique entre le médecin-coordinateur et les patients pris en charge par son service ou groupement de services. L'article 20 paragraphe (3) du projet de loi n°6469, qui permettrait le partage des données entre médecins et autres professionnels de la santé faisant partie d'une même équipe de soins n'aurait donc pas vocation à s'appliquer. Il s'ensuit que le principe du secret médical devra donc pleinement être respecté.

L'accès du médecin-coordinateur aux données avec le consentement des patients

La Commission nationale a considéré que l'accès du médecin-coordinateur aux données des patients individuels ne devrait être possible qu'avec le consentement du patient.

Ce consentement devrait par ailleurs être distinct des autres consentements nécessaires à la prise en charge du patient dans le cadre du traitement médical au sein de l'hôpital ou de l'établissement hospitalier spécialisé. En dehors des cas d'urgence, le consentement devrait en outre être préalable à la prise en charge du patient au sein de l'hôpital ou de l'établissement hospitalier spécialisé, afin que cette manifestation de volonté du patient soit suffisamment informée. Lorsque le patient est admis aux services d'urgences, le consentement du patient devrait être recueilli a posteriori.

Le contrôle de l'accès aux dossiers individuels des patients

La CNPD a estimé dans son avis que le rôle du médecin-coordinateur ne comporte pas de mission de contrôle ou de surveillance sur les médecins traitants. Dans la plupart des cas, le suivi des bonnes pratiques élaborées au sein d'un service devrait pouvoir se faire sur base de chiffres agrégés ou de statistiques, ce qui n'exclut pas que dans certains cas le médecin-coordinateur puisse consulter certains dossiers individuels.

Dès lors, une certaine transparence à l'égard des médecins traitants s'impose. C'est pourquoi la Commission nationale a suggéré de prévoir la mise en place d'une journalisation des accès. Ainsi, à des intervalles réguliers, les médecins traitants devraient se voir communiquer la liste des dossiers de leurs patients auxquels le médecin-coordinateur a accédé.

2.2.2 Projet de loi n°6394 portant approbation de différents accords en matière de coopération transfrontalière

La Commission nationale s'est prononcée au sujet du projet de loi n°6394 portant approbation : de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg, le Gouvernement du Royaume de Belgique, le Gouvernement de la République fédérale d'Allemagne et le Gouvernement de la République française, concernant la mise en place et l'exploitation d'un centre commun de coopération policière et douanière dans la zone frontalière commune, signé à Luxembourg, le 24 octobre 2008 ; de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République française relatif à la coopération dans leurs zones frontalières entre les autorités de police et les autorités douanières, signé à Luxembourg, le 15 octobre 2001.

Les deux accords prévoient la mise en place et l'exploitation d'un centre commun de coopération policière et douanière ainsi que des échanges de renseignement entre les autorités policières et douanières des pays participants, renseignements qui peuvent comporter des données à caractère personnel.

Si les deux accords prévoient le traitement de données à caractère personnel, force est de constater que les accords ne contiennent aucune précision quant aux catégories de données faisant l'objet du traitement. La Commission nationale aurait préféré que l'accord comporte une énumération des catégories de données concernées.

Elle a par ailleurs regretté qu'elle n'ait été consultée ni au cours de la phase de négociation,

ni avant la signature de l'accord de 2008, alors que le projet de loi sous examen n'a pour but que d'approuver les deux accords signés qui ne peuvent plus être modifiés, à moins de les renégocier avec les Etats concernés.

2.2.3 La réforme de la législation sur la fonction publique

Dans son avis du 14 juin 2013, la Commission nationale a exposé ses réflexions et commentaires au sujet des projets de loi relatifs aux réformes dans la fonction publique, mais en particulier des dispositions ayant trait à la protection des données visées à l'article 41 du projet de loi n°6457.

La Commission nationale a salué l'introduction dans la loi cadre fixant le statut général des fonctionnaires de l'Etat d'une disposition ayant pour vocation d'encadrer les traitements dont les données des fonctionnaires et employés des services de l'Etat font l'objet tout comme ceux des pensionnés ou candidats à un emploi public.

Dans son avis, la CNPD a mis l'accent sur le fait que les finalités susceptibles de justifier l'accès aux données devront être bien déterminées. Le texte proposé le fait en des termes généraux, en faisant référence aux processus centraux et locaux de gestion du personnel, et il énumère de façon explicite 9 champs d'activités essentiels. Le terme « notamment » précédant cette énumération ne paraît acceptable que dans la mesure où il n'ouvre pas la voie à un spectre illimité d'objets pour lesquels les données pourraient être traitées. La Commission nationale a donc marqué son accord avec le libellé proposé, sous la réserve expresse que l'utilisation du terme « notamment » ne puisse pas être comprise comme permettant d'ajouter aux finalités énumérées d'autres finalités que celles se rattachant aux processus de gestion des ressources humaines visés par un texte légal ou réglementaire.

Pour ce qui est des données recueillies et traitées, la préférence de la CNPD en la matière irait clairement en faveur d'une énumération directe dans l'article de loi, spécifiant au moins les grandes catégories de données visées décrites dans leur généralité.

La Commission nationale a noté avec satisfaction que l'accès aux données sera strictement limité aux personnes habilitées à cet effet et contrôlé. Le règlement d'exécution à prendre devra spécifier que ces accès feront l'objet d'un système de journalisation (logging) de nature à faciliter le contrôle et la détection d'éventuels abus.

Finalement, la CNPD a fait remarquer que le texte proposé n'indique pas de durée de conservation des données recueillies et traitées. Il conviendrait pour le moins de spécifier quelles informations doivent être retenues en cas de cessation de l'occupation de l'agent dans les administrations et services de l'Etat et pendant combien de temps suivant son départ.

2.2.4 L'organisation du Service de Renseignement de l'Etat

La Commission nationale s'est prononcée au sujet de l'avant-projet de règlement grand-ducal pris en exécution de l'article 4 de la loi modifiée du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat et portant création et fixant les modalités de fonctionnement d'un fichier relatif au traitement de données à caractère personnel par le Service de Renseignement de l'Etat ainsi qu'au sujet de l'avant-projet de règlement grand-ducal pris en exécution de l'article 23 de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité et portant création et fixant les modalités de fonctionnement d'un fichier relatif au traitement de données à caractère personnel par le Service de Renseignement de l'Etat.

Avant-projet de règlement grand-ducal pris en exécution de l'article 4 de la loi modifiée du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat

La Commission nationale a noté dans son avis que les catégories de données énumérées sont décrites de manière assez vague. Ainsi, sans la lecture du commentaire des articles, il n'est pas aisé de faire la différence par exemple entre les données d'identification personnelles et les caractéristiques personnelles. Les expressions « données d'identification électroniques » et « données de localisation électroniques » ne sont pas très parlantes et la CNPD a proposé de mentionner leur origine de de manière plus expresse. En ce qui concerne les « données financières », la CNPD se demande quelle pourrait bien être l'origine des données.

De manière générale, la Commission nationale suppose que toutes les données correspondant aux catégories énumérées à l'article 5 ne sont pas collectées systématiquement d'office pour chaque personne concernée, mais que seules les données dont la collecte s'avère indispensable sont collectées conformément aux principes de nécessité et proportionnalité.

Cela vaut en particulier pour les données dites sensibles, à savoir les données raciales ou ethniques ou les convictions philosophiques, politiques et religieuses ainsi que l'appartenance syndicale. Le traitement de ces données est en principe interdit par l'article 6 paragraphe (1) de la loi modifiée du 2 août 2002, à moins que le traitement ne soit mis en œuvre par voie de règlement grand-ducal tel que prévu à l'article 17 de la même loi, ce que le gouvernement se propose de faire par le texte sous examen. La Commission nationale a noté que le SRE ne sera donc pas autorisé à collecter des données relatives à la santé et à la vie sexuelle.

Quant aux écoutes téléphoniques, la CNPD s'est posé la question suivante : ne faudrait-il pas insérer une référence expresse à la procédure prévue aux articles 88-3 et 88-4 du Code d'instruction criminelle ? Il en est de même pour les données de traçage de télécommunications, pour autant que celles-ci ne relèvent pas de l'article 5 paragraphe 1 points 3 et 4 de l'avant-projet de règlement.

De manière plus générale, la CNPD a rappelé qu'aucune mesure affectant un droit constitutionnellement protégé par la Constitution - tel que le secret des communications ou l'inviolabilité du domicile - ne

pourra être prise sans qu'un texte légal n'en précise le cadre et les conditions.

Il convient de relever que la loi modifiée du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat ne comporte pas de base légale spécifique pour des techniques subreptices de collecte de données et d'enregistrement de sons et d'images autres que celles couvertes par les articles 88-3 et 88-4 à l'instar de ce qui existe, en matière policière, avec les articles 48-12 à 48-23 du Code d'instruction criminelle sur l'observation et l'infiltration et en particulier l'observation effectuée à l'aide de moyens techniques prévue par l'article 48-13 paragraphes (2) et (3) du même Code.

L'article 11 prévoit que lors de chaque traitement de données, les informations relatives à l'agent du SRE ayant procédé au traitement ainsi que la date et l'heure du traitement devront être enregistrées. La CNPD a estimé qu'une telle journalisation est une condition nécessaire pour pouvoir protéger le citoyen contre les risques de dérives et d'abus. La journalisation est aussi un outil indispensable aux contrôles internes.

L'avant-projet de règlement prévoit que les données de journalisation seront effacées après un délai de trois ans. Eu égard aux dysfonctionnements au sein du SRE, la Commission nationale a estimé que les données de journalisation devraient faire l'objet d'un archivage pendant une durée de 10 ans après l'expiration du délai de trois ans prémentionné. De plus, la CNPD a estimé qu'il faudra prévoir pour le moins une information sommaire sur les motifs d'une consultation des données.

Avant-projet de règlement grand-ducal pris en exécution de l'article 23 de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité

L'article 5 énumère les catégories de données appelées à figurer dans le fichier « e-ANS ». La Commission nationale a salué que le texte donne une énumération plus précise des données traitées, mais a déploré cependant que le texte ne donne aucune précision sur l'origine des données.

L'article 9 prévoit plusieurs délais de conservation des données dans la partie « archivage ». Selon la CNPD, ces délais semblent justifiés et proportionnés, sauf celui prévu au paragraphe 4 suivant lequel la fiche succincte doit être conservée pendant un délai de trente ans. Malgré les explications fournies au commentaire des articles, cette durée de conservation semble excessive.

2.2.5 La réforme de l'exécution des peines et de l'administration pénitentiaire

La Commission nationale s'est prononcée au sujet du projet de loi n°6381 portant réforme de l'exécution des peines, du projet de loi n°6382 portant réforme de l'administration pénitentiaire et du projet de règlement grand-ducal portant organisation des régimes internes des établissements pénitentiaires.

Réforme de l'exécution des peines

Si la Commission nationale s'est félicitée de ce qu'une base légale soit conférée à la pratique de la surveillance électronique avec le projet de loi n°6381, ce texte a appelé les remarques suivantes dans son avis :

- Le projet de loi ne précise pas par qui ou sous les instructions de quelle institution ou personne la surveillance sera effectuée. Le texte devrait dès lors déterminer de manière claire et précise le responsable du traitement de données à des fins de surveillance.
- Les principes de base des modalités et du fonctionnement de la surveillance électronique devraient également être déterminés et précisés dans le texte.
- Enfin, il convient de se poser la question s'il n'est pas recommandable de demander le consentement de la personne concernée, vu qu'un tel traitement de données a un caractère extrêmement intrusif dans la vie privée des personnes concernées.

Réforme de l'administration pénitentiaire

L'article 4 du projet de loi n°6382 prévoit que le traitement de données à caractère personnel sera mis en œuvre et géré par l'administration pénitentiaire. Selon la CNPD,

il conviendrait de préciser davantage qui, à l'intérieur de l'administration pénitentiaire et des différents établissements pénitentiaires, est responsable de quelles données et qui a accès à quelles données. A ce titre, il serait judicieux d'établir deux niveaux d'accès pour tous les dossiers des détenus. Sur un premier niveau se trouveraient les informations de base accessibles à l'administration pénitentiaire. A un second niveau se trouveraient des informations plus détaillées qui ne seraient accessibles qu'aux personnes habilitées en raison de leur fonction à l'intérieur de l'établissement pénitentiaire concerné.

Les catégories de données susceptibles d'être communiquées aux autorités judiciaires et policières par l'administration pénitentiaire et les établissements pénitentiaires mériteraient d'être précisées dans le texte. Il en est de même pour ce qui est des finalités permettant une telle communication.

L'article 42 prévoit la prise d'empreintes digitales et de photographies des détenus. La prise et la conservation de photographies peuvent constituer une atteinte à la vie privée et au droit à l'image. Vu la finalité d'authentification inhérente à cette prise de photographies, une telle atteinte paraît néanmoins justifiée et proportionnée. Mais la Commission nationale a estimé que le texte devrait déterminer la durée de conservation des photographies et des empreintes digitales.

Projet de règlement grand-ducal portant organisation des régimes internes des établissements pénitentiaires

L'article 45 de ce projet prévoit la possibilité de soumettre une cellule à des mesures de vidéosurveillance. La Commission nationale n'exclut pas une éventuelle nécessité d'un placement sous vidéosurveillance. Mais le recours à un dispositif de surveillance des cellules ne doit se faire que lorsque des questions de sécurité urgentes l'exigent, par exemple en cas de menace de suicide. Et même dans un tel cas la caméra de surveillance ne devrait pas remplacer les autres mesures, à savoir les rondes fréquentes qui permettent un contact humain et qui assurent une surveillance efficace de l'état de santé du détenu.

Un système de masquage électronique des images devrait être mis en place pour la zone des sanitaires et toilettes et, le cas échéant, les douches dans les cellules, afin de garantir l'intimité de la personne, sauf avis contraire explicite d'un médecin dans des cas tout à fait exceptionnels.

En cas d'enregistrement des images, celles-ci devront être supprimées rapidement après leur enregistrement.

2.2.6 Règlementation de l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales

La Commission nationale s'est prononcée au sujet de l'avant-projet de règlement grand-ducal portant création des traitements de données à caractère personnel nécessaires à l'exécution de l'article 32 de la loi du 2 septembre 2011 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales.

L'objectif de l'avant-projet de règlement consiste à déterminer les conditions et critères à respecter par le Ministre qui veut accéder aux données nécessaires pour vérifier si une personne satisfait aux exigences posées par la loi du 2 septembre 2011.

La loi du 2 septembre 2011 pose le principe de la mise en place d'un registre des entreprises dans lequel devront figurer toutes les données nécessaires au Ministère des Classes moyennes. L'avant-projet de règlement grand-ducal énumère en détail les données dont il s'agit. La Commission nationale a salué la précision avec laquelle les données sont énumérées, sauf pour ce qui est du tiret écrit dans les termes suivants : « toutes autres informations fournies par l'administré ou par d'autres administrations ». Contrairement aux quatre premiers tirets, ce libellé est trop vague pour faire apparaître le caractère pertinent et nécessaire de ces informations, et il constitue en quelque sorte une catégorie « fourre-tout », de sorte qu'il conviendrait de préciser davantage quelles données sont exactement visées.

L'article 2 de l'avant-projet de règlement grand-ducal énumère de façon limitative les données auxquelles le Ministre peut accéder via un système informatique direct afin de contrôler si une personne satisfait aux exigences posées par la loi du 2 septembre 2011. En ce qui concerne cette énumération, la CNPD a considéré que des précisions devraient être apportées afin de clarifier quelles données des ascendants et descendants de la personne concernée sont à fournir, et en quoi ces informations sont pertinentes et nécessaires.

La Commission nationale a noté avec satisfaction qu'elle a été suivie dans son avis du 15 avril 2011 relatif à l'article 32 du projet de loi n°6158 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales alors que les dispositions des articles 3 et 4 de l'avant-projet de règlement grand-ducal, assurant la traçabilité des accès aux données de fichiers publics, constituent une bonne garantie contre d'éventuels abus.

Le paragraphe (2) de l'article 4 dispose que les données de journalisation sont effacées après un délai d'une année à compter de leur premier enregistrement, sauf si elles font l'objet d'une procédure de contrôle. A ce sujet, la CNPD a proposé d'aligner la durée de conservation sur celle qui a été retenue par la loi du 5 juin 2009 relative à l'accès des autorités judiciaires, de la Police, de l'Inspection générale de la Police à certains traitements de données à caractère personnel mis en œuvre par des personnes morales de droit public, qui prévoit que les informations relatives aux magistrats et aux membres du personnel de l'administration judiciaire ayant procédé à la consultation ainsi que les informations consultées, la date et l'heure de la consultation sont enregistrées et conservées pendant un délai de 3 ans. Cette durée paraît plus appropriée que celle d'un an envisagée pour préserver les possibilités de vérification du caractère licite de la consultation des données.

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

La CNPD a avisé le projet de loi n°6566 facilitant l'échange transfrontalier d'informations concernant les infractions en matière de sécurité routière.

Ce projet de loi a pour objet de transposer en droit national la directive 2011/82/UE du 25 octobre 2011, qui prévoit la mise en place d'une procédure d'échange d'informations transfrontalier en vue de permettre l'application transfrontière de sanctions relatives aux infractions les plus graves en matière de sécurité routière, lorsque celles-ci sont commises dans un pays de l'Union européenne autre que celui dans lequel le véhicule est immatriculé. L'Etat membre sur le territoire duquel une infraction déterminée en matière de sécurité routière sera commise par un conducteur dont le véhicule est immatriculé dans un autre Etat membre pourra accéder sur demande aux données relatives à l'immatriculation de ce véhicule.

Etant donné que ce texte prévoit l'échange de données à caractère personnel transfrontalier concernant les auteurs présumés d'infractions routières, le projet a des implications directes en matière de protection des données.

Le projet de loi transpose fidèlement la directive européenne précitée, laquelle prévoit déjà des garanties appropriées suffisantes en termes de protection des données. A ce titre, la CNPD s'est ralliée à l'avis (2008/C 310/02) du Contrôleur européen de la protection des données du 8 mai 2008 relatif à la proposition de directive du Parlement européen et du Conseil facilitant l'application transfrontière de la législation dans le domaine de la sécurité routière, lequel avait avisé favorablement la légitimité et la nécessité de l'échange de données transfrontalier, de même que la qualité des données personnelles traitées dans ce contexte.

Si la CNPD a accueilli favorablement le projet de loi dans son ensemble, l'article 7 appelle cependant quelques observations. La CNPD est d'avis que la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale n'a jamais fait l'objet d'une transposition proprement dite en droit national. L'absence d'un texte spécifique de transposition et la dispersion de dispositions de protection des données en matière pénale dans 20 différents textes légaux ne sont pas de nature à favoriser

ou à faciliter la prévisibilité et l'exercice effectif des droits protecteurs des citoyens.
Pour cette raison, la CNPD a recommandé au gouvernement de transposer de façon plus appropriée la décision-cadre 2008/977/JAI, à savoir dans un seul et même texte législatif national, alors qu'il y a un besoin pressant dans l'intérêt des citoyens à voir clarifier leurs droits et libertés fondamentaux protégés. Une coopération plus étroite entre les services répressifs devrait aller de pair avec le respect des droits fondamentaux, notamment le droit au respect de la vie privée et le droit à la protection des données.

L'article 7 paragraphe (2) du projet de loi confère à tout résident luxembourgeois, auteur présumé d'une infraction à la circulation routière commise dans un autre Etat membre, le droit d'accéder aux données relatives à l'immatriculation de son véhicule qui ont été transmises par la Police grand-ducale au point de contact national de l'Etat membre de l'infraction. Il s'agit là d'un droit d'accès dit « direct ». Or, la loi modifiée du 2 août 2002 relative à la protection des données ne confère aux personnes concernées qu'un accès dit « indirect », qui ne peut s'exercer que par l'intermédiaire de l'autorité de contrôle spécifique « Article 17 ». Etant donné qu'une loi spéciale (projet de loi n°6566) déroge à la loi générale (loi modifiée du 2 août 2002) et dans un souci de sécurité juridique, la CNPD est d'avis que l'article 7 paragraphe (2) du projet de loi devrait instaurer pour le moins un droit d'accès en faveur des personnes concernées qui s'exerce directement auprès de la Police grand-ducale.

2.2.8 Organisation du centre socio-éducatif de l'Etat

La Commission nationale s'est prononcée au sujet de

- l'avant-projet de loi portant modification : 1. de la loi du 16 juin 2004 portant réorganisation du centre socio-éducatif de l'Etat ; 2. de la loi du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'Etat ; 3. de la loi du 29 juin 2005 fixant les cadres du personnel des établissements d'enseignement secondaire et secondaire technique ; 4. de la loi du 23 juillet 1952 concernant l'organisation militaire (ci-après désigné *« le projet de loi »*) ;

- et du projet de règlement grand-ducal portant organisation de l'unité de sécurité du centre socio-éducatif de l'Etat (ci-après désigné *« le projet de règlement »*).

Les deux textes ont £principalement pour objet de rendre l'organisation de l'unité de sécurité du centre socio-éducatif de l'Etat conforme aux principes applicables au niveau international aux mineurs privés de liberté, de préciser le régime disciplinaire applicable au sein de l'unité de sécurité et de faire fonctionner celle-ci.

La Commission nationale a limité ses observations aux dispositions qui ont trait à la protection des données et à la vie privée et plus particulièrement à l'article I point 10 du projet de loi et aux articles 5 à 9 du projet de règlement grand-ducal. Ces dispositions prévoient notamment la mise en place d'un registre général ainsi que des dossiers individuels des pensionnaires qui peuvent être établis sous forme de bases de données informatiques.

En ce qui concerne les finalités du traitement, la CNPD a noté qu'elles ont bien été décrites dans les commentaires du projet de loi, mais qu'il conviendrait de les spécifier dans le texte même de la loi.

La CNPD a ensuite formulé quelques observations concernant la collecte et l'utilisation des données personnelles dans le cadre du dossier individuel.
A ce titre, elle a estimé que :

- La prise et la conservation de photographies sont susceptibles de constituer une atteinte à la vie privée et au droit à l'image, mais paraissent légitimes et proportionnées dans ce contexte.

- L'information relative à la confession ne pourra être collectée qu'avec le consentement exprès du pensionnaire. Ce consentement doit être libre. Il faudra donc que l'indication de la confession par le pensionnaire soit facultative et non obligatoire.

- L'accès au dossier médical est strictement réservé au personnel médical et exceptionnellement au directeur du centre. L'accès par le directeur est susceptible de constituer une violation du secret médical. Cette dérogation doit obligatoirement être prévue dans un texte légal.

La Commission nationale a par ailleurs constaté que les projets de loi et de règlement ne spécifient rien sur l'origine des données. Par souci de clarté juridique, l'origine des données et le caractère obligatoire ou facultatif des données devraient être précisés dans les textes.

Concernant l'accès aux données, la CNPD a noté que les textes analysés devraient préciser qui a accès à quelles données, suivant le principe que chaque agent ne doit avoir accès qu'aux données nécessaires à l'accomplissement de ses tâches. Quant aux destinataires externes, les modalités d'accès par les différents organismes devraient être précisées et il conviendrait de prévoir un système qui permette de retracer a posteriori qui a eu accès à quelles données, et pour quelle raison, afin d'éviter des abus éventuels.

Finalement, la CNPD a constaté que les textes avisés ne définissent aucun délai légal de conservation des données et ne prévoient pas de dispositions relatives aux mesures de sécurité et de confidentialité des données. A cet égard, elle a estimé qu'il serait nécessaire que les textes fixent une durée de conservation maximale dans les bases de données, et qu'il conviendrait de prévoir des mesures de sécurité spécifiques dans le texte du règlement grand-ducal, notamment en ce qui concerne le contrôle de l'utilisation, de l'accès et de la transmission des données.

2.2.9 Modalités du comptage de l'énergie électrique et du gaz naturel

La Commission nationale a rendu, en date du 13 décembre 2013,

un avis portant sur l'avant-projet de règlement grand-ducal relatif aux modalités du comptage de l'énergie électrique et du gaz naturel.

La Commission nationale a considéré que le déploiement des compteurs intelligents nécessite la mise en place d'un système de sécurisation des données performant et évolutif. Afin de garantir la confidentialité des renseignements à caractère personnel, le chiffrement des données et la traçabilité des connexions aux serveurs doivent être assurés, et un système d'habilitation des personnes ayant accès aux données doit être mis en place. De plus, la sécurité des données doit se faire tout au long de la chaîne de communication, au travers de tous les acteurs et de tous les moyens de communication. Cette obligation de sécurité découle des articles 21 à 23 de la loi modifiée du 2 août 2002.

Par ailleurs, la Commission nationale a mis en lumière dans son avis le risque de dérives potentielles lié à l'utilisation des compteurs intelligents conduisant à une intrusion disproportionnée dans la sphère privée des foyers raccordés. Le déploiement des compteurs intelligents est un projet d'envergure nationale visant à long terme l'ensemble des habitations luxembourgeoises. Au regard des informations précises collectées par lesdits compteurs, il sera donc possible d'en déduire les habitudes de vie (heures du lever et du coucher, présence ou absence au domicile,…) ou même, dans des cas spécifiques, le type d'appareils utilisés. Il y a donc lieu de définir strictement les conditions dans lesquelles les gestionnaires de réseaux et les fournisseurs pourront utiliser les données de comptage, afin que les compteurs intelligents ne portent pas atteinte à la vie privée des citoyens d'une part, et qu'ils améliorent la gestion de l'énergie pour les acteurs du marché de l'énergie d'autre part.

Plusieurs articles de l'avant-projet ont donné lieu à des observations de la part de la Commission nationale :

- Article 1 : Il faut préciser que les gestionnaires de réseaux ne sont pas seulement à considérer comme étant responsables de l'activité de déploiement des modalités de comptage, mais également comme responsables du traitement de données au sens de la loi précitée ;

- Article 3 : A côté des finalités des traitements effectués par les fournisseurs, il faudrait également énumérer les traitements effectués par les gestionnaires de réseaux, étant donné qu'ils traitent des données pour des finalités distinctes ou similaires ;

- Article 4 : La CNPD est d'avis que les gestionnaires de réseaux ainsi que les fournisseurs doivent conserver les données de comptage « quart-horaire » pour l'électricité et « horaire » pour le gaz naturel pendant une période de 6 mois (au lieu des 15 ans prévus dans le projet) lorsque la facture a été payée et n'a pas fait l'objet d'un litige ou d'une contestation. Les données de comptage doivent ensuite être agrégées, afin de conserver une unique donnée de comptage par mois, et ce sur une période de cinq ans. En effet, la prescription quinquennale prévue à l'article 2277 du Code civil s'applique aux créances d'électricité.

2.2.10 Règlement interne du Registre National du Cancer

Avec le Registre National du Cancer, le Luxembourg a mis en place un outil unique lui permettant de suivre à la fois l'incidence des cancers, leur prise en charge mais aussi la survie des patients. Le Centre de Recherche Public de la Santé (CRP-Santé) pilote le projet en tant qu'institution responsable en liaison avec les hôpitaux et les autres acteurs clés du domaine du cancer au Luxembourg.

Les activités en 2013

Conformément au règlement grand-ducal du 18 avril 2013 déterminant les modalités et conditions de fonctionnement du Registre National du Cancer, le règlement interne - qui comprendra la charte de sécurité, les modalités de contrôle qualité à opérer et les modalités relatives à la publication des résultats - est soumis pour approbation au ministre ensemble avec la Commission nationale.

Cette dernière s'est prononcée au sujet des documents concernant le règlement interne du Registre National du Cancer. Le règlement interne, tel que soumis à la Commission nationale, est composé du document du règlement interne, de la charte de sécurité des systèmes d'information, du manuel qualité, de la procédure de diffusion des résultats et de la brochure d'information des patients.

Concernant la charte de sécurité, la CNPD a suggéré de mettre en place une formation continue sur la sensibilisation à la sécurité, qu'elle propose d'organiser suivant un cycle au minimum annuel au lieu d'une seule formation.

La CNPD recommande par ailleurs d'isoler le système d'information propre au registre national du cancer de toutes autres activités nécessitant l'utilisation d'un système d'information (navigation Internet, e-mail, gestion administrative,…).

Concernant la gestion des mots de passe, la CNPD a proposé de mettre en place une politique de construction de mots de passe forcée techniquement, afin que les utilisateurs soient contraints d'utiliser des mots de passe avec le niveau de complexité requis. De plus, elle a exigé la mise en œuvre d'une authentification forte pour l'accès à la base de données du RNC.

La CNPD a encore fait plusieurs suggestions concernant les règles élémentaires à appliquer par le collaborateur. Elle a notamment conseillé :

- de mettre en œuvre des blocages techniques pour que les utilisateurs ne se connectent pas aux réseaux locaux des équipements non autorisés par le CRP-Santé ou son établissement ;

- l'implémentation d'un outil qui permet le contrôle des supports mobiles pour assurer la protection des informations sensibles du RNC et ne pas les transporter sans protection ;

- d'ajouter la mise en œuvre d'un blocage automatique du poste de travail après quelques minutes d'inactivité ;

- d'indiquer aux collaborateurs un point de contact unique auquel ils peuvent s'adresser en

cas de suspicions d'incident ou d'incident avéré ;

- d'intégrer une section relative à l'utilisation du téléphone/courriel et d'indiquer aux collaborateurs les règles de divulgation et de collecte d'informations par téléphone/courriel ;

- d'insérer une section sur la mise en œuvre de mesures relatives à la continuité de service et la récupération de production (BCP / DRP).

Finalement, la CNPD a estimé important et nécessaire de rajouter au formulaire de refus du patient une phrase qui informe le patient que son opposition au traitement de ses données n'entraîne aucun préjudice pour lui et ne porte pas atteinte à son droit à recevoir des soins de santé appropriés.

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 pesant sur 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.

Thierry Lallemang à la table ronde „Wéi ass meng Foto hei geland?"

2.3.1 Actions de sensibilisation du public

Le 28 janvier 2013, la Commission nationale a organisé une conférence de Monsieur Dean Spielmann, Président de la Cour Européenne des Droits de l'Homme, sur le thème *« La protection des données dans la jurisprudence de la Cour Européenne des Droits de l'Homme de Strasbourg »*[3]. La conférence s'est tenue dans le nouveau bâtiment administratif de l'Etat à Esch-Belval en présence de Monsieur François Biltgen, Ministre de la Justice, Ministre des Communications et des Médias. 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'ouverture à 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.

Le 7 février 2013, Thierry Lallemang, membre effectif de la CNPD, a participé à la table ronde *„Wéi ass meng Foto hei geland?"*, animée par

[3] Pour plus de déatils : partie 3.1.

Les activités en 2013

Conférence de presse à l'occasion de la présentation du rapport d'activités 2012

le journaliste Marco Goetz. Les autres participants étaient Tom Krieps du Conseil National des Programmes, Romy Schmit du Ministère de l'Education, Caroline Mart de RTL et Georges Knell de BEE SECURE, tous experts dans les domaines de l'éducation, du journalisme et du droit. Cet événement a été organisé par BEE SECURE dans le cadre du Safer Internet Day sous le slogan « *Online rights and responsibilities* ». Cette journée, organisée sur initiative de la Commission européenne, a engendré un large éventail d'activités à travers le monde.

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. Le Président et les membres effectifs ont accordé plus de 40 interviews aux organes de presse.

Parmi les thèmes traités par les médias en 2013, citons : les révélations autour du programme

« PRISM » de la National Security Agency (NSA) américaine, la révision de la législation européenne sur la protection des données, le cloud computing et la base de données relative aux élèves.

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 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). En 2013, elle a reçu 38% des notifications sous forme électronique.

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

A 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.

Gérard Lommel, en ses qualités de Président de la CNPD et membre du Groupe Article 29, a été sollicité d'intervenir comme orateur lors de la 6e conférence annuelle « Traitement des Données Personnelles », organisée par *Development Institute International* à Paris. Le titre de sa présentation était : « *Responsabilisation des acteurs, évaluations d'impacts sur la vie privée, documentations… Les clés pour être conforme au principe d'accountability issu du nouveau projet de règlement* ».

Le 12 mars, les chargés de la protection des données se sont

Les activités en 2013

Pierre Weimerskirch à la conférence sur la classification des bases de données étatiques

réunis à Luxembourg[4]. Avec le soutien de la CNPD, l'AFCDP (Association Française des Correspondants à la protection des Données à caractère Personnel) a organisé une conférence à l'auditoire de la BGL BNP Paribas. Gérard Lommel a présenté un bref historique de la fonction du chargé de la protection des données dans les pays « pionniers » dans le domaine (notamment l'Allemagne) et il a abordé les droits et devoirs spécifiques du chargé issus de la législation luxembourgeoise.

Le 25 avril, le Président de la CNPD est intervenu en tant que keynote speaker à la conférence organisée par ISACA Luxembourg *(« Informations Systems Audit and Control Association »)* sur les enjeux et défis que va apporter le nouveau règlement pour les entreprises à Luxembourg. Le thème de l'intervention était *« Accountability for data protection : le nouveau règlement européen et l'exigence de conformité dynamique ».*

Le 11 septembre, Gérard Lommel a participé à une table ronde, organisée par l'Université du Luxembourg en coopération avec la Ville d'Esch et intitulée *« Prism - lutte antiterroriste, sauvegarde de la sphère privée et protection des intérêts économiques sont-ils compatibles ? ».* Au cours de l'année 2013, les révélations

[4] Voir partie 3.3 pour plus de détails.

Gérard Lommel à la table ronde « Prism - lutte anti-terroriste, sauvegarde de la sphère privée et protection des intérêts économiques sont-ils compatibles ? »

d'Edward Snowden dans la grande presse internationale ont mis à jour le système PRISM relevant essentiellement de la National Security Agency. Ce système de surveillance électronique à grande échelle constitue-t-il l'outil nécessaire à la lutte antiterroriste ? Quelles questions relatives à la protection de la sphère privée soulève l'existence d'un tel système ? Quel impact peut avoir un tel système sur la protection de la propriété intellectuelle et des secrets technologiques, et notamment les intérêts économiques européens ? L'objet de la table ronde était d'élucider certaines de ces questions. Les orateurs étaient Stefan Braum (Doyen de la Faculté de Droit, d'Economie et de Finance, Professeur en Droit Pénal, Université du Luxembourg) ; Mark Cole (Assistant Professeur en Droit des Nouvelles Technologies de l'Information, des Médias et des Communications, Université du Luxembourg) ; Franck Leprévost (Vice-Président de l'Université du Luxembourg et co-auteur du rapport « Development of surveillance technology and risk of abuse of economic information » STOA-Parlement Européen, 1999 ayant trait au réseau ECHELON) et Ralph-Philipp Weinman (Collaborateur Scientifique, spécialiste de Reverse-Engineering, SnT, Université du Luxembourg).

Le 30 août, le Président de la CNPD a participé à la conférence intitulée « *Evolving European Data Protection and e-Privacy* » organisée par KPMG. Il a présenté les changements à venir en matière de protection des données. Les autres participants étaient : Freddy Dezeure (CERT-EU), Michael Hofmann (Head of IT& Regulatory Compliance KPMG), Christoffer Karsberg (ENISA), Helmut Eiermann (Chargé de la protection des données de Rhénanie-Palatinat), François Thill (CASES) et Marcus Hild (Autorité de protection des données de l'Autriche).

Le 19 septembre, Pierre Weimerskirch, membre effectif de la CNPD, a participé à une conférence organisée par le Cyber Security Board sur la classification des banques de données étatiques. Sa présentation a porté sur les enjeux en matière de protection des données et de sécurité des traitements.

Dans la semaine du 18 novembre, la CNPD a collaboré à l'organisation d'un atelier de formation sur la sécurité de l'information organisée par CASES et suivie par 143 employés, enseignants et éducateurs de la commune de Differdange. Les cours se sont déroulés pendant 3 jours au Centre Marcel Noppeney à Oberkorn. La CNPD a contribué

avec une présentation sur les droits et devoirs en matière de protection de données à caractère personnel pour les individus, en tant que citoyens et en tant qu'employés. Parmi les thèmes abordés figuraient les concepts fondamentaux de la sécurité, les logiciels malveillants, l'économie parallèle, la sécurité physique et le social engineering.

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 25 et 26 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 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.

Aux côtés des acteurs publics et privés

En 2013, la Commission nationale a participé à plus de 102 réunions avec les acteurs du secteur public et à 75 réunions avec ceux du secteur privé. Elle était notamment 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) ;
- Ministère de l'Economie : échange de vues sur coopération règlement 2006/2004 (protection des consommateurs), smart metering, conseil de la concurrence ;

- Ministère des Finances : réunion groupe d'experts mise en œuvre technique de l'échange automatique d'informations ;

- Ministère de l'Education nationale et de la Formation professionnelle : fichier élèves ;

- Ministère de l'Enseignement supérieur et de la Recherche : échange de données à des fins statistiques ;

- Service des Communications et des Médias : réforme du cadre européen sur la protection des données ;

- Administration des Contributions directes : entrevue sur projets de réorganisation, de gestion et d'optimisation des fichiers fiscaux ;

- Administration des Douanes : collaboration dans le domaine informatique Luxembourg/ Autriche ;

- Ville de Luxembourg : discussion projet BYOD, vidéosurveillance dans les arrêts de bus ;

- CTIE : groupe de travail « inventaire des banques de données ».

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

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

Accompagnement des acteurs du secteur de la recherche et de la santé

Dans le domaine de la recherche, elle était en lien avec le Comité National d'Ethique et de Recherche (CNER), le Centre d'étude et de formation interculturelles et sociales (CEFIS), le Fonds national de la Recherche, le CEPS INSTEAD (Enquête SHARE sur la santé, le vieillissement et la retraite) ou encore le STATEC. 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.

Le Réseau d'étude sur le marché du travail et de l'emploi (RETEL) a consulté la CNPD dans le cadre d'un projet de création d'un data warehouse. L'objectif de ce projet est de mieux connaître le marché de l'emploi et d'évaluer les mesures en mettant à disposition des données agréées pour le grand public et des micro-données pour les chercheurs. Plus précisément, ces données, études et analyses sont nécessaires pour la conduite de la politique en faveur du marché de travail, de l'emploi et la lutte contre le chômage.

Dans le domaine de la santé, la Commission nationale a participé 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 au niveau du fonctionnement quotidien des hôpitaux. Il s'agit notamment de trouver des solutions pour empêcher tout accès illégitime au dossier électronique du patient et d'harmoniser les règles observées concernant le stockage et les flux internes de données ainsi que les échanges avec des tiers.

2.4.2 Demandes de renseignements

La Commission nationale a reçu 2.077 demandes de renseignements en 2013. Dans

Les activités en 2013

Les caméras installées dans les voitures (« dashcams ») sont-elles licites ?

En 2013, la CNPD s'est vue confrontée à un nombre croissant de demandes de renseignement relatives à des caméras installées dans les voitures de particuliers et destinées à filmer des comportements de la circulation, pour se constituer un moyen de preuve dans l'hypothèse d'un accident. A ce titre, elle avait rappelé que l'utilisation de telles vidéocaméras (« dashcams ») dirigées sur la voie publique et susceptibles de capter des images de personnes reconnaissables n'était pas licite.

Le captage et l'enregistrement par de tels dispositifs d'images de personnes identifiables ou de véhicules dont la plaque minéralogique apparaît lisiblement constituent un traitement de données à caractère personnel et, s'agissant d'une surveillance, seraient soumis à autorisation préalable de la part de la CNPD.

La loi modifiée du 2 août 2002 ne prévoit cependant aucun critère de légitimation sur lequel un demandeur pourrait se baser afin de justifier l'utilisation d'une telle caméra. Selon le principe de proportionnalité, l'utilisation de ces caméras devrait par ailleurs être considérée comme disproportionnée, considérant que tous les usagers de la route, voire de la voie publique, seraient filmés à leur insu. Une information des personnes surveillées, telle que requise par la loi, serait par ailleurs impossible à réaliser dans le cadre d'une telle installation. Même si l'intérieur de la voiture est considéré comme un espace privé et domestique, il n'est pas pour autant permis de filmer la voie publique à partir de cet intérieur.

La CNPD tient à préciser que seule l'utilisation d'une telle caméra au sein de l'espace public ouvert à la circulation d'autres personnes est à considérer comme illégale, mais pas l'appareil en lui-même. Par ailleurs, il ne faudrait pas confondre ces caméras de surveillance avec les dispositifs installés dans les voitures aidant le conducteur à se garer et qui n'enregistrent pas les images.

la majorité des cas, il s'agissait de questions juridiques ou de requêtes relatives aux formalités à accomplir pour mettre en œuvre un traitement de données.

Elle a répondu à 1.803 demandes par téléphone et à 274 par écrit. Presque la moitié des demandes émanent d'entreprises. Les autres proviennent 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 Participation aux travaux européens

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 sa complexité. La Commission nationale, représentée par un ou plusieurs de ses membres, a participé en 2013 à 39 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 réunion annuelle de l'Association francophone des autorités de protection des données personnelles ;
- de la conférence de printemps des commissaires européens à la protection des données à Lisbonne ;
- de la conférence internationale des commissaires à la protection des données et de la vie privée à Varsovie.

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 » et des autorités douanières.

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 Etats membres de l'Union européenne.

Parmi les sujets traités par le groupe de travail en 2013, citons :

- la révision du cadre légal européen de la protection des données ;
- l'intérêt légitime du responsable du traitement ;
- la directive « open data » ;
- les données API (Advanced Passenger Information) ;

- l'amélioration de la coopération internationale ;
- le nouveau code de la WADA (World Anti-Doping Agency) ;
- PRISM et autres programmes des services de renseignement.

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.

2.6.1.1 Contribution au débat sur la réforme européenne de la protection des données

Le Groupe « Article 29 » a apporté des contributions supplémentaires au débat sur la réforme de la protection des données, complétant sa prise de position détaillée de 2012.

Proposition de règlement général sur la protection des données

Le document de travail WP 200 aborde la question de savoir si toutes les dispositions permettant à la Commission européenne d'adopter des actes délégués et des actes d'exécution étaient effectivement justifiées et nécessaires.

Depuis l'entrée en vigueur du traité de Lisbonne, la Commission peut être habilitée à adopter ces actes. Les actes délégués reposent sur l'article 290 du TFUE et ils peuvent être adoptés pour compléter ou modifier certains éléments non essentiels d'un acte législatif (dans le cas présent, le règlement proposé). Les actes d'exécution reposent sur l'article 291 du TFUE et sont utilisés lorsque des conditions uniformes d'exécution des actes juridiquement contraignants de l'Union sont nécessaires.

Le groupe de travail énumère les critères pertinents pour déterminer si les actes d'exécution sont justifiés et pour établir leur nécessité. Il procède ensuite à une évaluation article par article de toutes les possibilités d'adoption d'actes d'exécution offertes.

Proposition de directive relative à la protection des données traitées dans les domaines de la police et de la justice pénale

Dans l'avis 1/2013, le groupe de travail formule d'autres orientations relatives à plusieurs éléments particuliers de la directive proposée. Il s'agit de l'utilisation des données concernant des personnes non suspectes, des droits des personnes concernées, de l'utilisation des analyses d'impact sur la vie privée et des pouvoirs des autorités chargées de la protection des données, notamment en ce qui concerne les informations confidentielles ou classifiées.

Le groupe de travail suggère d'abord de faire une distinction entre le traitement des données à caractère personnel concernant des personnes non suspectes et le traitement des données relatives à des personnes liées à une infraction particulière. Tous les groupes de personnes relevant de la catégorie générale des « personnes non suspectes » doivent bénéficier d'une protection particulière. Cela est d'autant plus vrai lorsque le traitement n'est pas effectué dans le cadre d'une enquête ou de poursuites pénales particulières.

Quant aux droits des personnes concernées, le groupe estime que les exemptions et restrictions actuellement applicables sont trop larges. Il est d'ailleurs indéfendable que, sans autre explication, les Etats membres soient autorisés à refuser le droit d'accès à des catégories entières de données à caractère personnel.

Le groupe de travail a encore noté qu'il est satisfait des amendements proposés par le rapporteur du Parlement européen qui imposent au secteur répressif des obligations en matière d'analyse d'impact sur la vie privée, ce qui n'était pas le cas avant.

Finalement, le groupe a estimé que la directive représente une grande avancée par rapport à la décision-cadre en vigueur concernant les dispositions consacrées aux missions et pouvoirs des autorités de protection des données. Elle ne contient non seulement des dispositions soulignant la nécessité de disposer d'une autorité indépendante pour contrôler toutes les opérations de traitement des données qui se déroulent dans le cadre de la directive, mais aussi un chapitre spécifique sur la coopération entre ces autorités.

Malheureusement, les dispositions de la directive sont bien moins précises que celles de la proposition de règlement. Si les autorités nationales ne possèdent pas des pouvoirs similaires dans toute l'Union européenne, il pourra être très difficile de préserver les droits des citoyens. Il se pourrait qu'une autorité soit habilitée, en vertu de sa législation d'exécution nationale, à entrer dans les locaux d'un service répressif pour y effectuer une inspection sans avoir préalablement obtenu le consentement de ce service, tandis qu'une autorité similaire d'un pays voisin pourrait ne pas y être autorisée et donc se voir refuser l'accès à ces locaux.

En ce qui concerne la situation des autorités de protection des données en matière d'information, la coopération pourrait se révéler d'autant plus compliquée si les pouvoirs de ces autorités restaient non harmonisés, comme c'est le cas actuellement. Le groupe de travail « Article 29 » propose donc que la directive mentionne les types d'informations dont l'accès doit être accordé aux autorités chargées de la protection des données dans le cadre de l'exercice de leurs missions de contrôle.

2.6.1.2 Recommandations sur les applications mobiles pour smartphones ou tablettes

ELe G29 a analysé les risques en matière de protection des données des applications mobiles. L'avis 2/2013 examine également la position des différents acteurs impliqués et précise les obligations légales à respecter en application de la directive.

En moyenne, un utilisateur d'un « smartphone » télécharge 37 applications

Ces « apps », désormais omniprésentes dans notre

vie quotidienne, sont proposées à un prix très faible ou encore gratuitement pour tout type de smartphone, tablette et même pour des téléviseurs interactifs.

Plusieurs centaines de milliers d'applications sont disponibles en téléchargement dans les « app stores », et le nombre de leurs utilisateurs croît aussi rapidement que l'offre sans que les dangers engendrés par leurs différentes fonctionnalités soient clairement appréhendés.

Les risques pour la vie privée

La forte imbrication entre les applications et le système d'exploitation des appareils permet techniquement d'accéder à un nombre de données beaucoup plus important qu'avec un logiciel isolé ou un navigateur traditionnel, à moins que des restrictions aient été mises en place.

Les applications sont capables de collecter - souvent à l'insu de l'utilisateur - de nombreuses données à partir de l'appareil et de les traiter dans le but d'offrir des services nouveaux et innovants.
Dans certains cas, elles ont notamment accès au carnet d'adresses, données de localisation, informations bancaires, photos, vidéos et même aux données provenant de différents capteurs comme le microphone, la boussole ou encore le détecteur de mouvement.

Les données collectées peuvent être transmises en quelques secondes à différentes parties tierces localisées n'importe où autour du globe : les développeurs des applications, les fabricants des appareils et des systèmes d'exploitation, les « app stores » ou encore d'autres parties tierces qui traitent les données à caractère personnel (régies publicitaires, prestataires d'analyse, opérateurs télécom).

Les développeurs de ces applications, qui parfois ignorent les exigences liées à la protection des données à caractère personnel, peuvent être à l'origine de risques importants pour la vie privée et la réputation des utilisateurs de ces appareils.

Importance du consentement éclairé de l'utilisateur

Le manque de transparence et d'emprise de l'utilisateur sur le recours à et l'utilisation de ses données personnelles constitue donc un risque majeur pour la protection des données. L'information claire et spécifique de l'utilisateur doit être à chaque fois garantie préalablement à la mise en œuvre, et l'accès aux données doit pouvoir être bloqué de façon ponctuelle ou systématique, au choix de l'utilisateur.

2.6.1.3 Analyse de la notion de « limitation de la finalité »

Le groupe de travail a analysé la notion de « limitation de la finalité » dans son avis 3/2013. Dans des documents de travail antérieurs, le groupe avait déjà précisé le concept de données à caractère personnel, les notions de « responsable du traitement » et de « sous-traitant », le principe de la responsabilité et le consentement.

Le principe de finalité prend une importance particulière dans le contexte de la réforme de la protection des données au niveau européen. Même s'il y a un consensus sur le principe de la limitation de la finalité en soi, sa signification exacte et ses exceptions font l'objet de discussions. Pour cette raison, il importe à ce stade de clarifier la portée de ce principe pour ne pas risquer l'adoption d'un texte en dessous des standards de la directive de 1995.

Le groupe de travail n'analyse non seulement le principe de la limitation de la finalité sous le régime actuel de la directive 95/46/CE, mais il formule également des recommandations pour l'avenir.

Définition du principe de finalité

L'utilisation des données personnelles (y compris des images et sons) d'un individu doit être strictement limitée à une finalité explicitement déterminée au préalable.

La collecte, l'enregistrement et l'utilisation de ces données personnelles sont strictement limités à ce qui est nécessaire pour atteindre des buts expressément fixés d'avance par l'administration, l'entreprise, l'association, le professionnel ou l'indépendant qui s'y livre.

Ceux-ci ne doivent pas les transmettre à d'autres organismes ou personnes, sauf si ces derniers en ont besoin dans le cadre de la réalisation des mêmes buts et ne les utiliseront que de manière compatible.

Exemples

Dans son document de travail, le G29 présente un grand nombre d'exemples pour illustrer le principe de la limitation de la finalité en pratique (voir Annexe 3 de l'avis, p.51 à 70), notamment dans le domaine du marketing direct, de la vidéosurveillance, des registres de la population, de l'échange de données entre administrations, du profilage ou encore du smart metering.

2.6.1.4 Règles d'entreprise contraignantes (BCR) applicables aux sous-traitants

En 2010, la Commission européenne a adopté une nouvelle série de clauses contractuelles types pour les transferts de données entre les responsables du traitement et les sous-traitants, afin de répondre à l'expansion des activités de traitement et, en particulier, à l'apparition de nouveaux modèles de gestion pour le traitement international des données à caractère personnel. Ces clauses contractuelles types de 2010 contiennent des dispositions spécifiques autorisant, sous certaines conditions, l'externalisation des activités de traitement vers des sous-traitants ultérieurs, tout en offrant des garanties suffisantes concernant les données personnelles transférées.

Garantir en permanence un niveau de protection adéquat grâce aux outils créés pour encadrer les transferts internationaux de données se révèle difficile, principalement à cause de la complexité et du nombre croissants de transferts internationaux de données (résultant, par exemple, de l'informatique en nuage, de la mondialisation, des centres de données, des réseaux sociaux, etc.).

Si les clauses contractuelles types semblent suffire pour encadrer les transferts non massifs effectués par un exportateur de données établi dans l'UE vers un importateur de données établi dans un pays tiers, les professionnels de la sous-traitance, eux, demandent depuis longtemps un nouvel instrument juridique qui permette une approche globale de la protection des données dans le milieu de la sous-traitance et qui reconnaisse officiellement les règles internes que les organisations peuvent avoir mises en œuvre. Ce nouvel instrument juridique permettrait d'encadrer les transferts massifs effectués par un sous-traitant vers des sous-traitants ultérieurs appartenant à la même organisation et agissant pour le compte d'un responsable du traitement, selon ses instructions.

Vu l'intérêt croissant que portait l'industrie à un tel instrument, le groupe de travail a adopté, en 2012, un document de travail qui établissait un tableau présentant les éléments et principes que doivent contenir les règles d'entreprise contraignantes applicables aux sous-traitants et un formulaire de demande d'approbation de ces règles. Le groupe de travail a confirmé le lancement des règles d'entreprise contraignantes applicables aux sous-traitants le 5 décembre 2012.

2.6.1.5 Examen du modèle d'AIPD sur les réseaux et systèmes de relevés intelligents

Le groupe « Article 29 » a examiné le modèle d'analyse d'impact relative à la protection des données pour les réseaux intelligents et les systèmes de relevés intelligents (modèle d'AIPD) élaboré par le groupe d'experts 2 de la task-force sur les réseaux intelligents de la Commission européenne.

Le modèle d'AIPD devrait décrire les opérations de traitement envisagées, évaluer les risques pour les droits et libertés des personnes concernées, présenter les mesures envisagées pour faire face aux risques, les garanties, les mesures de sécurité et les mécanismes visant à assurer la protection des données à caractère personnel et à démontrer la conformité avec la directive 95/46/CE, en tenant compte des droits et intérêts légitimes des personnes concernées, entre autres par les données.

A partir des données détaillées sur la consommation d'énergie collectées par l'intermédiaire des compteurs intelligents, il est possible de déduire beaucoup d'informations sur l'utilisation de produits ou dispositifs spécifiques par les consommateurs, leurs habitudes quotidiennes, leur façon de vivre, leurs activités, leur mode de vie et leur comportement.

Par conséquent, l'utilisation de réseaux intelligents et de systèmes de relevés intelligents crée pour les personnes concernées de nouveaux risques susceptibles d'avoir des conséquences dans différents domaines (par exemple, la discrimination en matière de prix, le profilage à des fins de publicité comportementale, la fiscalité, l'accès des services répressifs, la sécurité des ménages). Auparavant, ces risques n'existaient pas dans le secteur de l'énergie, mais se trouvaient déjà typiquement dans d'autres environnements (télécommunications, commerce électronique et web 2.0).

Après analyse, le groupe de travail regrette que le modèle d'AIPD soumis n'aborde pas directement les incidences réelles sur les personnes concernées, comme, par exemple, les pertes financières dues à des factures inexactes, la discrimination en matière de prix ou les actes criminels facilités par un profilage non autorisé. Par conséquent, le groupe de travail «Article 29» considère que le modèle d'AIPD, sous sa forme actuelle, ne saurait atteindre son objectif. L'AIPD ne prévoit pas d'outil pratique pour analyser les incidences sur les personnes concernées.
Si les risques et leurs

conséquences sur les personnes concernées ne sont pas considérés dans leur intégralité, il n'est pas possible de déterminer et d'appliquer correctement les contrôles et les garanties nécessaires.

2.6.1.6 Examen du paquet « frontières intelligentes » de la Commission européenne

Le 28 février 2013, la Commission européenne a présenté des propositions concernant la création d'un système d'entrée/sortie (EES) et d'un programme d'enregistrement des voyageurs (RTP) pour l'espace Schengen, connues sous le nom de paquet «frontières intelligentes». Une proposition visant à apporter au code frontières Schengen certaines modifications nécessaires a également été présentée.

La proposition concernant le système d'entrée/sortie repose sur un système de stockage centralisé des données d'entrée et de sortie relatives aux ressortissants de pays tiers admis dans l'espace Schengen dans le cadre de séjours de courte durée, qu'ils soient tenus ou non de disposer d'un visa Schengen. Au lieu du système consistant à apposer des cachets sur les passeports de ces ressortissants à leur entrée dans l'espace Schengen et à leur sortie, les données relatives à l'identité des visiteurs, de même qu'à la durée et au motif du séjour seront encodées dans le système à l'entrée et seront vérifiées à la sortie, afin de garantir que les ressortissants de pays tiers n'auront pas dépassé la durée de séjour autorisée. La proposition d'EES concerne un système reposant au départ sur les données à caractère personnel nécessaires à l'identification de personnes, les « données biométriques » n'étant introduites qu'après trois ans. Après deux ans, il sera procédé à une évaluation afin de déterminer si les services répressifs et les pays tiers devraient avoir accès au système.

Le RTP propose un programme d'enregistrement pour les voyageurs se rendant fréquemment dans l'espace Schengen, par exemple des hommes d'affaires. Les ressortissants de pays tiers peuvent demander le statut de voyageur enregistré et franchir les frontières plus rapidement. Le RTP reposera sur un registre central avec des données biométriques et un jeton d'authentification détenu par le voyageur et contenant un identifiant unique.

Dans son avis, le groupe de travail « Article 29 » a émis des réserves au sujet des propositions du point de vue de la protection des données. Il a conclu que la valeur ajoutée de l'EES pour la réalisation des objectifs qu'il s'est fixés ne satisfait pas au principe de nécessité qui peut justifier une atteinte aux droits prévus à l'article 8 de la Charte des droits fondamentaux de l'Union européenne. De plus, il a estimé que la valeur ajoutée de l'EES n'est pas proportionnelle à l'ampleur de ses répercussions sur les droits fondamentaux pour chacun de ses objectifs, et que d'autres solutions peuvent permettre d'atteindre ces objectifs.

2.6.1.7 Guidance concernant le consentement pour les « cookies »

Dans son document de travail 2/2013, le G29 a donné des recommandations pratiques concernant l'utilisation des cookies et a clarifié davantage les exigences d'un consentement valable dans ce contexte. Ce document complète l'avis du groupe de 2011 et celui de 2012 sur les exceptions au principe du consentement explicite.

La directive « e-privacy » (Directive 2002/58/CE), révisée en 2009 et transposée en droit national par la loi du 28 juillet 2011 (portant modification de la loi modifiée du 30 mai 2005 concernant la vie privée dans

le secteur des communications électroniques), stipule qu'il est seulement possible de placer des cookies sur l'ordinateur de l'utilisateur sous condition de recevoir son consentement explicite. Ce consentement peut prendre différentes formes en pratique. Il peut s'agir notamment d'une notice immédiatement apparente sur la page d'accueil d'un site et signalant l'emploi de cookies.

Pour qu'une telle notice d'information puisse être considérée comme induisant un consentement valide, même implicite, l'information de l'utilisateur devra être plus spécifique et renvoyer sur une page comprenant des explications complémentaires et une possibilité simple et conviviale pour l'utilisateur de s'opposer au traitement de ses données via des cookies. De plus, la possibilité de refuser le recours aux cookies doit être offerte à l'utilisateur avant que le traitement des données ne commence, c'est-à-dire que son acceptation implicite doit être constatée avant que les cookies soient placés. Une autre exigence veut que le consentement soit être donné librement et de manière non ambiguë. En d'autres mots, il ne doit pas y avoir de doute que l'utilisateur ait donné son consentement, il faut qu'il ait un choix réel et qu'il n'y ait pas de risque de déception, de coercition ou des conséquences négatives s'il choisit de ne pas donner son consentement.

2.6.1.8 Demande d'éclaircissements sur l'affaire « PRISM »

Le groupe de l'article 29 a décidé d'évaluer l'impact du programme de surveillance « PRISM » de la NSA (Agence nationale de la sécurité américaine) et a saisi la Commission européenne afin d'obtenir des clarifications.

Le programme « PRISM » ne cesse de susciter la controverse en Europe. Selon les révélations de l'ancien consultant de la NSA Edward Snowden, ce programme permettrait à la NSA d'espionner les communications électroniques mondiales échangées sur les services en ligne comme Facebook, Google ou Skype.

Dans un courrier du 13 août 2013 à Madame Viviane Reding, vice-présidente de la Commission européenne, le groupe a notamment demandé des éclaircissements sur :

- la nature exacte des informations collectées en vertu des législations américaines,
- les conditions dans lesquelles les autorités américaines peuvent y accéder,

- le type de contrôle exercé aux Etats-Unis sur ces procédures et

- sur les voies de recours dont peuvent disposer les citoyens européens.

Il s'agit par ailleurs d'apprécier dans quelle mesure les législations américaines sont en accord avec le droit international et européen en matière de protection des données.

Le G29 a estimé qu'il lui appartient d'entamer une investigation indépendante même s'il est déjà représenté dans un groupe de travail UE-US qui s'intéresse à la question de l'accès par les services de renseignements américains aux données de citoyens non-américains.

Le 27 novembre 2013, la Commission européenne a exposé les mesures qui doivent être prises pour rétablir la confiance dans les transferts de données entre l'UE et les Etats-Unis, en réponse aux vives préoccupations suscitées par les révélations sur les programmes américains de collecte de renseignements à grande échelle, qui ont altéré les relations transatlantiques.

La réponse de la Commission a pris la forme :

1. d'une communication sur les transferts de données transatlantiques, qui présente les enjeux et les risques faisant suite aux révélations sur les programmes américains de collecte de renseignements, ainsi que les mesures à prendre pour y répondre ;

2. d'une analyse du fonctionnement de la «sphère de sécurité», qui réglemente les transferts de données à des fins commerciales entre l'Union européenne et les Etats-Unis ; et

3. d'un rapport sur les conclusions du groupe de travail UE-Etats-Unis sur la protection des données, créé en juillet 2013.

Par ailleurs, la Commission européenne a présenté aussi son réexamen des accords en vigueur sur les données des dossiers passagers (données PNR) et sur le programme de surveillance du financement du terrorisme (TFTP), qui réglementent les échanges de données à des fins répressives dans ces secteurs.

2.6.1.9 Action de redressement concertée contre Google

En octobre 2012, les autorités de protection des données européennes avaient donné quatre mois à Google pour mettre en conformité ses règles de confidentialité avec la législation européenne. A l'issue de ce délai et d'une réunion avec des représentants de Google Inc. en mars 2013, aucune mesure concrète n'avait été adoptée par la firme de Mountain View. Leurs requêtes n'ayant pas été prises en compte, six autorités européennes de protection des données (France, Allemagne, Italie, Pays-Bas, Espagne, Royaume-Uni) ont décidé d'engager une action concertée contre Google.

L'autorité française CNIL avait été mandatée pour analyser la politique de confidentialité de Google, introduite le 1er mars 2012. Cette politique simplifiée permet au géant américain d'unifier les informations provenant de plusieurs services, autrefois séparés, comme Gmail, Google+ ou YouTube. Google peut ainsi utiliser les données d'un utilisateur recueillies lors d'une requête sur son moteur de recherche pour lui proposer des publicités ciblées sur un autre de ses services.

L'analyse menée par la CNIL ne permettait pas de s'assurer que Google respecte les principes essentiels des règles européennes en matière de protection des données personnelles. Les autorités européennes recommandaient notamment

une information plus claire des personnes et un meilleur contrôle par les utilisateurs de la combinaison de données entre les nombreux services offerts par Google.

Après cette analyse générale, il appartenait à chaque autorité nationale de poursuivre ses investigations au regard de son droit national.

Le 28 novembre 2013, l'autorité de protection des données néerlandaise a conclu, après une investigation, que la politique de confidentialité de Google ne respectait pas la loi des Pays-Bas sur la protection des données. L'investigation a notamment montré que les utilisateurs n'étaient pas informés préalablement de manière adéquate et que leur consentement n'était pas demandé.

L'autorité de protection des données française CNIL a même prononcé au début de l'année 2014 une amende maximum de 150 000 € à l'encontre de Google. En décembre 2013, l'équivalent espagnol de la CNIL avait déjà infligé une amende de 900 000 € à l'entreprise de Mountain View. Les deux autorités ont conclu, comme l'autorité néerlandaise en novembre 2013, que la politique de confidentialité de Google ne respectait pas la loi sur la protection des données de leur pays.

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 2013, le T-PD s'est penché principalement sur :

- la modernisation de la Convention 108 ;
- la protection des données médicales ;
- 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 collecte et le traitement de données biométriques et
- la liberté d'expression et la démocratie à l'ère numérique (Résolution de Belgrade).

L'Uruguay devient le premier pays non européen à adhérer à la Convention 108

L'Uruguay est devenu le premier Etat non européen à adhérer

à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, aussi appelée la Convention 108, et à son Protocole additionnel. Etant ouverte à la signature de tous les Etats, la Convention 108 est le seul outil juridiquement contraignant ayant le potentiel d'être appliqué à l'échelle mondiale et assurant la certitude juridique et la prévisibilité nécessaires dans les relations internationales.

La Convention est entrée en vigueur à l'égard de l'Uruguay le 1er août 2013. L'Uruguay est le 45e Etat à devenir partie à la convention.

Le Conseil de l'Europe alerte les gouvernements sur les risques du suivi numérique et de la surveillance

Le Conseil de l'Europe a attiré l'attention de ses 47 Etats membres sur les dangers que présentent le suivi numérique et les autres technologies de surveillance pour les droits de l'homme, la démocratie et la prééminence du droit, et a rappelé la nécessité de veiller à la légitimité de leur utilisation.

Dans une Déclaration aux gouvernements, le Comité des Ministres a fait observer que les lois autorisant une surveillance excessive des citoyens peuvent porter atteinte à leur vie privée et inhiber la liberté d'expression et la liberté des médias. Cette déclaration est venue à un moment où ce sujet était au cœur de l'actualité avec les révélations sur l'espionnage électronique de masse par l'agence américaine NSA.

Le Comité a rappelé que les mesures de suivi et de surveillance mises en œuvre par les forces de l'ordre doivent être conformes aux normes du Conseil de l'Europe en matière de droits de l'homme, telles qu'énoncées par la Convention européenne des droits de l'homme. Ces mesures doivent aussi respecter rigoureusement les limites, les exigences et les garanties énoncées dans la Convention 108.

La Déclaration a également attiré l'attention sur les implications pénales d'activités de surveillance et de suivi illicites et sur l'importance de la Convention de Budapest sur la cybercriminalité pour relever ce défi.

Enfin, le Comité a encouragé les Etats à mettre en place des contrôles à l'exportation adéquats pour éviter qu'une mauvaise utilisation des technologies n'affaiblisse les normes en matière de droits de l'homme.

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. A la lumière des informations récentes sur les services de renseignement, le Groupe de Berlin a rappelé dans un document de travail qu'il a mis l'accent à plusieurs occasions sur l'importance du secret des correspondances. Selon le groupe, l'interception de ces informations par les services de renseignement peut être nécessaire pour des raisons légitimes, mais doit rester l'exception.

Par ailleurs, le groupe a adopté des documents de travail sur le traçage sur Internet, sur la publication de données personnelles sur Internet et sur la surveillance aérienne lors de deux réunions en 2013 à Prague et à Berlin.

2.6.3.1 Traçage et protection de la vie privée sur Internet

Le document de travail du Groupe de Berlin concernant le traçage sur Internet analyse l'impact de cette pratique sur la vie privée des citoyens et met l'accent sur les principes de « choix » et de « contrôle ».

Le traçage sur Internet désigne la collecte, l'analyse et l'utilisation

Les activités en 2013

de données concernant l'activité des utilisateurs sur un ordinateur ou un autre appareil pour les combiner et les analyser à des fins multiples (charitable, philanthropique ou commerciale). Cela peut inclure les données d'enregistrement de l'utilisateur, ses activités de recherche, la manière dont il interagit avec des publicités ou avec des services sur Internet. Les intérêts de l'utilisateur, ses opinions politiques ou encore son état pathologique peuvent être déduits des informations collectées.

Aujourd'hui les professionnels du marketing peuvent surveiller chaque aspect du comportement d'un utilisateur identifiable sur Internet. Il serait même possible de reconstituer toute l'histoire « en ligne » d'une personne.
Le groupe de travail a abordé la question des risques pour la vie privée des utilisateurs en formulant plusieurs recommandations :

- L'utilisateur doit être informé préalablement sur les finalités de la collecte et ces finalités ne peuvent pas être modifiées sans son accord.
- Il est interdit d'utiliser des éléments de traçage invisibles.
- L'utilisateur doit être notifié de manière intelligible lorsque le traçage est en cours.
- Il faut que l'utilisateur puisse vraiment choisir s'il souhaite être tracé ou non.

- Les paramètres par défaut devraient être configurés de façon que l'utilisateur ne soit pas tracé (« Privacy by default »).

2.6.3.2 Droit à l'oubli sur Internet et indexation de contenus de sites Web

Avec la structure actuelle de l'Internet, il est difficile d'instaurer un vrai « droit à l'oubli » (« Right to be forgotten »). Il devient difficile, voire impossible, d'effacer des données une fois qu'elles sont publiées. L'Internet n'oublie jamais et il n'existe pas (encore) de bouton d'effacement. Même si on arrive à effacer le contenu sur le site original, il est possible que cette information ait déjà été copiée et se retrouve sur d'autres sites.

Mais les droits des individus peuvent toutefois être protégés à travers les outils disponibles aux administrateurs de sites web. Il existe notamment plusieurs moyens permettant de rendre des contenus « invisibles » aux moteurs de recherche. Ce procédé est complètement volontaire et basé sur la coopération entre les parties concernées.

Le groupe a fait plusieurs recommandations aux administrateurs de sites web :

- Ils devraient informer les utilisateurs sur les données qu'ils collectent et à quelles fins ils le font. Ils devraient leur fournir un moyen facile pour accéder aux données, les modifier ou les effacer.

- A la demande d'un utilisateur, ils devraient effacer les données le concernant et faire réindexer cette partie du site auprès des moteurs de recherche.

Dans son document de travail, le groupe s'est également adressé aux moteurs de recherche avec les recommandations suivantes :

- Ils devraient toujours respecter les préférences d'indexation d'un site web.

- Ils devraient améliorer la communication avec les sites web pour être notifiés immédiatement en cas de changements en matière de préférence d'indexation.

- Ils devraient offrir des documents de guidance aux sites web concernant l'indexation.

- Ils devraient être plus transparents quant aux intervalles de l'indexation des sites web.

2.6.3.3 Protection de la vie privée dans le cadre de la surveillance aérienne

La surveillance aérienne désigne la surveillance à l'aide d'images ou de vidéos prises à partir d'un véhicule qui vole, comme par exemple un drone.

Plusieurs aspects de ce type de surveillance suscitent des inquiétudes concernant la protection de la vie privée. Cette surveillance peut notamment être cachée, intrusive, sans discernement et/ou continue. Si beaucoup de gens se prononcent en faveur de ce type de surveillance (p.ex. dans le cadre de catastrophes naturelles), le groupe de travail craint que cette technologie puisse être utilisée à d'autres fins plus intrusives pour la vie privée. Un autre risque est le traçage des personnes qui pourra se développer, si une telle surveillance persiste dans le temps. Selon le groupe de travail, ce type de surveillance peut même s'avérer plus intrusif que la vidéosurveillance.

Le groupe de travail a fait plusieurs recommandations afin de préserver la protection de la vie privée des citoyens :

- L'utilisation des moyens de surveillance aériens devrait être limitée à des fins spécifiques (p.ex. pour la recherche de personnes disparues, la surveillance des frontières, etc.).

- L'utilisation de ces images d'agences gouvernementales ou comme preuve au tribunal

devrait seulement être possible avec un mandat judiciaire.

- Dans la mesure du possible, le public devrait être informé de l'utilisation des moyens de surveillance aérienne.
- La surveillance devrait être limitée à une zone aussi réduite que possible.

2.6.4 Le séminaire européen « Case Handling Workshop »

L'autorité de protection des données de Bosnie-Herzégovine a organisé le séminaire européen « Case Handling Workshop » à Sarajevo, les 2 et 3 octobre 2013.

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

En 2013, le séminaire a abordé les thèmes suivants :

- Nouveaux médias :
  - Protection des données sur Internet
  - Réseaux sociaux, Internet et enfants
- Défis concernant la protection des données et les applications mobiles
- Transferts de données internationaux des banques et administrations fiscales
- Marketing direct : avantages et conséquences
- Vidéosurveillance dans les secteurs public et privé
- Protection des données dans le domaine de la santé
- Protection des données dans le domaine de la police
- Collecte illicite de données biométriques

2.6.5 Conférence Internationale des commissaires à la protection des données

Du 23 au 26 septembre, l'autorité de protection des données polonaise a organisé la 35e Conférence Internationale des commissaires à la protection des données et de la vie privée à Varsovie. Le thème était *« La direction du développement de la protection de la vie privée dans un monde incertain »*.

La conférence internationale a eu lieu pour la première fois en 1979. Elle est constituée d'une séance ouverte à tous les experts dans le domaine de la protection des données, d'une session fermée réservée aux autorités

de protection des données ainsi que de plusieurs événements parallèles organisés par les organisations internationales et les ONG.

Les séances de la conférence étaient réparties en trois volets pour permettre une discussion plus approfondie :

1. Les réformes dans le monde entier. L'interopérabilité entre les régions.

2. La protection des données personnelles et la technologie.

3. Les principaux acteurs : perspectives, rôles, intérêts.

A la fin des séances à huis clos, les autorités des différents pays ont adopté la « *Déclaration de Varsovie* » sur l'omniprésence des applications mobiles et 8 résolutions supplémentaires :

- résolution sur l'accréditation ;
- résolution sur le profilage ;
- résolution sur la direction stratégique de la conférence ;
- résolution sur la coopération internationale ;
- résolution sur la nécessité d'ancrer la protection des données et de la vie privée en droit international ;
- résolution sur la transparence des traitements de données à caractère personnel ;
- résolution sur l'éducation numérique ;
- résolution sur le traçage numérique et la protection de la vie privée.

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

Du 16 au 17 mai, le Portugal a accueilli la conférence de printemps *(« Spring Conference »)* des autorités européennes à la protection des données à Lisbonne.

Après l'édition de 2012 qui a eu lieu au Luxembourg, l'autorité de contrôle portugaise a invité cette année-ci les délégués des autorités des autres pays européens ainsi que les représentants de la Commission européenne, du Conseil de l'Europe et de l'OECD.

« Protecting Privacy : the challenges ahead »

Comme l'année passée, le thème principal de la conférence était la réforme de la législation européenne sur la protection des données. Les textes légaux au niveau du Conseil de l'Europe et de l'Union européenne sont actuellement en cours de révision.

Lors des différentes séances, les commissaires ont notamment discuté des moyens pour rendre la protection des données plus efficace en pratique et pour garantir les droits des individus sur Internet. D'autres sujets abordés étaient la sécurité des données et le futur rôle des autorités de protection des données européennes.

Resolution on the Future of Data Protection in Europe

A la fin de la conférence, les commissaires ont adopté plusieurs résolutions dont une sur l'avenir de la protection des données en Europe. Ils rendent attentifs au fait que les décisions qui seront prises maintenant auront un impact important sur le droit fondamental à la protection des données des citoyens dans les années à venir.

Les autorités européennes ont par ailleurs adopté des résolutions « *pour assurer la protection des données dans une zone de libre-échange transatlantique* » et « *pour assurer un niveau adéquat en matière de protection des données chez Europol* ».

2.6.7 Conférence de l'Association francophone des autorités à la protection des données

Les 21 et 22 novembre, l'Association francophone des autorités de protection des données personnelles (AFAPDP) a organisé à Marrakech, en partenariat avec l'Organisation internationale de la Francophonie (OIF) et la Commission Nationale de contrôle de la protection des données à caractère personnel (CNDP) du Maroc, la 7e Conférence sur la protection des données personnelles de l'AFAPDP.

Cette conférence a été l'occasion de traiter des questions qui interpellent les autorités de protection des données à caractère personnel. Les discussions ont porté sur la défense des libertés sur Internet, la protection des données personnelles et sur la place des appareils et services mobiles dans la société. Sur ces deux points, les visions et les pratiques singulières dans la Francophonie ont apporté un regard nouveau au débat international.

La conférence a permis aux autorités de protection des données personnelles et aux pays francophones désireux d'adopter une loi de protection des données d'échanger, au cours de deux ateliers pratiques, sur la gestion des communications externes et des médias et l'exercice du pouvoir de contrôle.

2.6.8 Révision des lignes directrices de l'OCDE sur la vie privée

Les lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données à caractère personnel ont été révisées en 2013. L'objectif des lignes directrices, adoptées le 23 septembre 1980, reste le même: protéger la vie privée et les données personnelles, tout en évitant des restrictions inutiles aux flux transfrontières de données. Les changements les plus significatifs concernent la responsabilisation des entreprises et acteurs publics et les notifications des violations de sécurité.

Dans la version de 2013, un responsable du traitement doit avoir un « programme de gestion de la vie privée » et il doit être préparé à le présenter sur demande à une autorité de protection des données. Les lignes directrices introduisent aussi le concept du « privacy risk assessment », qui doit permettre d'évaluer l'impact d'un traitement sur la vie privée des personnes. Le texte fait par ailleurs référence aux « privacy enforcement

authorities » (autorités de protection des données), ce qui n'était pas le cas dans l'ancienne version.

Un autre point important du texte révisé concerne les notifications des violations de sécurité. Une telle notification doit être faite par le responsable du traitement aux autorités de protection des données lorsqu'il y a une « faille de sécurité significative touchant à la protection des données à caractère personnel ». Si des citoyens de plusieurs pays sont concernés, les lignes appellent à une coopération transfrontière.

Gérard Lommel (Vice-président G29), Christopher Graham (Information Commissioner UK) et Isabelle Falque-Pierrotin (Présidente G29)

Les lignes directrices, non contraignantes, représentent les engagements politiques des 34 pays membres de l'OCDE. Elles ont été présentées lors de la conférence internationale des commissaires à la protection des données et de la vie privée qui s'est tenue à Varsovie du 23 au 26 septembre 2013.

2.6.9 La CNPD devient membre du Global Privacy Enforcement Network (GPEN)

En 2013, la CNPD est devenue membre du « Global Privacy Enforcement Network » (GPEN). Le GPEN a été établi pour faciliter la coopération transfrontalière entre autorités de protection des données.

En 2007, les gouvernements des pays de l'OCDE ont adopté une recommandation relative à la coopération transfrontière dans l'application des législations protégeant la vie privée. Cette recommandation a fait appel aux pays membres de mettre en place un réseau informel des autorités chargées de protéger la vie privée pour :

- débattre des aspects pratiques de la coopération pour l'application des lois protégeant la vie privée,
- échanger des pratiques exemplaires face aux problèmes transfrontières,
- œuvrer à la définition de priorités communes en matière d'application des lois, et
- soutenir des initiatives et campagnes conjointes en matière d'application des lois et de sensibilisation.

L'initiative était motivée par une prise de conscience du fait que l'évolution de la nature et du volume des flux transfrontières de données ont augmenté les risques pour la vie privée des personnes physiques, et elle a fait ressortir le besoin d'une meilleure coopération entre les autorités chargées de les protéger.

La recommandation s'appuie sur les Lignes directrices de l'OCDE de 1980 sur la vie privée, qui demeurent un énoncé influent des principes qui fondent la protection de la vie privée, plus de 30 ans après leur adoption.

3 Les temps forts de 2013

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

3.1 Conférence de M. Dean Spielmann à l'occasion des 10 ans de la CNPD

Le 28 janvier 2013, la Commission nationale pour la protection des données a organisé une conférence de Monsieur Dean Spielmann, Président de la Cour Européenne des Droits de l'Homme, sur le thème « *La protection des données dans la jurisprudence de la Cour Européenne des Droits de l'Homme de Strasbourg* ». La conférence s'est tenue dans le nouveau bâtiment administratif de l'Etat à Esch-Belval en présence de Monsieur François Biltgen, Ministre de la Justice, Ministre des Communications et des Médias.

28 janvier 2013 : Septième Journée de la Protection des Données

Pourquoi le 28 janvier ? M. Spielmann en parle dans son introduction à l'occasion de la célébration du 10e anniversaire de la CNPD : « *Au niveau européen, on sait que le Conseil de l'Europe a été, en quelque sorte, un pionnier en la matière puisque, dès 1973 et 1974, des recommandations furent adoptées dans le domaine de la protection des données et que, surtout, le 28 janvier 1981, la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, dite Convention 108, fut ouverte à la signature des Etats membres du Conseil de l'Europe.* »

La « Convention 108 » a été le premier instrument international juridiquement contraignant en la matière. Depuis plus de 30 ans, la loi vise à protéger toute personne contre l'utilisation abusive des données qui la concernent et à assurer la transparence quant aux fichiers et traitements des données personnelles.

Le Conseil de l'Europe, avec le soutien de la Commission européenne, a proclamé solennellement le 28 janvier de chaque année comme Journée de la Protection des Données. Son but est de sensibiliser les citoyens européens sur l'importance de la protection de leurs données personnelles et du respect de leurs libertés et droits fondamentaux, en particulier de leur vie privée.

La protection des données dans la jurisprudence de la Cour Européenne des Droits de l'Homme de Strasbourg

Lors de son exposé, Monsieur Spielmann a résumé les enjeux actuels en matière de protection des données :

« Il importe de rappeler que le traitement et l'utilisation automatisés de données à caractère personnel, s'ils sont récents, correspondent à un phénomène mondial dont les effets sont largement bénéfiques. Nous en sommes les acteurs et les témoins dans tous les actes de notre vie quotidienne. La réservation de billets de train ou d'avion, les demandes de remboursements de frais médicaux, les démarches relatives à l'obtention de documents d'identité sont des exemples non exhaustifs des circonstances très nombreuses dans lesquelles nous sommes conduits à divulguer à autrui, notamment aux administrations, des informations de nature tout à fait privée, voire intime. Toutes ces données sont non seulement collectées, ce qui, en soi, ne soulève pas de difficulté majeure, mais elles peuvent surtout être traitées, croisées, conservées, tout cela sans que nous en soyons même informés. Ceci a été grandement facilité par les progrès de la technologie dont nous sommes les principaux bénéficiaires en raison de l'amélioration que cela amène dans notre vie quotidienne. Cependant, il arrive que nous en soyons les victimes.
Il n'est pas surprenant que les autorités nationales aient très rapidement compris l'usage qui pouvait être fait de ces données personnelles multipliées à l'infini et à partir desquelles un portrait très complet de chacun d'entre nous peut être effectué. Certes, les raisons pour lesquelles les Etats démocratiques font usage des données personnelles sont principalement liées à la lutte contre le terrorisme et la criminalité, mais également à l'exercice efficace par l'État de ses fonctions administratives, objectifs auxquels nous ne pouvons que souscrire. Toutefois, il s'agit clairement d'ingérences dans notre vie privée. (…) La Cour accepte ces ingérences, mais exige que celles-ci soient prévues par la loi (une loi accessible et prévisible dans ses effets) ; qu'elles poursuivent un but légitime ; qu'elles soient nécessaires dans une société démocratique. »

De gauche à droite : Pierre Weimerskirch, Thierry Lallemang, François Biltgen, Gérard Lommel et Dean Spielmann

Après cette introduction, le Président de la Cour Européenne des Droits de l'Homme a consacré la première partie de son intervention à la collecte des données. Il a parlé, dans un second temps, de la conservation et de l'exploitation des données. Puis, il a évoqué la question de la divulgation des données et l'accès des personnes aux données qui les concernent.

10 ANS

2002 – 2012

COMMISSION NATIONALE
POUR LA PROTECTION
DES DONNÉES

Commission Nationale
pour la Protection
des Données

2002-2012 : 10 ans CNPD

Tout commence dans les années 70… Face à l'émergence de l'informatique dans les administrations publiques, il devenait nécessaire de créer des règles juridiques pour que les données recueillies sur les citoyens se limitent à ce qui est légitime et nécessaire. Ainsi, le 31 mars 1979, une loi est votée afin de réglementer l'utilisation des données nominatives dans les traitements informatiques. Le Luxembourg devient alors le 8e pays au monde à se doter d'une législation en la matière.

Si la loi de 1979 était adaptée à son époque, elle était dépassée à la fin des années 90. La nouveauté ? Avec le développement des ordinateurs, l'informatique devient omniprésente dans la vie des citoyens. Il devenait donc impératif de rafraîchir la législation. C'est ainsi que cette dernière a été abrogée et remplacée par la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Instituée par la loi du 2 août 2002, la CNPD est chargée de vérifier la légalité des traitements des données à caractère personnel et d'assurer le respect des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée. Face à l'essor croissant des flux de données personnelles par voies électroniques (e-mails, SMS, réseaux sociaux, etc.), sa mission consiste 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.

Que ce soit auprès des commerces, des banques, des acteurs du secteur de la santé ou des ministères, l'objectif de la CNPD est de promouvoir au fil des années une véritable culture de la protection des données au Luxembourg. Dès le début, elle a opté pour une approche d'information, de sensibilisation et de responsabilisation des différents acteurs.

Après ses premières années d'existence, elle s'est dégagée de sa fonction purement administrative pour se consacrer davantage à d'autres tâches telles que ses fonctions de consultation, de guidance et de coopération avec les différents acteurs. Elle fut également plus disponible à répondre aux plaintes et aux demandes d'information formulées par les citoyens. Davantage connue qu'à ses débuts, l'autorité de protection des données luxembourgeoise rencontre désormais une oreille attentive auprès du gouvernement, des administrations et des entreprises.

En vue de vérifier le respect des obligations légales, la Commission nationale procède à des contrôles et investigations. Ce domaine va de plus en plus gagner en importance. Mais auprès du grand public, sa principale mission reste l'information et la sensibilisation.

3 Les temps forts de 2013

Gérard Lommel (Président de la CNPD)

François Biltgen (Ministre des Communications et des Médias)

M. Spielmann a conclu son exposé en estimant « *que ce soit au niveau national ou au niveau européen, la protection des données personnelles aura été considérablement améliorée depuis le début des années soixante-dix. Des instances et des mécanismes de protection ont été créés et des conventions ont été adoptées. Je considère que le rôle joué par des commissions telles que la vôtre est crucial. Mais la Cour européenne des droits de l'homme y contribue également par les développements de sa jurisprudence.* »

Dean Spielmann (Président de la Cour Européenne des Droits de l'Homme)

Conférence de Dean Spielmann à l'occasion des 10 ans de la CNPD

3.2 Validation de la charte BCR du groupe ArcelorMittal

Le groupe ArcelorMittal a adopté sa charte interne définissant les règles applicables au traitement des données personnelles par ses entreprises en cas de transferts en dehors de l'Union européenne y compris sur le territoire des pays qui n'ont pas de législation contraignante protégeant la vie privée. Ces règles (BCR - « Binding Corporate Rules »), rendues obligatoires pour toutes les entités juridiques de la multinationale et ses responsables et salariés dans tous les pays, ont pour but de garantir un niveau adéquat de protection aux employés, clients et fournisseurs d'ArcelorMittal.

ArcelorMittal est le numéro un mondial de l'exploitation sidérurgique et minière intégrée, avec une présence dans plus de 60 pays. L'entreprise multinationale est également leader sur tous les principaux marchés d'acier au carbone mondiaux, y compris l'automobile, la construction, l'électroménager et l'emballage, ainsi qu'un acteur de premier plan dans le domaine de la R&D et de la technologie.

Pendant un an et demi, la Commission nationale a mené des discussions avec ArcelorMittal conjointement avec les autorités de protection des données de 25 autres pays européens où le groupe est implanté. Ces dernières ont validé le résultat obtenu par la CNPD. Celle-ci devait en tant qu'autorité chef de file (« lead authority ») analyser le document d'une cinquantaine de pages de façon à ce qu'il soit conforme aux standards ambitieux de la législation européenne et aux souhaits des autres autorités nationales concernées.

Soucieuse de protéger les informations personnelles concernant ses employés, clients et fournisseurs, la multinationale a

Gérard Lommel à la conférence de l'AFCDP

décidé d'introduire volontairement cette charte « BCR ». Son respect sera obligatoire pour plus de 700 sociétés, succursales et filiales occupant quelque 260.000 employés dans une soixantaine de pays du monde. Elle vise en premier lieu à garantir que la protection dont bénéficient les individus dans les Etats membres de l'Union européenne continue à s'appliquer lorsque les informations sont transférées en dehors de cette « sphère de sécurité ».

Les BCR permettront en outre à ArcelorMittal de ne plus avoir à recourir à des autorisations ponctuelles pour chaque transmission intra-groupe de données personnelles. Cette simplification considérable des démarches administratives assure une certaine « flexibilité » dans l'accomplissement des tâches quotidiennes du groupe tout en garantissant un niveau élevé de protection des données.

En 2009, la Commission nationale avait déjà approuvé la charte BCR d'eBay/Paypal.

3.3 L'AFCDP s'adresse aux chargés de la protection des données

Le 12 mars 2013, les chargés de la protection des données se sont réunis à Luxembourg. Avec le soutien de la CNPD, l'AFCDP (Association Française des Correspondants à la protection des Données à caractère Personnel) a organisé une

conférence à l'auditoire de la BGL BNP Paribas.

Cette manifestation visait à encourager l'essor de la fonction de correspondant/délégué à la protection des données au sein même des entreprises et des organismes privés et publics et de fédérer les échanges d'expériences (bonnes pratiques sectorielles, etc.). La fonction du chargé de la protection des données (en France « correspondant informatique et libertés »; en Allemagne « Betrieblicher Datenschutzbeauftragter ») est appelée à prendre plus d'importance avec la réforme de la protection des données en cours au niveau européen, qui mise encore davantage sur la responsabilisation des acteurs.

La conférence était également l'occasion de réunir les membres luxembourgeois de l'association et les chargés de la protection des données dans le cadre de l'évolution de leur métier et de contribuer à une extension de leur présence dans les entreprises. Cet événement n'était pas seulement ouvert aux chargés de la protection des données, mais à tout professionnel concerné par le respect des lois de la protection des données (avocats, juristes d'entreprise, RSSI, risk managers, déontologues, etc). Par ailleurs, la volonté de créer une entité luxembourgeoise de l'AFCDP a été exprimée lors de la conférence.

Après un mot de bienvenue de Monsieur Carlo Thill, président du comité de direction de BGL BNP Paribas et de Monsieur Paul-Olivier Gibert, président de l'AFCDP, la conférence a été lancée par Madame Nathalie Sprauer (compliance and privacy officer auprès de la BGL BNP Paribas). Elle a apporté des solutions aux problèmes spécifiques rencontrés par les responsables du traitement ayant recours au « cloud computing ».

Ensuite, Monsieur Gérard Lommel, président de la CNPD, a présenté un bref historique de la fonction du chargé de la protection des données dans les pays « pionniers » dans le domaine, dont l'Allemagne, et a abordé les droits et devoirs spécifiques du chargé issus de la législation luxembourgeoise.

Maître Cyril Pierre-Beausse, avocat à la Cour, a montré l'importance d'une bonne interaction entre le RSSi (responsables de la sécurité et des systèmes de l'information) et le chargé, notamment parce que ces deux fonctions poursuivent le même but au sein d'une entreprise ou de tout autre organisme traitant des données personnelles. Lors d'une faille de sécurité, cette coopération devient indispensable afin de garantir une réactivité accrue du responsable du traitement (information des autorités et personnes concernées).

Maître Pascale Gelly, administratrice de l'AFCDP en charge de l'international, a fait le point sur l'état d'avancement des travaux sur le projet de règlement européen actuellement en discussion au Parlement européen et au Conseil. Maître Gelly a précisé que plusieurs versions des dispositions quant à l'obligation de désignation d'un chargé (selon le nombre de salariés auprès du responsable du traitement, selon le nombre de personnes concernées, selon la nature des données traitées) sont proposées en tant qu'amendements par les différentes commissions parlementaires.

Ces présentations ont été suivies par une table ronde, animée par Maître Pascale Gelly, avec les chargés Cédric Nédélec (PricewaterhouseCoopers), Richard Bertrand (Actecil) et Violaine Langlet (Vanksen) sur la vision du rôle futur des chargés dans les entreprises et organisations luxembourgeoises.

Enfin, la conférence a été clôturée par Monsieur Bruno Rasle, délégué général de l'AFCDP, qui a dessiné un bref historique et un portrait actuel de l'association organisatrice.

3.4 Analyse détaillée du contrat des services de Microsoft

Microsoft a mis à jour son contrat des services (MSA) en septembre 2012, en y incluant des modifications liées à la protection de la « vie privée ». Avant de pouvoir accéder à un service en ligne, comme, par exemple, « Outlook.com » ou « OneDrive », l'utilisateur doit accepter les conditions du MSA. Suite à cette mise à jour, le groupe de travail de l'article 29 a mandaté la CNPD, en collaboration avec la CNIL, pour effectuer une analyse des pratiques de Microsoft sur le sujet pour compte de toutes les autorités européennes de protection des données à caractère personnel.

Cette analyse a conduit à l'élaboration d'un questionnaire détaillé permettant l'obtention d'une transparence sur les pratiques de Microsoft au regard de ses traitements de données à caractère personnel, ses obligations et le respect des droits des utilisateurs en la matière. Les sujets traités concernaient aussi bien le contenu de l'information fourni aux utilisateurs, le contrôle par les utilisateurs quant à l'exercice de leurs droits, la gestion de la publicité comportementale, les combinaisons de données entre services offerts, les périodes de rétention des données et encore les potentielles analyses de contenu des utilisateurs effectué par Microsoft.

Suite à une collaboration fructueuse avec la société Microsoft, celle-ci va implémenter, au cours de l'année 2014, des changements au sein de ses systèmes, offrant aux utilisateurs un meilleur contrôle et plus de transparence par rapport aux traitements effectués avec leurs données.

3.5 Privacy Impact Assessment : accompagnement du GIE Luxmetering dans la mise en place des compteurs intelligents

Les termes « compteurs intelligents » ou « smart meters » désignent une nouvelle génération de compteurs d'énergie. Ceux-ci disposent de technologies avancées qui identifient de manière plus détaillée et en temps réel la consommation énergétique d'une habitation. L'objectif de l'Union européenne est d'atteindre une couverture de 80% des consommateurs d'ici

2020. Pour le Luxembourg, il est prévu que 95% des clients finals seront équipés de compteurs intelligents fin 2018 pour l'électricité et fin 2020 pour le gaz.

Le groupement d'intérêt économique Luxmetering est en charge de la mise en place de l'infrastructure et du déploiement national d'environ 350.000 compteurs intelligents. Le GIE a été créé le 28 novembre 2012 par les sept gestionnaires de réseau d'électricité et de gaz Creos Luxembourg, Ville d'Ettelbruck, Ville de Diekirch, Hoffmann Frères (Electris), Ville de Dudelange, Sudstroum et Sudgaz. Son activité se base sur la loi du 7 août 2012 modifiant la loi du 1er août 2007 relative à l'organisation des marchés d'électricité et de gaz.

La CNPD accompagne les activités de Luxmetering, qui a décidé d'évaluer l'impact des compteurs intelligents 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.

Dans un premier temps, la CNPD a déjà pris position par rapport à l'avant-projet de règlement grand-ducal relatif aux modalités du comptage de l'énergie électrique et du gaz naturel en décembre 2013 (voir partie 2.2.9.). Dans le contexte du PIA qui a commencé début 2014, la CNPD n'a non seulement un rôle fédérateur et de contrôle, mais contribue aussi au transfert d'informations en se basant sur les expériences internationales existantes.

Avantages du « smart metering »

Les compteurs intelligents peuvent communiquer de façon bidirectionnelle avec un système informatique central de collecte et de gestion des données situé chez les gestionnaires de réseaux. Ils informent les clients de la quantité d'énergie qu'ils consomment et ces informations peuvent aussi être transmises aux fournisseurs d'énergie et à d'autres parties désignées.

Le smart metering offre de nouvelles fonctionnalités, comme la production d'information détaillée sur la consommation d'énergie, la possibilité d'effectuer des relevés à distance, l'élaboration de nouveaux tarifs et services sur la base de profils énergétiques, la possibilité d'interrompre la fourniture à distance, l'établissement de factures en temps réel et le repérage des postes qui coûtent le plus cher au client.

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

Risques pour la protection de la vie privée

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

La problématique de la sécurité et confidentialité des données de consommation d'électricité et de gaz a également été abordée par le groupe « Article 29 » en 2011. Dans son avis 12/2011, le groupe de travail européen a préconisé que le responsable du traitement devait être clairement identifié et avoir connaissance

des obligations que lui impose la législation, notamment du point de vue de la prise en compte du respect de la vie privée dès la conception, de la sécurité et des droits des personnes concernées. Celles-ci devaient être correctement informées de la façon dont sont traitées leurs données et avoir conscience des différences fondamentales dans les modes de traitement pour être en mesure de donner valablement leur consentement.

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

Application du principe de « Privacy by Design »

Le Groupe de Berlin a par ailleurs noté que le « smart metering », qui se trouve encore à ses débuts, est particulièrement bien adapté à l'application des principes du « Privacy by Design ». Le respect de la vie privée dès la conception signifie : dès le début du développement des compteurs intelligents il faut prendre en compte les exigences en matière de protection des données et intégrer les outils de protection directement dans le produit, au lieu de les ajouter ultérieurement sous forme de compléments.

Idéalement, aucune action du consommateur ne devrait être nécessaire pour protéger sa vie privée (« Privacy by Default »). En outre, seules les données strictement nécessaires à la finalité de ces compteurs devraient sortir de la maison du consommateur par un « smart meter » (principe de minimisation des données). Enfin, le Groupe a insisté sur le fait que les consommateurs ne devraient pas être contraints de choisir entre la protection de leur sphère privée et l'efficacité énergétique.

3.6 Prospection électorale et protection des données

Dans le cadre des élections législatives anticipées du 20 octobre 2013, la CNPD a rappelé les dispositions de l'article 4 de la loi modifiée du 2 août 2002 érigeant la finalité d'un traitement de données en un principe essentiel dans le domaine de la protection des données.

Si les candidats et leurs partis politiques avaient bien évidemment un souci légitime d'approcher les électeurs et de leur exposer leurs programmes dans le cadre de leur campagne électorale, la CNPD leur a rappelé qu'ils ne doivent pas utiliser à cette fin des fichiers qu'ils se seraient procurés en dehors de toute base légale ou réglementaire auprès d'organismes ou institutions publics. L'article 6 de la loi précitée prévoit que les associations à but non lucratif ne doivent communiquer la liste de leurs membres à des tiers sans le consentement des personnes concernées.

En revanche, la loi électorale leur permet d'inspecter les listes électorales ainsi que d'en prendre copie. La Commission nationale considère que la prospection des électeurs inscrits par les divers partis politiques, notamment pour leur adresser les programmes politiques, rentre également dans le cadre de cette finalité électorale. Or, les données à caractère personnel des listes électorales doivent être utilisées loyalement et licitement et ne doivent pas être traitées ultérieurement de manière incompatible avec leur finalité électorale, elles ne doivent pas faire l'objet d'une quelconque utilisation – par exemple commerciale – incompatible avec la finalité électorale. L'utilisation des listes électorales à des fins de prospection pour la finalité électorale doit également être limitée à la période de l'élection pour laquelle elles ont été obtenues.

La CNPD a rappelé par ailleurs qu'une prospection politique par téléphone ou courrier électronique (ou tout autre moyen de communication électronique) ne peut se faire qu'en cas d'accord des personnes contactées.

Finalement, il y a lieu d'éviter un profilage excessif des citoyens qui serait disproportionné par rapport à la finalité électorale notamment par le rapprochement des listes électorales avec des données des électeurs provenant d'autres fichiers.

4 Perspectives

Au programme du nouveau gouvernement assermenté le 4 décembre 2013, on retrouve la question de la protection des données côte à côte avec la volonté de développer le potentiel économique lié au phénomène du « Big Data ».

Concilier la protection de la vie privée des citoyens et l'exploitation de leurs données sera un réel défi. Comment créer de la valeur à partir du traitement de ces grandes masses de données, tout en respectant les contraintes de confidentialité ?

La protection des données est aujourd'hui plus importante que jamais. Avec l'essor des technologies modernes, de plus en plus de renseignements individuels sont collectés, échangés et traités, souvent sans que les personnes concernées ne sachent par qui, pourquoi, pendant quel laps de temps et avec quels effets. La globalisation et les nouveaux outils de connexion (réseaux sociaux, smartphone, smart home, connected car, etc.) ont repoussé les limites traditionnelles qui modéraient ou cloisonnaient la disponibilité de données sur notre personnalité, notre entourage et nos habitudes de vie. Nous laissons des traces sur Internet, à travers nos communications, nos démarches administratives, nos achats et paiements, déplacements, etc. Des profils sont établis et gouvernent le type de publicité qui nous est adressé. L'exploitation de données à caractère personnel est en effet à la base du « business model » des géants d'Internet tels que Google, Amazon, Apple ou Facebook.

Toutes ces évolutions ont étendu le champ de données disponibles produites par l'individu lui-même ou par des ordinateurs. Le phénomène du « Big Data » se caractérise par l'immense volume des informations traitées et par la variété de leurs sources (données d'utilisation d'applications mobiles, clicks sur des sites web, données provenant de réseaux sociaux, données de localisation d'un appareil portable ou d'un véhicule, courriers électroniques, chats, données de communication d'appels téléphoniques, etc.). Au volume et à la variété s'ajoutent la vitesse d'analyse des données (« real-time data »), l'aptitude de faire des prévisions et de reconnaître des relations entre les données.

Le géant de l'Internet Amazon a récemment fait l'acquisition d'un brevet appelé « anticipatory shipping » (livraison anticipée). Le détaillant en ligne saura avant ses clients ce qu'ils comptent acheter : en compilant des

tonnes de données, Amazon sera en mesure de livrer dans ses entrepôts régionaux les biens qu'il estimera les plus prometteurs en termes de vente, accélérant du coup les délais de livraison. Déjà en 2009, Google avait lancé un outil de suivi de la grippe, qui repérait les recherches de termes liés à la maladie dans son moteur. En 2012, l'annonce de la Schufa, centrale de crédit, (abréviation de Schutzgemeinschaft für allgemeine Kreditversicherung) d'explorer l'utilisation des données des réseaux sociaux comme Facebook ou Twitter pour évaluer la solvabilité des citoyens allemands a soulevé une levée de boucliers en Allemagne.

L'émergence de l' « Internet des objets » va encore amplifier cette explosion des données, en ajoutant aux informations disponibles celles issues d'objets interconnectés tels que des cafetières, des thermostats, des montres, des pèse-personnes ou encore des maisons et voitures intelligentes. Au Luxembourg, dès le 1er juillet 2015, tout nouveau raccordement sera doté de compteurs intelligents. Fin 2018 (pour les compteurs électriques) et fin 2020 (pour le gaz naturel), 95 % du parc devront être remplacés.

L'arrivée de ces objets connectés pose de nouveaux défis en matière de protection des données des citoyens. Le « smart metering » ne semble constituer que le début de ces objets qui peuvent révéler les habitudes de vie des personnes. Google a notamment annoncé un projet de lentilles de contact intelligentes qui pourront mesurer, en temps réel, le taux de glucose des patients diabétiques à travers leurs larmes. L'entreprise américaine a également mis la main sur Nest, qui produit des alarmes anti-incendie et des thermostats intelligents connectés à Internet. Ces produits correspondent parfaitement aux efforts de Google en direction des « wearables », des objets connectés dont l'exemple le plus connu est Google Glass.

Tous ces exemples montrent que la vie connectée prend de plus en plus d'importance avec l'e-commerce, l'e-santé, l'e-gouvernement et l'e-banking. En même temps, le danger d'une utilisation abusive de la masse des données personnelles qui circulent et de la cybercriminalité augmente. Les annonces de failles de sécurité, fuites de données, attaques informatiques et violations de confidentialité dans la presse nationale et internationale se multiplient. En l'espace de quelques mois seulement, le BSI allemand (Bundesamt für Sicherheit in der Informationstechnik) a découvert le piratage de 16 millions d'adresses avec les mots de passe associés pour des services en ligne, la police danoise s'est fait voler 1,2 millions de données du système d'information Schengen, la chaîne de distribution américaine Target a annoncé que les données personnelles de 70 millions de clients et 40 millions de coordonnées de cartes bancaires et codes PIN avaient été dérobés. Ces failles de sécurité ne concernent pas seulement les services en ligne comme l'ont montré le cas de la SNCB en Belgique ou le « Medicoleak » au Luxembourg.

Rendre davantage de contrôle à l'individu sur l'usage qui est fait des informations le concernant, lui restituer les moyens de sa liberté de préserver un certain degré d'anonymat et l'intimité de sa vie privée sont des attentes partagées aujourd'hui par une grande partie de la population. Sans renier l'attrait et les bénéfices des avancées technologiques auxquelles la plupart d'entre nous ne voudraient plus renoncer, les risques d'atteinte illégitime à la confidentialité des données communiquées et la sécurité des systèmes en inquiètent plus

d'un. L'enjeu véritable est donc le rétablissement de la confiance dans les nouvelles technologies, les applications mobiles, l'usage de la biométrie, les achats et transactions financières sur Internet et de plus en plus d'autres services innovateurs en ligne et communications électroniques par les acteurs privés et publics. Pour libérer les utilisateurs de leurs appréhensions diffuses et permettre à l'économie et à la civilisation numériques de se déployer pleinement en accord avec la dignité et les droits individuels, il faut renforcer et rendre plus effective la protection des données en Europe.

Alors que les citoyens sont confrontés à la possibilité d'être tracés et profilés grâce à ces nouvelles technologies, mais aussi avec les révélations sur la collecte des données par la NSA américaine, la question se pose comment il sera possible d'adapter les principes de la protection des données du Conseil de l'Europe de 1981 et de l'Union européenne de 1995 à ce monde nouveau.

La Commission européenne a présenté deux propositions législatives le 25 janvier 2012, à savoir un règlement général sur la protection des données et une directive spécifique pour le domaine de la police et de la justice.

Les nouveaux textes devraient à la fois dépoussiérer les règles applicables – sans toucher aux principes essentiels – et remplacer les contraintes formalistes par une plus grande responsabilisation des acteurs, favoriser une démarche de « privacy by design » et la mise en œuvre de bonnes pratiques à l'initiative des entreprises et organisations elles-mêmes, tout en renforçant les moyens des autorités de protection des données et les possibilités de contrôle et de sanction à leur disposition.

En cas de traitement illicite ou d'abus constatés dans le cadre de l'utilisation de données personnelles, des amendes administratives importantes pourront être infligées.

Les services en ligne actifs en Europe, dont la société mère est établie dans un pays tiers, seront tenus de respecter les règles européennes. Il s'agit là d'un élément indispensable pour renforcer la confiance que les utilisateurs et consommateurs accordent à Internet, au cloud computing et à la confidentialité de leurs communications électroniques. Un renforcement de la confiance est essentiel pour le développement des services en ligne, de l'industrie numérique, pour l'utilisation des nouvelles technologies et la stimulation

de l'innovation dans l'Union européenne.

Le 21 octobre 2013, la Commission des libertés civiles, de la justice et des affaires intérieures (LIBE) du Parlement européen a franchi une étape décisive en adoptant sa position concernant la proposition de règlement général sur la protection des données, ainsi que la proposition de directive présentée en parallèle dans le domaine de la police et de la justice. Le Parlement est ainsi parvenu à un compromis sur quelque 4000 amendements déposés. Toutefois, les négociations s'avèrent plus longues que prévu. Le Conseil de l'UE n'a pas encore été en mesure de trouver un accord à la fin de l'année 2013.

En juin 2013, le scandale « PRISM » autour de la surveillance massive de l'Internet par les services secrets a ravivé les inquiétudes des citoyens sur la sécurité de leurs données à caractère personnel. La réforme proposée des règles de l'Union sur la protection des données pourrait contribuer à apaiser ces craintes et donnerait aux Européens une plus grande maîtrise de leurs données personnelles. Ceux-ci veulent des règles qui empêchent la violation de leurs droits par des entreprises ou des services de renseignement ou de police européens ou de pays tiers. Les outils nécessaires sont prévus par la proposition de la Commission européenne.

La modernisation de la protection des données au niveau européen fournit une occasion unique de conférer les mêmes droits aux 500 millions de citoyens de notre continent, pour leur assurer la transparence et la protection nécessaires dans l'ère numérique.

5 Ressources, structures et fonctionnement

5.1 Rapport de gestion relatif aux comptes de l'exercice 2013

Dépenses

Le total des frais de fonctionnement de l'établissement public au cours de l'exercice 2013 s'élève à 1.583.519,14 €. Ce chiffre représente une diminution de 0,96% par rapport à l'exercice précédent et reste en retrait des prévisions budgétaires.

Les charges relatives au personnel permanent sont nettement inférieures aux prévisions budgétaires (-98.989,19 €) alors que deux postes de collaborateurs sont restés inoccupés pendant une grande partie de l'année.

Les dépenses d'honoraires et frais d'experts et de prestataires externes de 12.324,47 € restent en dessous des 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.

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 37.352,99 €, ils ont légèrement dépassé les prévisions. Cependant ils 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 de la communication de 33.368,99 € restent conformes aux prévisions budgétaires. Sont toutefois venus s'ajouter des dépenses ponctuelles non récurrentes, à savoir celles liées à la célébration du 10e anniversaire de la Commission nationale dans le cadre d'une conférence/réception.

A défaut de disposer des ressources spécialisées nécessaires en interne pour la

maintenance des systèmes et réseaux informatiques, les frais correspondants d'un montant de 21.904,59 € n'ont pas pu être diminués en 2013.

Les amortissements comptabilisés en 2013 atteignent un montant total de 12.364,24 €. 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 99.846,10 €, il a dépassé nos prévisions de 44.846,10 €. En outre, des produits financiers (intérêts créditeurs) ont été enregistrés à hauteur de 2.056,03 €.

Résultat d'exploitation

Compte tenu de la dotation annuelle de 1.552.000 € dont la Commission nationale a bénéficié en 2013 de la part de l'Etat en application de l'article 37 paragraphe (4) de la loi, le résultat d'exploitation de l'établissement public s'établit à 70.382,99 € au 31 décembre 2013. Il sera reporté sur l'exercice suivant.

5 Ressources, structures et fonctionnement

5.2 Personnel et services

Collège
Gérard LOMMEL,
président
Thierry LALLEMANG,
membre effectif
Pierre WEIMERSKIRCH,
membre effectif

Membres suppléants
Josiane PAULY
Marc HEMMERLING
Tom WIRION

Service juridique
Georges WEILAND,
attaché de direction 1er en rang
Michel SINNER,
attaché de direction 1er en rang
Christian WELTER,
attaché de direction 1er en rang
Laurent MAGNUS,
juriste-expert (CDD)
Arnaud HABRAN,
juriste-expert (CDD)

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

Service informatique et de la logistique
Alain HERRMANN,
attaché de direction stagiaire
Consultant technologies et sécurité (prestataire externe)

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

Service communication et documentation
Tom KAYSER,
attaché de direction

5.2.1.1 Assermentation d'un ingénieur-informaticien

Le 3 juin 2013, M. le ministre des Finances Luc Frieden, en sa qualité de ministre des Communications et des Médias, a procédé à l'assermentation de M. Alain Herrmann en tant qu'ingénieur-informaticien nommé à la Commission nationale.

Alain Herrmann et Luc Frieden

5.3 Organigramme de la Commission nationale

Secrétariat
Tessy PATER, secrétaire de direction
Serge FERBER, employé de l'Etat

Collège
Gérard LOMMEL, Président
Thierry LALLEMANG, membre effectif
Pierre WEIMERSKIRCH, membre effectif

Administration générale, personnel, budget et finances

Communication et documentation
Tom KAYSER

Service juridique
Georges WEILAND, Michel SINNER
Christian WELTER, Laurent MAGNUS
Arnaud HABRAN

Service informatique et logistique
Alain HERRMANN,
informaticien (prestataire externe) / consultant technologies

Notifications
Transferts de données vers des pays tiers
Marc MOSTERT

Autorisations préalables
Stéphanie MATHIEU

Guidance et investigations
(compostion ad hoc
juriste + informaticien)

Registre public

6 La Commission nationale en chiffres

Formalités préalables

	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	
a) Notifications												TOTAL
Notifications ordinaires	2.646	850	500	250	760	385	345	295	355	437	421	7.244
Notifications simplifiées	750	900	720	890	537	-	-	-	-	-	-	3.797
Engagements de conformité	-	-	-	-	-	942	227	15	46	149	651	2.030
(Total a)	3.396	1.750	1.220	1.140	1.297	1.327	572	310	401	586	1.072	13.071
b) Autorisations préalables												TOTAL
Demandes d'autorisation	765	406	317	295	392	606	542	607	604	706	833	6.073
Engagements de conformité	718	14	17	19	151	220	70	92	49	70	149	1.569
(Total b)	1.483	420	334	314	543	826	612	699	653	776	982	7.642
(Total général a + b)	4.879	2.170	1.554	1.454	1.840	2.153	1.184	1.009	1.054	1.362	2.054	20.713
Déclarants (responsables ayant accompli des formalités)	2.220	2.500	2.850	3.300	3.754	4.357	4.772	5.110	5.399	5.821	6.559	

Demandes de renseignements

	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
a) Demandes de renseignements par écrit										
(Total a)	156	117	150	148	138	138	213	173	273	274
b) Demandes de renseignements par téléphone										
(Total b)	1.780	1.550	1.930	1.870	1.586	1.407	1.405	1.634	1.424	1.803
(Total général a + b)	1.936	1.667	2.080	2.018	1.724	1.545	1.618	1.807	1.697	2.077

Plaintes

	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Plaintes et demandes de vérification de licéité	15	38	40	30	34	63	133	145	115	133	177

Séances de délibération

	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
	39	36	39	40	40	37	38	35	27	31

Participations aux groupes de travail sur le plan européen

	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
	28	33	23	22	22	32	40	37	43	39

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

	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Secteur public	47	62	32	56	52	54	56	69	71	102
Secteur privé	30	38	12	40	44	52	54	71	61	75
(Total)	77	100	44	96	96	106	110	140	132	177

Séances d'information, conférences, exposés

	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
	4	10	11	14	11	23	21	15	10	18

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

	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Articles et interviews parus dans										
- les quotidiens	14	16	67	127	59	104	202	105	94	139
- les hebdomadaires	5	6	4	9	11	10	30	22	12	21
- les mensuels	0	7	5	4	2	1	5	4	1	3
- les médias audiovisuels	1	3	3	3	16	13	21	7	17	24
- Internet							49	36	51	52
(Total)	20	32	79	143	88	128	307	174	175	239

7 Annexes

Avis concernant le projet de règlement grand-ducal relatif au statut, aux modalités de désignation et aux attributions du médecin-coordinateur

Délibération n°28/2013
du 7 février 2013

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

Faisant suite à la demande lui adressée par Monsieur le Ministre de la Santé en date du 5 juillet 2012, la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet du projet de règlement grand-ducal « relatif au statut, aux modalités de désignation et aux attributions du médecin-coordinateur», et plus particulièrement sur son article 5 ayant trait aux données à caractère personnel.

Le projet de règlement grand-ducal sous examen entend préciser le statut, les modalités de désignation et les attributions du médecin-coordinateur, fonction créée par la loi du 17 décembre 2010 portant réforme du système de soins de santé et modifiant notamment l'article 29 de la loi du 28 août 1998 sur les établissements hospitaliers.

La Commission nationale limite ses observations aux questions de protection des données, soulevées plus particulièrement par l'article 5 du projet de règlement grand-ducal sous examen. Celui-ci dispose en effet notamment que *« pour les besoins de sa mission, le médecin-coordinateur a accès aux dossiers individuels visés à l'article 36 de la loi modifiée du 28 août 1998 des patients qui sont pris en charge par son service ou groupement de services ».*

1) Le secret médical

La disposition sous examen suscite la question de savoir si le médecin-coordinateur peut et doit effectivement avoir accès aux dossiers individuels de patients qui ne lui sont pas adressés et dont il n'est *a priori* pas en charge, ou si le principe du secret médical (auquel les médecins traitants sont tenus) s'y oppose.

Le secret médical peut être défini comme l'interdiction pour tout professionnel de la santé de divulguer les informations sur son patient dont il prend connaissance lors de l'exercice de sa profession, sous peine de sanctions prévues à l'article 458 du Code pénal.

Le secret médical est fondé, depuis son origine séculaire[1], sur la relation de confiance qui doit exister entre le médecin et son patient. Cette relation, qui induit nécessairement de la part du médecin une connaissance aussi large que possible de tous renseignements sur la santé physique et psychique de son patient, est établie par le choix du médecin traitant par le patient, et donc sur son consentement. La Cour européenne des droits de l'homme a déjà eu l'occasion de préciser que le secret médical *« est capital non seulement pour protéger la vie privée des malades, mais également pour préserver leur confiance dans le corps médical et les services de santé en général »*[2].

Il est communément accepté que cette relation, qui existait traditionnellement sous forme de binôme, englobe aujourd'hui l'équipe thérapeutique des autres praticiens concourant le cas échéant dans leurs spécialités respectives à l'action du praticien choisi par le médecin[3].

Cette situation de besoin croissant de la prise en charge pluridisciplinaire du patient à l'hôpital a amené le législateur français à insérer dans sa législation la notion de « secret partagé »[4], plus précisément à l'article L. 1110-4 du Code de la santé publique. Cette disposition permet le partage des données entre médecins et autres professionnels de la santé faisant partie d'une même équipe de soins avec le consentement implicite du patient.

Le projet de loi n°6469 relatif aux droits et obligations du patient et aux droits et obligations correspondants du prestataire de soins de santé[5], s'inspire largement de cet article[6] en entendant consacrer en droit luxembourgeois cette même notion de « secret partagé ».

L'article 20 paragraphe (3) dudit projet de loi prévoit en effet que *« deux ou plusieurs professionnels de la santé peuvent, sauf opposition du patient dûment averti, échanger des informations relatives à une même personne prise en charge, afin d'assurer la continuité des soins ou de déterminer la meilleure prise en charge possible. Lorsque la personne est prise en charge par une équipe de soins dans un établissement hospitalier ou toute autre personne morale ou entité au sein duquel des soins de santé sont légalement prestés, les informations la concernant sont réputées confiées par le malade à l'ensemble de l'équipe. Le patient, dûment informé, peut refuser à tout moment que soient communiquées des informations le concernant à un ou plusieurs professionnels de santé. Le professionnel de la santé qui est à l'origine de la prestation garde toutefois toujours un accès aux éléments du dossier en rapport avec sa prestation ».*

L'exposé des motifs du projet de loi relève que l'article 20 paragraphe (3) vise à *« faciliter, dans l'intérêt de la prise en charge, le flux de l'information au sein de l'équipe médicale ainsi qu'avec un autre intervenant dans la prise en charge lorsqu'il y a un lien thérapeutique ».*[7]

2) Les missions du médecin-coordinateur

L'article 29 de la loi du 28 août 1998 sur les établissements hospitaliers précise que les médecins-coordinateurs *« assurent des fonctions de coordination et de planification de l'activité médicale du ou des services(s) et veillent :*

- *au bon fonctionnement du ou des services et à la qualité des prestations ;*
- *à la standardisation de la prise en charge de patients ;*
- *à l'utilisation efficiente des ressources disponibles ».*

---

[1] Le principe du secret médical trouve son fondement dans le serment d'Hippocrate, probablement rédigé au IVème siècle av. J.-C., qui comporte notamment la phrase suivante : *« Quoique je voie ou entende dans la société pendant, ou même hors de l'exercice de ma profession, je tairai ce qui n'a jamais besoin d'être divulgué, regardant la discrétion comme un devoir en pareil cas »* (traduction attribuée à Emile Littré).

[2] Cour européenne des droits de l'homme, Z. contre Finlande, arrêt du 25 février 1997, Rec. 1997-I.

[3] Cette position a été pour la première fois en France consacrée par le Conseil d'Etat dans son arrêt n°76799 du 11 février 1972.

[4] C. Zorn-Macrez, Données de santé et secret partagé : pour un droit de la personne à la protection de ses données de santé partagées, Nancy, Presse Universitaires de Nancy, 2010, p. 125.

[5] Projet de loi n°6469 relatif aux droits et obligations du patient et aux droits et obligations correspondants du prestataire de soins de santé, portant création d'un service national d'information et de médiation dans le domaine de la santé et modifiant la loi modifiée du 28 août 1998 sur les établissements hospitaliers et la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

[6] Exposé des motifs du projet de loi n°6469 relatif aux droit et obligations du patient et aux droits et obligations correspondants du prestataire de soins de santé, article 20, p. 44.

[7] *Idem.*

Les missions du médecin-coordinateur sont davantage précisées par le projet de règlement grand-ducal sous examen. Celui-ci investit le médecin-coordinateur d'une mission de coordination au sein des hôpitaux ou établissements hospitaliers spécialisés. Il contribue ainsi, *« ensemble avec les médecins de son ou de ses services »*, à *« garantir le bon fonctionnement de l'activité médicale au sein de son service ou groupement de services en promouvant la qualité et l'amélioration continue des prestations de soins ainsi que le respect de la réglementation applicable en milieu hospitalier ».*[8]

La fonction de médecin-coordinateur en milieu hospitalier n'existe pas en tant que telle en Belgique ou en France. Cependant, les missions du médecin-coordinateur présentent certaines similarités avec celles attribuées au médecin-chef en Belgique, au médecin responsable de l'information médicale et au médecin coordonnateur des établissements hébergeant des personnes âgées dépendantes (« EHPAD ») en France, même si on ne saurait assimiler les régimes belge et français à celui du médecin-coordinateur.

Bien que le médecin-coordinateur ne soit pas un chef du personnel médical de son service[9], contrairement au médecin-chef en Belgique, il se voit attribuer un rôle similaire à ce dernier, respectivement la coordination du département médical et une responsabilité organisationnelle dans la continuité et la qualité des soins au sein de son service.[10] Le Conseil national de l'Ordre des médecins en Belgique a estimé que *« l'exécution des dispositions* [applicables au médecin-chef], *et plus largement le fonctionnement harmonieux de l'institution hospitalière, justifient que le médecin-chef ait accès au dossier médical du patient dans les limites de l'exécution de ses missions »*[11].

En France, le médecin responsable de l'information médicale a notamment pour mission d' *« organiser, traiter et analyser l'information médicale dans le cadre du programme de médicalisation des systèmes d'information (« PMSI ») en garantissant la confidentialité des informations médicales »*[12]. Le médecin coordonnateur des EHPAD, quant à lui, *« contribue, auprès des professionnels de santé exerçant dans l'établissement, à la bonne adaptation aux impératifs gériatriques des prescriptions de médicaments »*[13] et *« assure l'encadrement médical de l'équipe soignante »*[14].

---

[8] Exposé des motifs du projet de règlement grand-ducal relatif au statut, aux modalités de désignation et aux attributions du médecin-coordinateur, p. 1.
[9] *Idem*.
[10] Arrêté royal du 15 décembre 1987 portant exécution des articles 13 à 17 inclus de la loi sur les hôpitaux, coordonnée par l'arrêté royal du 7 août 1987, *M.B.*, 25 déc. 1987, art. 2 et s.
[11] Avis du Conseil de l'Ordre des médecins concernant la consultation du dossier-médical par le médecin-chef de l'hôpital.
[12] *Cf.* répertoire des métiers de la fonction publique hospitalière, « fiche métier » éditée par le Ministère de la santé et des sports – Direction générale de l'offre de soins, disponible à l'adresse suivante : http://www.metiers-fonctionpubliquehospitaliere.sante.gouv.fr/pdf/metier.php?idmet=125.
[13] Article L. 313-12, paragraphe (V) du Code de l'action sociale et des familles.
[14] Article D. 312-158 du Code de l'action sociale et des familles.

Au Luxembourg, le Collège médical estime, dans son avis du 25 juillet 2012, que « *dans une organisation hospitalière dépourvue d'hiérarchie verticale, le fonctionnement optimal d'un service ne peut se réaliser que par le biais d'un médecin-coordinateur* ».

La Commission nationale estime également, en tenant compte tant de l'organisation hospitalière propre au Grand-duché de Luxembourg que de la situation dans nos pays voisins, que l'introduction du rôle de médecin coordinateur dans notre législation est de nature à contribuer à améliorer la qualité de notre système de soins.

En particulier, la Commission nationale ne met pas en doute que, pour l'exercice et dans les limites de ses missions légales et réglementaires, le médecin-coordinateur devrait avoir accès aux dossiers individuels des patients pris en charge par son service ou groupement de services. Elle est cependant d'avis que cet accès devra être encadré par certaines garanties précisées ci-après.

3) L'absence de lien thérapeutique entre le médecin-coordinateur et le patient

La Commission nationale souhaite attirer l'attention sur le fait que les missions du médecin-coordinateur, aussi légitimes et précieuses qu'elles soient, ne s'inscrivent pas dans un lien thérapeutique, mais bien dans une démarche d'amélioration de la qualité des soins, telle qu'expliquée plus en détail ci-dessus[15].

En effet, les attributions du médecin-coordinateur mentionnées à l'article 29 de la loi modifiée du 28 août 1998 sur les établissements hospitaliers et précisées par le projet de règlement grand-ducal sous objet laissent apparaître qu'il n'existe pas *a priori* de lien thérapeutique entre le médecin-coordinateur et les patients pris en charge par son service ou groupement de services.

Par ailleurs, l'article 6 du projet de règlement grand-ducal sous examen précise qu' « *hormis les cas d'urgence, son statut de médecin-coordinateur ne l'autorise cependant pas à intervenir ou à prendre une décision relative au traitement médical d'un patient pris en charge par un médecin de ce service ou groupement de services* ».

L'article 20 paragraphe (3) du projet de loi n°6469, que nous avons déjà évoqué[16], permettrait le partage des données entre médecins et autres professionnels de la santé faisant partie d'une même équipe de soins « *lorsqu'il existe un lien thérapeutique* », ce qui n'est toutefois pas le cas en l'espèce.

La Commission Nationale est dès lors d'avis que l'article 20 paragraphe (3) du projet de loi n°6469 relatif aux droits et obligations du patient, si le texte était adopté en l'état, n'aurait pas vocation à s'appliquer dans le cas sous examen. Il s'ensuit que le principe du secret médical devra donc pleinement être respecté.

4) L'accès du médecin-coordinateur aux données avec le consentement des patients

La Commission nationale estime, comme G. Vogel et E. Rudloff[17], que « *l'obligation au secret médical découle avant tout de l'intérêt éminemment respectable de celui qui a placé, sous l'empire d'une absolue nécessité, sa confiance dans la discrétion d'une personne appelée par profession à recevoir les confidences d'autrui* ». Etant donné ce caractère prédominant de l'intérêt privé attaché à la répression de la violation du secret médical, la Commission nationale considère que le consentement du patient, à la base du secret médical, permet de délier le médecin de son obligation de ne pas divulguer à un tiers certaines informations dont il prend connaissance à l'exercice de sa profession.

---

[15] *Cf. supra*, pp. 3-4.
[16] *Cf. supra*, p. 3.
[17] G. VOGEL et E. RUDLOFF, *Lexique de droit médical et hospitalier*, Luxembourg, Editions Promoculture, 2009, pp. 214-215, n°363.

Par le projet de règlement grand-ducal sous examen, le gouvernement se propose de réglementer spécifiquement l'accès du médecin-coordinateur aux dossiers individuels des patients qui sont pris en charge par son service ou groupement de services, ce qui revient à une communication de données à un tiers, alors qu'il n'existe pas de lien thérapeutique entre le médecin-coordinateur et les patients dont les données lui seraient communiquées.

L'article 7 paragraphe (4) de la loi du 2 août 2002 précise que « *sous réserve que leur traitement soit en lui-même licite au regard des articles 6 et 7, les données y visées peuvent être communiquées à des tiers ou utilisées à des fins de recherche, d'après les modalités et suivant les conditions à déterminer par règlement grand-ducal* ».

Le cas de figure sous objet doit être analysé comme un traitement de données relatives à la santé nécessaire aux fins de l'administration de soins ou de traitements, et est donc licite au sens de l'article 7 paragraphe (1) de la loi du 2 août 2002. Dès lors, les données des patients peuvent être communiquées à des tiers d'après les modalités et suivant les conditions déterminées par règlement grand-ducal.

Dans le cas spécifique sous examen, la Commission nationale considère que l'accès du médecin-coordinateur aux données des patients individuels ne devrait être possible qu'avec le consentement du patient.

Ce consentement devrait par ailleurs être distinct des autres consentements nécessaires à la prise en charge du patient dans le cadre du traitement médical au sein de l'hôpital ou de l'établissement hospitalier spécialisé. Cela paraît en effet nécessaire afin que le patient puisse manifester de façon suffisamment spécifique sa volonté d'accepter ou de refuser que ses données à caractère personnel ne soient divulguées au médecin-coordinateur.

En dehors des cas d'urgence, le consentement devrait en outre être préalable à la prise en charge du patient au sein de l'hôpital ou de l'établissement hospitalier spécialisé, afin que cette manifestation de volonté du patient soit suffisamment informée. Lorsque le patient est admis aux services d'urgences, le consentement du patient devrait être recueilli *a posteriori*.

5) Le contrôle de l'accès aux dossiers individuels des patients

Suivant le projet de règlement grand-ducal sous examen, le médecin-coordinateur dispose

certes d'un « *droit de regard sur les activités médicales du service ou groupement de services dont il coordonne l'activité* »[18] et ne doit être exercé, selon les termes du projet, que « *pour les besoins de sa mission* »[19].

Nous estimons que, de par les missions telles que définies, le rôle du médecin-coordinateur ne doit pas être compris comme celui d'un « *chef du personnel médical* »[20], comme on l'a déjà évoqué[21], impliquant une mission de contrôle ou de surveillance sur les médecins traitants.

Dans la plupart des cas, le suivi des bonnes pratiques élaborées au sein d'un service devrait pouvoir se faire sur base de chiffres agrégés ou de statistiques, ce qui n'exclut pas que dans certains cas le médecin-coordinateur puisse consulter certains dossiers individuels.

Dès lors, une certaine transparence à l'égard des médecins traitants s'impose. C'est pourquoi la Commission nationale suggère de prévoir la mise en place d'une journalisation des accès.

Ainsi, à des intervalles réguliers, les médecins traitants devraient se voir communiquer la liste des dossiers de leurs patients auxquels le médecin-coordinateur a accédé.

Ainsi décidé à Esch-sur-Alzette en date du 7 février 2013.

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°6394 portant approbation : de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg, le Gouvernement du Royaume de Belgique, le Gouvernement de la République fédérale d'Allemagne et le Gouvernement de la République française, concernant la mise en place et l'exploitation d'un centre commun de coopération policière et douanière dans la zone frontalière commune, signé à Luxembourg, le 24 octobre 2008; de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République française relatif à la coopération dans leurs zones frontalières entre les autorités de police et les autorités douanières, signé à Luxembourg, le 15 octobre 2001

Délibération n°178/2013
du 19 avril 2013

Conformément à l'article 32 paragraphe (3) lettre (e) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après désignée « la loi modifiée du 2 août 2002 »), la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale ») a notamment pour

[18] Article 6 du projet de règlement grand-ducal sous examen.
[19] Article 5 alinéa 2 du projet de règlement grand-ducal sous examen.
[20] Exposé des motifs du projet de règlement grand-ducal sous examen, p. 1.
[21] *Cf. supra*, p. 3.

mission d'*« être demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi »*.

Par courrier du 16 mai 2012, Monsieur le Ministre de l'Intérieur et à la Grande Région a invité la Commission nationale à se prononcer au sujet du projet de loi n°6394 portant approbation : de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg, le Gouvernement du Royaume de Belgique, le Gouvernement de la République fédérale d'Allemagne et le Gouvernement de la République française, concernant la mise en place et l'exploitation d'un centre commun de coopération policière et douanière dans la zone frontalière commune, signé à Luxembourg, le 24 octobre 2008 (ci-après l'accord de 2008); de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République française relatif à la coopération dans leurs zones frontalières entre les autorités de police et les autorités douanières, signé à Luxembourg, le 15 octobre 2001 (ci-après l'accord de 2001);

Les deux accords prévoient la mise en place et l'exploitation d'un centre commun de coopération policière et douanière ainsi que des échanges de renseignement entre les autorités policières et douanières des pays participants, renseignements qui peuvent comporter des données à caractère personnel.

L'article 4 de l'accord de 2008 précise qu'il *« est créé au sein du centre commun un fichier de données à caractère personnel dont la finalité est la collecte et la présentation de requêtes dans le cadre des missions visées à l'article 3. »*

L'article 5 de l'accord de 2001 dispose que *« les agents des services compétents recueillent, analysent et échangent au sein du centre commun toutes informations et données utiles à la coopération en matière policière et douanière. »*

Si les deux accords prévoient le traitement de données à caractère personnelles, force est de constater que les accords ne contiennent aucune précision quant aux catégories de données faisant l'objet du traitement. La Commission nationale estime qu'il aurait été préférable qu'une énumération des catégories de données concernées aurait été précisée dans l'accord.

La Commission nationale salue que l'accord de 2008 contienne, en son article 4, des dispositions

relatives à la protection des données et, à l'article 5, des dispositions relatives à la sécurité des données et que le projet de loi entend conférer un cadre légal à ces deux accords.

Elle regrette toutefois qu'elle n'a pas été consultée lors de la phase de négociation respectivement avant la signature de l'accord de 2008, alors que le projet de loi sous examen n'a pour but que d'approuver les deux accords signés qui ne peuvent plus être modifiés à moins de les renégocier avec les Etats concernés.

Enfin la Commission nationale est à se demander comment les deux accords, soumis à l'approbation parlementaire, doivent s'articuler avec d'autres textes législatifs européens en la matière dans la mesure où les échanges d'information entre les différentes autorités des pays en question devront respecter la Décision 2008/615/JAI du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière, la Décision 2008/616/JAI du 23 juin 2008 concernant la mise en œuvre 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 et la Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

Ainsi décidé à Luxembourg en date du 19 avril 2013.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

Avis au sujet des projets de loi relatifs à la réforme dans la Fonction Publique en particulier des dispositions ayant trait à la protection des données comprises dans le projet de loi n°6457

Délibération n°265/2013 du 14 juin 2013

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

Faisant suite à la demande lui adressée par Monsieur le Ministre de la Fonction Publique et de la Réforme administrative François BILTGEN en date du 29 mars 2013, lui demandant d'aviser les projets de loi relatifs aux réformes dans la Fonction publique, mais en particulier les dispositions ayant trait à la protection des données visées à l'article 41 du projet de loi n°6457, la Commission nationale expose ci-après ses

réflexions et commentaires au sujet de ces projets de loi.

Les modifications apportées à la législation relative à la Fonction Publique par les projets de loi sous examen ne soulevant pas d'autres questions de protection des personnes à l'égard du traitement des données à caractère personnel, la Commission nationale a décidé de limiter ses observations aux dispositions de l'article 41 du projet de loi n°6457. Cet article a pour objet d'insérer un article 35 bis dans la loi modifiée du 16 avril 1979 fixant le statut général des fonctionnaires de l'Etat qui régira le traitement des données du personnel (fonctionnaires et employés) des administrations et services de l'Etat, des postulants ayant introduit leur candidature pour un tel emploi ainsi que des bénéficiaires de pension de la part de l'Etat.

La Commission nationale salue l'introduction dans cette loi cadre d'une disposition ayant pour vocation d'encadrer les traitements dont les données des fonctionnaires et employés des services de l'Etat font l'objet tout comme ceux des pensionnés ou candidats à un emploi public.

Une telle disposition constitue un progrès dans la prise en compte des exigences des principes de légalité (art. 8 § 2 de la Convention européenne des droits de l'Homme du 4 novembre 1950), du principe de finalité (art. 6 § 1 lettre (b) de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995) et des droits individuels reconnus aux personnes physiques par ladite directive européenne.

La Commission nationale retient que l'article sous examen désigne le Ministre ayant la Fonction Publique et la Réforme administrative dans ses attributions comme responsable du traitement des données du personnel conjointement avec les autres départements ministériels, administrations et services de l'Etat concernés.

Il ressort clairement du premier paragraphe que ces derniers n'ont une légitimation de recevoir, consulter et utiliser que les données relatives aux agents publics y nommés ou affectés et concernant les candidats à un poste dépendant de ces entités et organismes étatiques et publics.

L'avant-dernier paragraphe précise encore que seules les personnes habilitées à accéder aux données en raison des besoins découlant de leur fonction pourront les consulter.

Il apparaît dès lors indispensable que les finalités susceptibles

de justifier un tel accès soient déterminées. Le texte proposé le fait en termes généraux en faisant référence aux processus centraux et locaux de gestion du personnel (des ressources humaines dirait-on en langage moderniste) et énumère de façon explicite 9 champs d'activités essentiels.

Le terme « notamment » précédant cette énumération ne paraît acceptable que dans la mesure où il n'ouvre pas la voie à un spectre illimité d'objets pour lesquels les données pourraient être traitées. Tel semble être la volonté des auteurs du texte proposé qui fait allusion aux seuls processus légitimes et nécessaires de la gestion des candidatures du personnel en service et des retraités et bénéficiaires d'une pension de l'Etat.

Si la description du « cycle de vie » des données collectées et traitées ne doit pas forcément être détaillée exhaustivement dans un seul et même article de loi, l'exigence de spécification des finalités (c.àd. des objectifs poursuivis par le traitement des données) qui est entérinée dans l'art. 8 de la Charte des droits fondamentaux de l'Union européenne, ne souffre pas d'exception en tant que telle.

Si des finalités additionnelles ou plus détaillées résultant d'autres textes légaux comme ceux cités au 2ème paragraphe du commentaire de l'article figurant au document parlementaire 6457/00 peuvent intervenir dans l'un ou l'autre des nombreux processus de la gestion des ressources humaines de l'Etat, elles doivent être transparentes et les personnes concernées en être informées pour satisfaire au principe de légalité et prévisibilité de toutes intrusions dans la vie privée des individus, y compris celles découlant des activités de l'Etat.

La finalité poursuivie constitue en effet la mesure pour l'appréciation de la nécessité et proportionnalité du recours aux différentes données, de la durée de leur conservation, de la légitimité de leur utilisation, voir transmission par/à différents intervenants respectivement de la nécessité de recueillir le consentement pour d'éventuels utilisations ultérieures ne pouvant pas être considérées comme compatibles avec les finalités initiales.

La Commission nationale marque donc son accord avec le libellé proposé sous la réserve expresse que l'utilisation du terme « notamment » ne pense pas être comprise comme permettant d'ajouter aux finalités énumérées d'autres finalités que celles se rattachant aux processus de gestion des ressources humaines visés par un texte légal ou réglementaire.

Pour ce qui est des données recueillies et traitées, elle ne s'oppose pas formellement à ce que l'article proposé ne comporte pas d'énumération détaillée dès lors qu'il est spécifié que ne seront enregistrées que les données nécessaires et non excessives par rapport aux finalités poursuivies et que les personnes concernées seront au courant de leur nature, soit parce qu'elles les auront elles-mêmes directement fournies, ou qu'elles en seront informées pour ce qui est des données résultant de leurs activités, du déroulement de leur carrière et de leurs droits et obligations statutaires.

Sa préférence en la matière irait toutefois clairement en faveur d'une énumération directement dans l'article de loi spécifiant au moins des grandes catégories de données visées décrites dans leur généralité.

Le texte proposé précise par ailleurs que « les personnes concernées seront informées de la finalité du traitement, du caractère obligatoire ou facultatif du recueil, des destinataires et des modalités d'exercice des droits qui leur sont ouverts au titre de la protection des données à caractère personnel (d'accès, rectification, voir d'effacement, d'opposition).

Les dispositions des paragraphes 3 et 4 visent les mesures techniques et organisationnelles en vue de la sécurisation et de la confidentialité des données figurant dans les fichiers du Ministère et des administrations et services associés.

La Commission nationale note avec satisfaction que l'accès aux données sera strictement limité aux personnes habilitées à cet effet et contrôlé.

Le règlement d'exécution à prendre devra spécifier que ces accès feront l'objet d'un système de journalisation (logging) de nature à faciliter le contrôle et la détection d'éventuels abus. Il est souhaitable de voir adopter également en pratique une procédure de contrôle ponctuel à laquelle il devra être recouru de façon systématique et rigoureuse de façon à exclure dans toute la mesure du possible les abus et de contribuer à renforcer la confiance que les agents publics sont en droit de placer dans les fichiers sensibles concernant le personnel de l'Etat et d'éviter aux responsables des suspicions injustifiées telles que celles dont il avait été fait état il y a quelque temps au sujet des pratiques de certains syndicats dont le public s'était étonné qu'il dispose toujours des coordonnées des agents embauchés ou en fonction dans les administrations et services de l'Etat.

Finalement peut-on faire remarquer que le texte proposé n'indique pas de durée de conservation des données recueillies et traitées. Il conviendrait pour le moins de spécifier quelles informations doivent être retenues en cas de cessation de l'occupation de l'agent dans les administrations et services de l'Etat et pendant combien de temps suivant son départ. Certes la conservation d'un nombre non négligeable de données personnelles se justifie-t-elle dans bien des cas pendant toute la durée de sa carrière et jusqu'à ce que tous droits et prétentions à pension de l'agent ou de ses ayants droits soient éteints ou ne seront plus susceptibles d'être invoqués.

On peut s'interroger cependant sur le point de savoir si pour certaines catégories d'informations le Ministère et les administrations associées ne pourraient pas se contenter d'un cycle de vie plus réduit des données à caractère personnel enregistrées dans les fichiers des ressources humaines de l'Etat.

Pour le surplus, la Commission nationale n'a pas d'autres observations à l'encontre du projet de loi visé.

Ainsi décidé à Esch-sur-Alzette en date du 14 juin 2013.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

Avis relatif à l'avant-projet de règlement grand-ducal pris en exécution de l'article 4 de la loi modifiée du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat et à l'avant-projet de règlement grand-ducal pris en exécution de l'article 23 de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité

Délibération n°274/2013
du 28 juin 2013

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

Par courrier du 16 mai 2013, Monsieur le Premier Ministre a invité la Commission nationale à se prononcer au sujet de l'avant-projet de règlement grand-ducal pris en exécution de l'article 4 de la loi modifiée du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat et portant création et fixant les modalités de fonctionnement d'un fichier relatif au traitement de données à caractère personnel par le Service de Renseignement de l'Etat ainsi qu'au sujet de l'avant-projet de règlement grand-ducal pris en exécution de l'article 23 de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité et portant création et fixant les modalités de fonctionnement d'un fichier relatif au traitement de données à caractère personnel par le Service de Renseignement de l'Etat.

La Commission nationale passe en revue les articles qui donnent lieu à observations.

1. L'avant-projet de règlement grand-ducal pris en exécution de l'article 4 de la loi modifiée du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat

Ad article 2

Il se dégage de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (convention 108) et la Directive 95/46/CE du Parlement européen

et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données que le traitement des données personnelles d'un individu doit être strictement limité à une ou plusieurs finalités explicitement déterminées au préalable. De même, la collecte, l'enregistrement et l'utilisation des données personnelles doivent être strictement limités à ce qui est nécessaire pour atteindre des buts expressément fixés d'avance.

Les traitements relatifs à la sûreté de l'Etat doivent faire l'objet d'une autorisation par voie règlementaire en vertu de l'article 17 paragraphe (1) lettre (b) de la loi modifiée du 2 août 2002.

Il incombe dès lors au règlement de fixer les finalités du traitement en question.

En l'espèce les finalités du traitement résultent de l'article 2 paragraphe 2. de l'avant-projet de règlement combiné à l'article 2 de la loi modifiée du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat qui décrit les missions du SRE.

La Commission nationale estime que les deux articles mentionnés ci-dessus satisfont à l'obligation de déterminer de manière précise les finalités du traitement.

Ad article 5

La Commission nationale note que les catégories de données énumérées sont décrites de manière assez vague. Certes, les nécessités d'un service de renseignement requièrent une certaine flexibilité en ce qui concerne les données à collecter de sorte qu'il serait difficile et peu judicieux de prévoir les données précises dans une liste exhaustive de décrire de manière exacte des types de données traitées. Le commentaire des articles donne néanmoins davantage de détails.

Ainsi, sans la lecture du commentaire des articles, il n'est pas aisé de faire la différence par exemple entre les données d'identification personnelles (paragraphe 1. point 1.) et les caractéristiques personnelles (paragraphe 1. point 7.)

Le commentaire des articles indique que les données d'identification personnelles englobent notamment le nom, le prénom et les adresses privée et professionnelle alors que les caractéristiques personnelles englobent notamment le sexe ainsi que le date et le lieu de naissance.

Or, la distinction entre les données du point 1. et celles du

point 7. a son intérêt puisque pour ce qui est des dirigeants des personnes morales concernées par le fichier e-RSN, les données du point 1. font l'objet d'un traitement alors que les données du point 7. ne le font pas.

En ce qui concerne les données d'identification émises par les administrations publiques (paragraphe 1. point 2.), la Commission nationale présume qu'il s'agit des données obtenues conformément aux articles 3 et 4 de la loi modifiée du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat. Si tel n'était pas le cas, il conviendrait de conférer à cette utilisation de données émises par les administrations une base juridique plus précise.

L'expression « *données d'identification électroniques* » (paragraphe 1. point 3.) n'est pas très parlante.

Il ressort du commentaire des articles que ce point englobe apparemment les données relatives au trafic de télécommunications obtenues vraisemblablement auprès des fournisseurs de services de télécommunications, comme par exemple les données de traçage d'appels téléphoniques. Du moins, l'utilisation de l'expression « moments de connexion », non plus amplement détaillée, laisse entendre cela.

La Commission nationale rappelle qu'en vertu des articles 4 paragraphe (3) lettre (b) et 5 paragraphe (2) premier tiret de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, il ne peut être accédé à ces données que selon la même procédure que celle applicable aux écoutes téléphoniques, à savoir celle régie par les articles 88-3 et 88-4 du Code d'instruction criminelle[22].

Elle propose dès lors de mentionner de manière expresse les « *données relatives au trafic en matière de télécommunications obtenues conformément aux articles 4 paragraphe (3) lettre (b) et 5 paragraphe (2) premier tiret de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et 88-3 et 88-4 du Code d'instruction criminelle* ».

Dans ce contexte, il y a par ailleurs lieu de soulever une incohérence :

En matière de données de trafic de télécommunications, l'article 5 paragraphe (2) premier tiret de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques dispose ce qui suit :

« *Tout fournisseur de services ou tout opérateur qui traite des données relatives au trafic concernant les abonnés et les utilisateurs, est tenu de prendre toutes les dispositions nécessaires pour que de telles données soient conservées pendant la période prévue sub (1) (a) de manière telle qu'il est impossible à quiconque d'accéder à ces données dès lors qu'elles ne sont plus nécessaires à la transmission d'une communication ou aux traitements prévus par les dispositions sub (3) et (4), à l'exception des accès qui sont:*
– ordonnés par les autorités judiciaires agissant au titre de l'article 67-1 du Code d'instruction criminelle et celles compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique et pour la prévention, la recherche, la constatation et la poursuite des infractions pénales visées au paragraphe (1) (a) (…) ».

Cet article comporte donc des renvois aux articles suivants[23] :

- l'article 67-1 du Code d'instruction criminelle qui prévoit le repérage des données de télécommunications (donc l'accès aux données de trafic) ordonné par un juge d'instruction
- les articles 88-1 et 88-2 du Code d'instruction criminelle

[22] hormis – bien entendu- l'hypothèse de l'accès ordonnée par un juge d'instruction.
[23] L'article 9 paragraphe (2) de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques comporte les mêmes renvois.

qui prévoient la surveillance et le contrôle des communications par un juge d'instruction, de fait le contrôle du contenu des communications comme par exemple les écoutes téléphoniques
- les articles 88-3 et 88-4 du Code d'instruction criminelle qui prévoient la surveillance et le contrôle des communications effectués par le SRE

Force est de constater que les articles 88-3 et 88-4 calqués sur les articles 88-1 et 88-2 (qui, eux, s'appliquent au contrôle du contenu des communications) sont censés couvrir à la fois le contrôle du contenu des communications et, en vertu de l'article 5 précité, le contrôle des données de trafic par le SRE, l'article 67-1 n'ayant pas de pendant pour les contrôles effectuées par le SRE.

En ce qui concerne les « données de localisation électroniques » (paragraphe 1. point 4.), la Commission nationale présume qu'il s'agit également pour l'essentiel de données obtenues auprès des fournisseurs de services de télécommunications.

Là encore, il résulte des articles 4 paragraphe (3) lettre (b) et 9 paragraphe (2) de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques qu'il ne peut être accédé à ces données que selon la même procédure que celle applicable aux écoutes téléphoniques, à savoir celle régie par les articles 88-3 et 88-4 du Code d'instruction criminelle[24].

La Commission nationale propose dès lors de mentionner de manière expresse les *« données de localisation obtenues conformément aux articles 4 paragraphe (3) lettre (b) et 9 paragraphe (2) de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et 88-3 et 88-4 du Code d'instruction criminelle ».*

Si d'autres données de localisation sont également visées- et la mention du terme *« GPS »* dans le commentaire des articles le laisse supposer- il conviendrait de le mentionner dans le règlement.

La Commission nationale se demande cependant quelle pourrait être l'origine de ces autres données de localisation. Proviendraient-elles par exemple de traceurs espions installés à l'insu des personnes surveillées ?

Dans ce contexte, il est renvoyé aux développements exposés ci-dessous à propos du paragraphe 3 concernant les *« informations que les techniques d'enregistrement utilisées par le*

[24] ici également hormis l'hypothèse de l'accès ordonnée par un juge d'instruction.

Service de Renseignement de l'Etat ont pu relever ».

En ce qui concerne les « *données financières* » (paragraphe 1. point 6.), la CNPD se demande à nouveau quel pourrait bien être l'origine des données. Le secret bancaire et fiscal ne peut-il pas être opposé au SRE ?

En ce qui concerne les « *données physiques* » (paragraphe 1. point 8.), il n'est pas clair ce qui distingue celles-ci des caractéristiques personnelles (paragraphe 1. point 6.)

Le paragraphe 1. point 10. prévoit la catégorie de données « *composition du ménage* » et le commentaire des articles évoque dans ce contexte « *les éventuels détails sur les autres membres de la famille ou du ménage* ». Que signifie les « *éventuels détails* » ? S'agit-il de l'ensemble des catégories de données listées dans le paragraphe 1 de l'article 5 ? La Commission nationale estime qu'il faudrait préciser les catégories de données pouvant faire l'objet d'un traitement en ce qui concerne les personnes cohabitant avec les personnes concernées par un traitement de données en vertu de l'article 2 paragraphe 1. de l'avant-projet de règlement.

De manière générale, selon l'exposé des motifs, les données pouvant être traitées en vertu du règlement projeté seraient seulement celles qui « *sont strictement nécessaires pour la réalisation des missions confiées par le législateur* ».

La Commission nationale suppose que toutes les données correspondant aux catégories énumérées à l'article 5 ne sont pas collectées systématiquement d'office pour chaque personne concernée, mais que sont collectées seulement les données dont la collecte s'avère indispensable conformément aux principes de nécessité et proportionnalité.

Cela vaut en particulier pour les données dites sensibles à savoir les données raciales ou ethniques (article 5 paragraphe 1. point 14) ou les convictions philosophiques, politiques et religieuses ainsi que l'appartenance syndicale (article 5 paragraphe 1 point 15).

Les points 9, 14 et 15 de l'article 5 se réfèrent à des données sensibles dont le traitement est en principe interdit par l'article 6 paragraphe (1) de la loi modifiée du 2 août 2002, à moins que le traitement ne soit mis en œuvre par voie de règlement grand-ducal tel que prévu à l'article 17 de la même loi (article 6 paragraphe (2) (h)), ce que le gouvernement se propose de faire par le texte sous examen.

La Commission nationale note que le SRE ne sera donc pas autorisé à collecter des données relatives à la santé et à la vie sexuelle.

Elle considère également que la formulation « *informations que les techniques d'enregistrement utilisées par le Service de Renseignement de l'Etat ont pu relever* » (article 5 paragraphe 3) pourrait être clarifiée et complétée par quelques précisions supplémentaires.

En ce qui concerne les écoutes téléphoniques, ne faudrait-il pas insérer une référence expresse à la procédure prévue aux articles 88-3 et 88-4 du Code d'instruction criminelle ? Il en est de même pour les données de traçage de télécommunications pour autant que celles-ci ne relèvent pas de l'article 5 paragraphe 1. points 3 et 4 de l'avant projet de règlement.

De manière plus générale, aucune mesure touchant à un droit constitutionnellement protégé tel que le secret des communications ou l'inviolabilité du domicile ne peuvent avoir lieu sans qu'un texte légal n'en précise les conditions.

Le principe de légalité et de prévisibilité instauré par l'article 8 paragraphe 2 de la Convention européenne des Droits de l'Homme et des Libertés fondamentales présuppose que

toute ingérence dans la vie privée des citoyens soit non seulement nécessaire dans une société démocratique pour un des intérêts publics majeurs y visés ou pour la protection des droits d'autrui (principe de proportionnalité), mais aussi qu'elle soit prévue par la loi.

Il convient de relever que la loi modifiée du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat ne comporte pas de base légale spécifique pour des techniques subreptices de collecte de données et d'enregistrement de sons et d'images autres que celles couvertes par les articles 88-3 et 88-4 prémentionnés à l'instar, de ce qui existe, en matière policière, avec les articles 48-12 à 48-23 du Code d'instruction criminelle sur l'observation et l'infiltration et en particulier l'observation effectuée à l'aide de moyens techniques prévue par l'article 48-13 paragraphes (2) et (3) du même Code.

Ad article 6

La Commission nationale salue la séparation des fichiers en une partie opérationnelle et une partie archives.

L'article 6 paragraphe 2. alinéa 2 dispose ce qui suit :

« Il sera procédé à un réexamen de la nécessité de conserver les données traitées au plus tard tous les cinq ans. Les délais commencent à courir à partir de la dernière mise à jour des renseignements concernant la personne physique ou morale visée en relation avec la finalité ayant donné lieu au traitement des données concernées. »

Le principe du réexamen de la nécessité tous les 5 ans paraît louable même si on peut se demander si le réexamen ne peut pas avoir lieu à des intervalles plus courts, comme tous les trois ans. D'ailleurs un tel réexamen a lieu tous les trois ans pour ce qui est des données des fichiers Europol[25] ainsi que des signalements du système d'information Schengen de deuxième génération[26].

La Commission nationale a cependant du mal à comprendre en quoi consiste précisément une « *mise à jour* » en l'espèce. S'agit-il simplement de n'importe quel ajout, modification ou suppression de données, voire même de la dernière consultation ? Ou s'agit-il d'une vérification de l'exactitude toutes les données concernant une personne déterminée, ce qui nous semble peu probable ?

Ceci s'avère important pour savoir à partir de quel moment on fait courir le délai de 5 ans.

Le texte du règlement devrait donner des réponses à ces questions.

[25] Article 20 paragraphe 1. de la Décision du Conseil du 6 avril 2009 portant création de l'Office européen de police (Europol) (2009/371/JAI), Journal officiel n°L 121 du 15/05/2009 p. 0037 - 0066.

[26] Article 29 paragraphe 2. du Règlement (CE) n°1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II), Journal officiel n°L 381 du 28/12/2006 p. 0004 - 0023.

Ad article 8

Cette disposition prévoit que le l'archivage des données, qui peut avoir lieu conformément à l'article 7, est, en principe, limité à une durée de 10 ans, sauf en cas de durée de conservation plus longue justifiée.

Au regard de la limitation des accès aux données des archives et des garanties prévues, ce délai de conservation n'apparaît pas comme disproportionné.

Ad article 11

L'article 11 prévoit que lors de chaque traitement de données, les informations relatives à l'agent du SRE ayant procédé au traitement ainsi que la date et l'heure du traitement doivent être enregistrées.

La Commission rend attentif au fait qu'en vertu de la définition du traitement par l'article 2 lettre (r) de la loi modifiée du 2 août 2002, cette journalisation concernera en l'espèce notamment la création d'un fichier, l'ajout de données supplémentaires, la modification de données, la suppression de données, mais également le simple accès aux données.

Elle estime qu'une telle journalisation est une condition nécessaire pour pouvoir protéger le citoyen contre les risques de dérives et d'abus. La journalisation est aussi un outil indispensable aux contrôles internes qui devraient régulièrement être effectuées au sein d'une organisation et permet un contrôle efficace par l'autorité de contrôle prévue par l'article 17 paragraphe (2) la loi modifiée du 2 août 2002.

L'avant-projet de règlement prévoit que les données de journalisation sont effacées après un délai de trois ans après leur premier enregistrement, sauf lorsqu'elles font l'objet d'une procédure de contrôle.

Cependant, en cas de fuite ou d'abus relatif aux données traitées, il est possible que les faits y relatifs ne soient connus que longtemps après leur survenance, éventuellement à un moment où les données de journalisation ont déjà été effacées. Or, il devrait être du bon droit de chaque citoyen de pouvoir recevoir des informations précises sur l'origine de la faute dont il est le cas échéant la victime. Eu égard aux dysfonctionnements au sein du SRE, révélés récemment, une durée de conservation plus longue pour les données de journalisation devrait s'imposer.

La Commission nationale estime dès lors que les données de journalisation devraient faire l'objet d'un archivage pendant une durée de 10 ans après l'expiration du délai de trois ans prémentionné.

Selon l'article projeté, sont enregistrées les informations relatives à l'agent du Service de Renseignement de l'Etat ayant procédé au traitement ainsi que la date et l'heure du traitement. L'article ne précise cependant rien sur les motifs d'une consultation.

La CNPD estime qu'il serait nécessaire qu'au moins une information sommaire sur les motifs d'une consultation des données soit prévue à l'instar d'autres textes législatifs comme par exemple l'article 34-1 de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection Générale de la Police ou l'article 138 de la loi du 29 août 2008 sur la libre circulation des personnes et l'immigration.

Ad article 12

L'article 12 prévoit la possibilité pour le SRE de communiquer des données à certaines institutions tierces. Il nous semble recommandable que ces transferts de données soient retraçables et fassent dès lors l'objet d'une documentation.

Ad articles 1, 3, 4, 7, 9, 10, 12,13 et 14

Ces articles n'appellent pas d'observations de la part de la Commission nationale.

2. L'avant-projet de règlement grand-ducal pris en exécution de l'article 23 de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité

Ad article 5

L'article 5 énumère les catégories de données appelées à figurer dans le fichier « e-ANS ».

La Commission nationale salue que le texte donne une énumération plus précise des données traitées que celle relative au fichier e-RSN de l'article 5 de l'avant-projet de règlement grand-ducal pris en exécution de l'article 4 de la loi modifiée du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat.

Elle déplore cependant que le texte ne donne aucune précision sur l'origine des données. Au moins, le texte devrait faire une distinction entre les données que le demandeur d'une habilitation doit fournir lui-même et celles qui sont collectées par d'autres moyens.

Ad article 6

L'article 6 énumère les données appelées à figurer sur la fiche succincte. Plusieurs types de données sont décrits de manière précise aux lettres a) à g).

La Commission nationale se demande cependant en quoi peuvent consister « *les remarques particulières générales* » (lettre h)). Sans davantage de précisions, n'y a-t-il pas un risque que le principe d'une conservation d'une quantité très limitée de données dans la fiche succincte ne soit contourné ?

Ad article 9

L'article 9 prévoit plusieurs délais de conservation des données dans la partie « archivage ». Ces délais apparaissent comme proportionnés, sauf en ce qui concerne celui prévu au paragraphe 4 suivant lequel la fiche succincte doit être conservée pendant un délai de trente ans. Malgré les explications fournies au commentaire des articles, cette durée de conservation nous semble excessive.

Ad article 13

L'article 13 prévoit la journalisation des traitements de données effectués.

La Commission nationale renvoie à ses observations relatives à l'article 11 de l'avant-projet de règlement grand-ducal pris en exécution de l'article 4 de la loi modifiée du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat en ce qui concerne la durée de conservation des données de journalisation.

De même, elle renvoie à ses commentaires relatifs à l'article 11 précité en ce qui concerne la journalisation des motifs de consultation des fichiers.

Ad article 14

En ce qui concerne la communication de données à d'autres autorités, nous renvoyons aux observations formulées ci-dessus relatives à l'article 12 de l'avant-projet de règlement grand-ducal pris en exécution de l'article 4 de la loi modifiée du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat

Pour le surplus, les autres articles du texte sous examen n'appellent pas d'observations de la part de la Commission nationale.

Ainsi décidé à Esch-sur-Alzette en date du 28 juin 2013.

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°6381 portant réforme de l'exécution des peines, au projet de loi n°6382 portant réforme de l'administration pénitentiaire et au projet de règlement grand-ducal portant organisation des régimes internes des établissements pénitentiaires

Délibération n°302/2013
du 5 juillet 2013

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

Par courrier du 12 janvier 2012, respectivement du 7 août 2012, Monsieur le Ministre de la Justice a invité la Commission nationale à se prononcer au sujet du projet de loi n°6381 portant réforme de l'exécution des peines, au sujet du projet de loi n°6382 portant réforme de l'administration pénitentiaire et du projet de règlement grand-ducal portant organisation des régimes internes des établissements pénitentiaires.

Etant donné que les trois projets sont liés, elles font l'objet d'un avis unique de la part de la CNPD. Ci-dessous sont passées en revue les dispositions qui donnent lieu à des observations.

Le projet de loi n°6381 portant réforme de l'exécution des peines

Le projet de loi n°6381 prévoit de conférer une base légale à la surveillance électronique de condamnés, alors que, selon le commentaire des articles du projet de loi, environ 200 condamnés ont fait l'objet d'un placement sous surveillance électronique depuis l'année 2007.

Si la Commission nationale se félicite de ce qu'une base légale soit conférée à la pratique de la surveillance électronique, le texte actuellement soumis appelle les remarques suivantes :

- Le projet de loi ne précise pas par ou sous les instructions de quelle institution ou personne, la surveillance sera effectuée.

Le texte en projet devrait dès lors déterminer de manière claire et précise le responsable du traitement de données à des fins de surveillance.

- Les principes de base des modalités et du fonctionnement de la surveillance électronique devraient par ailleurs aussi être déterminés et précisés dans le texte sous examen.

- Enfin, la question de la nécessité ou non de l'accord de l'intéressé mérite d'être posée, vu qu'un tel traitement de données a un caractère extrêmement intrusif dans la vie privée des personnes concernées. Dès lors, il convient de se poser la question s'il n'est pas recommandable de demander le consentement de la personne concernée.

A ce sujet, on peut citer le Parquet général qui, dans son avis du 12 avril 2012, a remarqué ce qui suit :
« Il importe de rappeler – les expériences l'ont d'ailleurs démontré à plusieurs reprises – qu'il y a des personnes qui psychiquement ne supportent pas une surveillance électronique. Il y a même des cas où des personnes ont préféré un retour en prison plutôt que d'être mis sous surveillance électronique. »

D'ailleurs, dans certains autres pays, l'accord de la personne concernée est requis. Tel est le cas en France notamment.[27]

Le projet de loi n°6382 portant réforme de l'administration pénitentiaire

Ad article 4

L'article prévoit que le traitement de données à caractère personnel est mis en œuvre et géré par l'administration pénitentiaire.

Le texte ne précise cependant pas par qui l'administration pénitentiaire est représentée. Il conviendrait de préciser davantage qui, à l'intérieur de l'administration pénitentiaire et des différents établissements pénitentiaires est responsable de quelles données et qui a accès à quelles données.

La Commission nationale estime qu'il serait judicieux d'établir deux niveaux d'accès pour tous les dossiers des détenus. Sur un premier niveau, se trouveraient les informations de base accessibles à l'administration pénitentiaire. A un second niveau se trouveraient des informations plus détaillées qui seraient accessibles seulement aux personnes habilitées en raison de leur fonction à l'intérieur de l'établissement pénitentiaire concerné.

Elle constate avec satisfaction que les finalités du traitement de données à caractère personnel ont bien été précisées dans le

[27] Article 723-7 du Code de procédure pénale renvoyant à l'article 132-26-1 du même code.

texte sous examen et salue cette délimitation des finalités. Dans ce contexte, il y a lieu de relever que comme tous les individus, les personnes privées de liberté doivent également pouvoir jouir des droits fondamentaux dont le droit au respect de la vie privée. Il est vrai aussi que la jouissance de ces droits s'exerce de manière restreinte eu égard aux particularités de l'univers carcéral, de sorte qu'un équilibre doit être trouvé entre les droits fondamentaux des détenus et les contraintes organisationnelles inhérentes à l'exécution des peines privatives de liberté. En effet, la règle no. 3 de la recommandation (2006)2 du Comité des Ministres du Conseil de l'Europe aux Etats membres sur les Règles pénitentiaires européennes prévoit que:
« 3. Les restrictions imposées aux personnes privées de liberté doivent être réduites au strict nécessaire et doivent être proportionnelles aux objectifs légitimes pour lesquelles elles ont été imposées. »

Ad article 14

La Commission nationale se rallie à l'avis du Conseil d'Etat du 13 juillet 2012 en ce qui concerne la nécessité de préciser et justifier d'éventuelles dérogations au secret médical.

Ad article 25

Les catégories de données susceptibles d'être communiquées aux autorités judiciaires et policières par l'administration pénitentiaire et les établissements pénitentiaires mériteraient d'être précisées dans le texte. Il en est de même pour ce qui est des finalités permettant une telle communication.

Ad article 26

Quant à la communication d'informations à l'administration pénitentiaire par les autorités judiciaires et policières, la CNPD se rallie à l'avis du Conseil d'Etat du 13 juillet 2012 pour ce qui est du manque de précisions dans le texte en projet.

Ad article 36

La rédaction très vague de l'article projeté laisse entendre que des dérogations au secret des communications seraient possibles en matière de communications électroniques. Si tel était effectivement le cas, il conviendrait de préciser les dérogations sans équivoque dans la loi. A titre d'exemple de disposition légale prévoyant de telles dérogations, on peut mentionner l'article 64 de la loi belge concernant l'administration pénitentiaire[28].

Ad article 42

Cette disposition prévoit la prise d'empreintes digitales et de photographies des détenus.

La prise et la conservation de photographies peut constituer une atteinte à la vie privée et au droit à l'image. Vu la finalité d'authentification inhérente à la prise de photographies en l'espèce, une telle atteinte paraît cependant justifiée et proportionnée.

La Commission nationale estime cependant que le texte devrait déterminer la durée de conservation des photographies et des empreintes digitales.

Le projet de règlement grand-ducal portant organisation des régimes internes des établissements pénitentiaires

Ad article 5

Il est renvoyé aux considérations formulées au sujet de l'article 4 du projet de loi n°6382.

Ad article 45

Cette disposition prévoit la possibilité de soumettre une cellule à des mesures de vidéosurveillance.

La Commission nationale n'exclut pas qu'il y ait des hypothèses dans lesquelles le placement

[28] *« (…) 5. Afin de permettre un contrôle des communications téléphoniques du détenu pour des raisons d'ordre et de sécurité, les numéros formés par le détenu peuvent être enregistrés, conservés et consultés par l'administration pénitentiaire et communiqués aux autorités judiciaires dans les cas prévus par la loi, selon les modalités et dans les délais déterminés par arrêté royal, après avis de la Commission de la protection de la vie privée. Le détenu est informé, selon les modalités déterminées par le Roi, de la possibilité de l'enregistrement, de la conservation et de la consultation des numéros de téléphone par l'administration pénitentiaire, ainsi que de la possibilité qu'il a de demander à la Commission de la protection de la vie privée l'exercice du droit visé à l'article 13 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. ».*
http://staatsbladclip.zita.be/moniteur/lois/2005/02/01/loi-2005009033.html

sous-vidéosurveillance puisse s'avérer nécessaire.

Cependant, l'utilisation d'un dispositif de surveillance des cellules ne doit servir que lorsque des questions de sécurité urgentes l'exigent, comme par exemple des indices de suicide possible ; même dans un tel cas, la caméra de surveillance ne devrait pas remplacer les autres mesures à savoir les rondes fréquentes qui permettent un contact humain et qui assurent une surveillance efficace de l'état de santé du détenu.

Dans son avis n°4/2004 sur les traitements des données à caractère personnel au moyen de la vidéo-surveillance (doc. WP 89 adopté le 11 février 2004)[29], le Groupe de travail « Article 29 » sur la protection des données auprès de l'Union européenne retient que selon le principe de proportionnalité les systèmes de vidéo-surveillance *« ne peuvent être mis en place que sur une base de subsidiarité »*, c'est-à-dire que le responsable du traitement doit s'astreindre à une *« obligation d'intervention minimum »* (page 16).

Par ailleurs, en ce qui concerne les toilettes et, le cas échéant, les douches des cellules, un système de masquage électronique des images devrait être mis en place afin de garantir l'intimité de la personne, à l'exception d'une recommandation explicite de la part d'un médecin dans des cas tout à fait exceptionnels.

Enfin, en cas d'enregistrement des images, celles-ci doivent être supprimées rapidement après leur enregistrement.

Ainsi décidé à Luxembourg en date du 5 juillet 2013.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

[29] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89_fr.pdf

Avis relatif à l'avant- projet de règlement grand-ducal portant création des traitements de données à caractère personnel nécessaires à l'exécution de l'article 32 de la loi du 2 septembre 2011 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérale

Délibération n°345/2013
du 12 juillet 2013

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 13 juin 2013, le Ministère des Classes moyennes et du Tourisme a invité la Commission nationale à se prononcer au sujet de l'avant-projet de règlement grand-ducal portant création des traitements de données à caractère personnel nécessaires à l'exécution de l'article 32 de la loi du 2 septembre 2011 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales.

L'objectif de l'avant-projet de règlement consiste à déterminer les conditions et critères selon lesquelles le Ministre peut accéder aux données nécessaires pour vérifier si une personne satisfait aux exigences posées par la loi du 2 septembre 2011. Le commentaire des articles de l'avant-projet de règlement grand-ducal précise à juste titre que « *l'énumération des bases de données faite par la loi du 2 septembre 2011 n'étant que générale, une indication précise et détaillées des données échangées par les différents organismes publics s'avère nécessaire. En l'absence de précisions textuelles, le ministre aurait en effet vocation à accéder à toutes les données figurant dans les différents fichiers. Or, cela dépasse ce qui est nécessaire. Pour cette raison, le présent texte autorise l'accès uniquement aux données qui intéressent le ministre et qui sont nécessaire à l'instruction administrative de ses dossiers. Pour des raisons de sécurité juridique, un haut degré de précision des données est nécessaire. Une précision textuelle détaillée des données permet au cours de la procédure un contrôle a priori du principe de proportionnalité d'une part, et un contrôle a posteriori de la mise en œuvre du système informatique, d'autre part* ».

1) <u>Ad article 1</u>

L'article 32 paragraphe (1) de la loi du 2 septembre 2011 pose le principe de la mise en place d'un registre des entreprises dans lequel devront figurer toutes les données nécessaires au Ministère des classes moyennes pour octroyer, modifier, annuler, révoquer et faire le suivi des autorisations d'établissement et des autorisations particulières ainsi que pour faire le suivi des notifications faites par les prestataires de service étrangers.

En exécution de cette disposition, le paragraphe (2) de l'article 1er de l'avant-projet de règlement grand-ducal énumère en détail de quelles données il s'agit.

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

La Commission nationale salue la précision avec laquelle les

données sont énumérées, sauf pour ce qui est du dernier tiret du paragraphe (2) qui est écrit dans les termes suivants : « *toutes autres informations fournies par l'administré ou par d'autres administrations* ». Contrairement aux quatre premiers tirets, ce libellé est trop vague pour faire apparaître le caractère pertinent et nécessaire de ces informations et constitue en quelque sorte une catégorie « fourre-tout », de sorte qu'il conviendrait de préciser davantage quelles données sont exactement visées.

Le paragraphe (3) détermine le Ministre des Classes Moyennes comme responsable du traitement au sens de la loi modifiée du 2 août 2002 et le Centre des technologies de l'information de l'Etat (CTIE) comme sous-traitant.

2) Ad article 2

La Commission nationale félicite les auteurs du texte sous examen d'avoir suivi sa recommandation (délibération n°125/2011 du 15 avril 2011 - Avis de la Commission nationale pour la protection des données relatif à l'article 32 du projet de loi n°6158 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales) de s'inspirer du règlement grand-ducal du 26 septembre 2008 pris en exécution de la loi du 29 août 2008 sur la libre circulation des personnes et l'immigration et déterminant les données à caractère personnel auxquelles le Ministre ayant l'immigration dans ses attributions peut accéder aux fins d'effectuer les contrôles prévus par cette loi qui constitue un précédent illustrant une manière appropriée de déterminer de façon claire et limitative les accès justifiés par la finalité légitime inscrite dans la loi au regard des critères de nécessité et de proportionnalité.

L'article 2 de l'avant-projet de règlement grand-ducal énumère de façon limitative les données auxquelles le Ministre peut accéder via un système informatique direct afin de contrôler si une personne satisfait aux exigences posées par la loi du 2 septembre 2011. La disposition en question suscite les observations qui suivent.

L'article 2 lettre (a) de l'avant-projet de règlement grand-ducal se réfère aux registre général des personnes physiques et morales créé par la loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales. Comme indiqué dans la correspondance reçue par le Ministère des Classes Moyennes, il y a lieu d'adapter l'article 2 lettre (a) en faisant référence à 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. Celle-ci prévoit que les modalités d'accès et de transmission des données du registre national seront déterminées par règlement grand-ducal (article 10 de la loi du 19 juin 2013).

En ce qui concerne l'énumération des données sous l'article 2 lettre (a), la Commission nationale considère que des précisions devraient être fournies par les auteurs du texte de l'avant-projet de règlement afin de clarifier quelles données des *« ascendants et descendants »* de la personne concernée peuvent être accédées, en partant du principe que seules les données des « ascendants et descendants » au premier degré soient concernées (conformément à l'article 5 paragraphe (2) lettres (j) et (k) de la loi du 19 juin 2013 susmentionnée). Par ailleurs, la Commission nationale estime qu'il convient de préciser en quoi ces informations sur les *« ascendants et descendants »* sont pertinentes et nécessaires, eu égard à l'article 4 paragraphe (1) lettre (b) de la loi modifiée du 2 août 2002.

Quant à la lettre (e) dudit article 2 (fichier relatif aux bénéficiaires du revenu minimum garanti), la CNPD estime que le libellé actuel « les bénéficiaires du revenu minimum garanti » est ambigu, alors qu'il laisse entendre que le Ministre pourrait avoir accès aux données de l'ensemble des bénéficiaires du revenu minimum garanti figurant dans le fichier géré par le Fonds national de solidarité, respectivement par le Service national d'action sociale.

Etant donné que le Ministre peut seulement avoir accès sur demande aux données ou communication des données relatives à une personne précise ou un nombre précis de personnes, nous proposons de clarifier le libellé de la lettre (e) de l'article 2 qui pourrait avoir la teneur suivante : *« l'information si un demandeur ou titulaire d'une autorisation d'établissement est bénéficiaire ou non d'un revenu minimum garanti ».*

Les lettres (c), (d), (f), (g) et (h) dudit article 2 n'appellent pas d'observations particulières.

Finalement, la Commission nationale aimerait encore relever que l'article 32 paragraphe (2) lettre (g) de la loi du 2 septembre 2011 susmentionnée deviendra caduc dès l'entrée en vigueur de la loi du 29 mars 2013 relative à l'organisation du casier judiciaire et aux échanges d'informations extraites du casier judiciaire entre les Etats membres de l'Union européenne, à savoir le 1er août 2013.

3) <u>Ad articles 3 et 4</u>

En vertu de la loi modifiée du 2 août 2002, le responsable du traitement a l'obligation de mettre en œuvre toutes les mesures techniques et l'organisation appropriées afin d'assurer la sécurité et la confidentialité du traitement des données à caractère personnel.

Les articles 3 et 4 de l'avant-projet de règlement grand-ducal mettent en place une procédure d'accès aux données ainsi qu'un système de traçabilité des consultations des données effectuées par les agents du ministère. L'article 4 précise 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 peuvent être retracés ».*

A ce titre, la Commission nationale note avec satisfaction qu'elle a été suivie dans son avis du 15 avril 2011 relatif à l'article 32 du projet de loi n°6158 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions

libérales) alors que les dispositions des articles 3 et 4 de l'avant-projet de règlement grand-ducal, assurant la traçabilité des accès aux données de fichiers publics, constituent une bonne garantie contre d'éventuels abus.

Le paragraphe (2) de l'article 4 dispose que les données de journalisation sont effacées après un délai d'une année à compter de leur premier enregistrement, sauf si elles font l'objet d'une procédure de contrôle.

A ce sujet, la CNPD propose d'aligner la durée de conservation sur celle qui a été retenue par la loi du 5 juin 2009 relative à l'accès des autorités judiciaires, de la Police, de l'Inspection générale de la Police à certains traitements de données à caractère personnel mis en œuvre par des personnes morales de droit public qui prévoit que les informations relatives aux magistrats et aux membres du personnel de l'administration judiciaire ayant procédé à la consultation ainsi que les informations consultées, la date et l'heure de la consultation sont enregistrées et conservées pendant un délai de 3 ans. Cette durée nous paraît plus appropriée que celle d'un an envisagée pour préserver les possibilités de vérification du caractère licite de la consultation des données.

Ainsi décidé à Esch-sur-Alzette en date du 12 juillet 2013.

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°6566 facilitant l'échange transfrontalier d'informations concernant les infractions en matière de sécurité routière

Délibération n°385/2013
du 25 juillet 2013

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 11 mars 2013, lui demandant d'aviser l'avant-projet de loi facilitant l'échange transfrontalier d'informations concernant les infractions en matière de sécurité routière, entre-temps devenu le projet de loi n°6566, la Commission nationale expose ci-après ses réflexions et commentaires au sujet du projet de loi en question.

Le projet de loi sous avis a pour objet de transposer en droit national la directive 2001/82/UE du 25 octobre 2011 qui prévoit la mise en place d'une procédure d'échange d'informations transfrontalier en vue de permettre l'application transfrontière de sanctions relatives aux infractions les plus graves en matière de sécurité routière, lorsque celles-ci sont commises dans un pays de l'Union européenne autre que celui dans lequel le véhicule est immatriculé. L'Etat membre sur le territoire duquel une infraction déterminée en matière de sécurité routière sera commise par un conducteur dont le véhicule est immatriculé dans un autre Etat membre pourra accéder sur demande aux données relatives à l'immatriculation de ce véhicule.

Etant donné que le texte sous examen prévoit l'échange de données à caractère personnel transfrontalier concernant les auteurs présumés d'infractions routières, le projet a des implications directes en matière de protection des données.

La CNPD accueille favorablement le projet de loi dans on ensemble, alors qu'il transpose fidèlement la directive européenne précitée laquelle prévoit déjà des garanties appropriées suffisantes en termes de protection des données. A ce titre, elle voudrait se rallier à l'avis (2008/C 310/02) du Contrôleur européen de la protection des données du 8 mai 2008 relatif à la proposition de directive du Parlement européen et du Conseil facilitant l'application transfrontière de la législation dans le domaine de la sécurité routière lequel avait avisé favorablement la légitimité et la nécessité de l'échange de données transfrontalier, de même que la qualité des données personnelles traitées dans ce contexte.

L'article 7 du projet de loi appelle cependant les observations suivantes :

<u>Ad article 7 paragraphe (1) du projet de loi</u>

Le traitement des données, c'est-à-dire l'échange de données relatives à l'immatriculation des véhicules est opéré par la Police grand-ducale laquelle est désignée à l'article 4 du projet de loi comme point de contact national.

L'article 7 paragraphe (1) précise que *« le traitement des données à caractère personnel dans le cadre de la présente loi se fait conformément à la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière*

pénale ». Cette décision-cadre a pour but d'assurer à l'échelle de l'UE un niveau élevé de protection des droits et libertés fondamentaux des personnes physiques lors du traitement de données à caractère personnel dans le cadre de la coopération policière et judiciaire en matière pénale.

En vertu de l'article 29 paragraphe 2 de la décision-cadre, les Etats membres étaient tenus de transmettre au secrétariat général du Conseil et à la Commission européenne le texte des dispositions qui transposent en droit national les obligations qui leur incombent jusqu'à la date du 27 novembre 2010. Or, cette décision-cadre n'a jamais fait l'objet d'une transposition proprement dite en droit national. Le Luxembourg a informé la Commission européenne avoir transposé les dispositions de la décision-cadre en faisant référence à 20 textes législatifs et réglementaires éparses en matière pénale pour la plupart antérieurs à la dite décision-cadre[30].

La CNPD, ayant analysé les 20 textes en question, est d'avis que ceux-ci ne peuvent pas être considérés comme opérant une transposition fidèle et exhaustive, alors qu'ils ne couvrent pas intégralement le champ d'application de la décision-cadre. En toute logique de transposition d'un texte européen en droit national, l'article 7 paragraphe (1) du projet de loi sous avis devrait faire référence aux textes nationaux concernés en l'espèce au lieu de renvoyer à la décision-cadre européenne. Même si l'article 7 paragraphe (1) fait aussi référence à la loi modifiée du 2 août 2002, toujours est-il que celle-ci ne couvre pas entièrement le champ d'application de la décision-cadre précitée.

Le commentaire de l'article 7 du projet de loi indique certes que « *le traitement de données en question est couvert par le règlement grand-ducal du 21 décembre 2004 portant autorisation de la création d'un fichier des personnes ayant subi un avertissement taxé en matière de circulation routière* ». Le fichier précité ne peut cependant traiter que les données relatives aux personnes ayant commises une infraction punie d'une peine de police conformément à la loi modifiée du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies publiques. Or, plusieurs des infractions à la circulation routière énumérées dans le projet de loi (p.ex. conduite en état d'ébriété, conduite sous l'influence de drogues, excès de vitesse) sont susceptibles de constituer des délits, punies par une peine correctionnelle. Le traitement des données relatives à ces infractions délictuelles n'est donc pas complètement couvert

[30] Rapport de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions fondé sur l'article 29, paragraphe 2, de la décision cadre 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 (COM(2012)12 final) {SEC(2012) 75 final}.

par le règlement grand-ducal du 21 décembre 2004 précité, mais est susceptible de tomber dans le champ d'application du règlement grand-ducal modifiée du 2 octobre 1992 relatif à la création et à l'exploitation d'une banque de données nominatives de police générale (« règlement Ingepol ») et, le cas échant, de la loi modifiée du 5 juin 2009 relative à l'accès des autorités judiciaires, de la Police et de l'Inspection générale de la Police à certains traitements de données à caractère personnel mis en œuvre par des personnes morales de droit public. La CNPD voudrait encore relever dans ce contexte que le règlement Ingepol qui date de 1992 ne répond pas à toutes les exigences juridiques de protection des données découlant de la loi modifiée du 2 août 2002, ni de la décision-cadre 2008/97/JAI précitée et qu'il devrait être remplacé par un nouvel règlement grand-ducal en exécution de l'article 17 paragraphe (1) lettre (a) de la loi modifiée du 2 août 2002. Dans ses rapports annuels, l'autorité de contrôle spécifique « Article 17 » a d'ailleurs régulièrement critiqué la prorogation annuelle du règlement Ingepol depuis l'adoption de la loi modifiée du 2 août 2002 ainsi que l'absence d'adoption d'un nouvel règlement grand-ducal.

Eu égard aux considérations ci-avant, la CNPD estime que l'absence d'un texte spécifique de transposition de la décision-cadre 2008/977/JAI et la dispersion de dispositions de protection des données en matière pénale dans 20 différents textes légaux ne sont pas de nature à favoriser ou à faciliter la prévisibilité et l'exercice effectif des droits protecteurs des citoyens. Elle recommande dès lors au gouvernement de transposer la décision-cadre 2008/977/JAI dans un seul et même texte législatif national, alors qu'il y a un besoin pressant dans l'intérêt des citoyens à voir protégés leurs droits et libertés fondamentaux.

Ad article 7 paragraphe (2) du projet de loi

L'article 7 paragraphe (2) du projet de loi dispose que « *toute personne concernée a le droit d'obtenir des informations sur les données à caractère personnel transmises dans le cadre de la présente loi au point de contact national de l'Etat membre de l'infraction, y compris la date de la demande et l'autorité compétente de l'Etat membre de l'infraction* ».

Cette disposition confère dès lors à toute personne concernée, c'est-à-dire à tout résident luxembourgeois, auteur présumé d'une infraction à la circulation routière commise dans un autre Etat membre, le droit d'accéder aux données relatives à l'immatriculation de son véhicule qui ont été transmises par la Police grand-ducale au point de contact national de l'Etat membre de l'infraction.

Il s'agit là d'un droit d'accès dit « direct » que la personne concernée devrait pouvoir exercer directement auprès de la Police grand-ducale. Toutefois, l'article 7(2) ne le précise pas. Le commentaire de l'article indique simplement que « *cette disposition ne règle pas la question de l'autorité à laquelle la personne concernée doit s'adresser en vue d'obtenir cette information. En effet, l'accès aux données est censé se faire conformément à la législation luxembourgeoise relative à la protection des données à caractère personnel* ».

Or, en ce qui concerne les traitements de données personnelles effectués par la Police grand-ducale, il s'avère que la loi modifiée du 2 août 2002 relative à la protection des données ne confère aux personnes concernées qu'un accès dit « indirect » qui ne peut s'exercer que par l'intermédiaire de l'autorité de contrôle spécifique « Article17 ». Celle-ci procède aux vérifications et investigations utiles, fait opérer les rectifications nécessaires et informe la personne concernée que le traitement en question ne contient aucune donnée

contraire aux conventions, à la loi et à ses règlements d'exécution (cf. article 17 paragraphe (2) dernier alinéa). Il résulte de cette disposition que la personne concernée ne reçoit pas communication ou n'a pas accès aux détails des données traitées par la Police. Se pose dès lors un problème de compatibilité de l'article 17 paragraphe (2) dernier alinéa de la loi modifiée du 2 août 2002 avec l'article 7 paragraphe (2) du projet de loi sous avis, alors que ce dernier confère à la personne concernée le droit d'obtenir les détails des données transmises dans un autre Etat membre, y compris la date de la demande et l'autorité compétente de l'Etat membre de l'infraction.

Etant donné qu'une loi spéciale (loi en projet sous examen) déroger à la loi générale (loi modifiée du 2 août 2002)[31] et dans un souci de sécurité juridique, la CNPD est d'avis que l'article 7 paragraphe (2) du projet de loi devrait instaurer pour le moins un droit d'accès en faveur des personnes concernées qui s'exerce directement auprès de la Police grand-ducale.

Il résulte encore de la disposition sous examen que le droit d'accès doit s'exercer sur demande. La CNPD se demande cependant s'il ne conviendrait pas mieux 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. Bien que la directive et le projet de loi prévoient que les données accédées dans un autre Etat membre ne peuvent pas être utilisées à d'autres fins, il ne peut pas être exclu qu'un Etat membre accède aux données en dehors du champ d'application défini dans la directive 2011/82/UE et la loi en projet.

Ainsi décidé à Esch-sur-Alzette en date du 25 juillet 2013.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

[31] La loi spéciale transposant par ailleurs un directive plus récente (2011/82/UE) que celle (1995/46/CE) ayant été transposée par la loi générale.

Avis relatif au projet de loi n°6593 portant modification de la loi du 16 juin 2004 portant réorganisation du centre socio-éducatif de l'Etat et de diverses autres lois et au projet de règlement grand-ducal portant organisation de l'unité de sécurité du centre socio-éducatif de l'Etat

Délibération n°386/2013
du 25 juillet 2013

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

Par courrier du 22 janvier 2013, respectivement du 12 juillet 2013 le Ministre de la Famille et de l'Intégration a invité la Commission nationale à se prononcer au sujet de

- l'avant-projet de loi portant modification de la loi 1. de la loi du 16 juin 2004 portant réorganisation du centre socio-éducatif de l'Etat 2. de la loi du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'Etat 3. de la loi du 29 juin 2005 fixant les cadres du personnel des établissements d'enseignement secondaire et secondaire technique 4. de la loi du 23 juillet 1952 concernant l'organisation militaire (ci-après désigné « *le projet de loi* »).

- et du projet de règlement grand-ducal portant organisation de l'unité de sécurité du centre socio-éducatif de l'Etat (ci-après désigné « *le projet de règlement* »).

Les deux textes sous avis ont principalement pour objet de rendre l'organisation de l'unité de sécurité du centre socio-éducatif de l'Etat conforme aux principes applicables au niveau international aux mineurs privés de liberté, de préciser le régime disciplinaire applicable au sein de l'unité de sécurité et de faire fonctionner celle-ci.

La Commission nationale limitera ses observations aux dispositions qui ont trait à la protection des données et à la vie privée et plus particulièrement à l'article I point 10° du projet de loi et les articles 5 à 9 du projet de règlement grand-ducal.

Ces dispositions prévoient notamment la mise en place d'un registre général ainsi que des dossiers individuels des pensionnaires qui peuvent être établis sous forme de bases de données informatiques.

1. Le responsable du traitement

L'article I point 10° du projet de loi précise sans équivoque que le ministre ayant la Famille dans ses attributions est le responsable du traitement des différents traitements à caractère personnel prévus par les textes sous avis.

2. Finalités du traitement

La CNPD note que les finalités des traitements de données à caractère personnel ont bien été décrites dans le commentaire de l'article I point 10° du projet de loi qui précise que

- le registre général est mis en œuvre afin :
  - de répertorier les pensionnaires vivant dans l'unité de sécurité, et
  - de répertorier l'ensemble des entrée et sorties des personnes ayant accès à l'unité de sécurité
- le dossier individuel a comme finalités de regrouper l'ensemble des informations utiles et nécessaires pour assurer un suivi des pensionnaires pendant leur séjour dans l'unité de sécurité.

Eu égard aux principes de légalité (article 8 de la Convention européenne des droits de l'Homme du 4 novembre 1950) et du principe de finalité (article 6 § 1 lettre (b) de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données), il conviendrait d'e spécifier les finalités des traitements ci-avant dans le texte même de loi. La Cnpd suggère dès lors d'adapter en ce sens l'article I point 10° du projet de loi.

3. Les catégories de données traitées

Les articles 5 à 8 du projet de règlement grand-ducal spécifient les données et catégories de données qui figureront dans le registre général, le dossier individuel et le bulletin disciplinaire. La CNPD constate avec satisfaction l'énumération détaillée des données traitées.

Les données traitées dans le cadre du registre général et du bulletin disciplinaires n'appellent pas d'observations particulières.

En ce qui concerne la collecte et l'utilisation des données personnelles dans le cadre du dossier individuel, la CNPD voudrait formuler les observations qui suivent.

L'article 6 du projet de règlement précise que le dossier individuel est constitué d'une série de documents et informations dont notamment une partie médicale dont les documents sont conservées dans une farde séparée à l'infirmerie et une notice individuelle comportant 19 catégories de données (énumérées à l'article 7 du projet de règlement).

L'article I point 10° premier alinéa du projet de loi et l'article 13 paragraphe (1) du projet de règlement prévoient la prise de photographies du visage du pensionnaire admis dans l'unité de sécurité. La photo d'identité du pensionnaire fera partie du dossier individuel en vertu de l'article 6 du projet de règlement.

La prise et la conservation de photographies est susceptible de constituer une atteinte à la vie privée et au droit à l'image. Eu égard à la finalité d'authentification inhérente à la prise de photographies en l'espèce, et les explications fournies dans le commentaire des articles du projet de loi, la collecte et le traitement de cette donnée paraissent cependant légitimes et proportionnés.

En ce qui concerne la collecte des données relatives à la

confession, la Commission nationale se pose la question de la nécessité de disposer de cette information.

De manière générale, l'article 6 de la loi modifiée du 2 août 2002 interdit le traitement des données dites sensibles parmi lesquelles figure les données relatives aux convictions religieuses, sauf dans les cas d'exception limitativement énumérés à l'article 6 paragraphe (2) de la loi (article 8 paragraphe 2 de la Directive 95/46/CE). Parmi les exceptions qui auraient vocation à s'appliquer en l'espèce figurent notamment le consentement de la personne concernée (article 6 paragraphe (2) lettre (a)) ou la collecte des données dans le cadre d'un traitement de données judiciaires au sens de l'article 8 de la loi modifiée du 2 août 2002 (article 6 paragraphe (2) lettre (i)).

Le projet de règlement précise que l'information relative à la confession ne pourra être collectée qu'avec le consentement exprès du pensionnaire. L'utilité de cette donnée serait justifiée dans le cadre de l'organisation éventuelle d'une entrevue du pensionnaire avec un ministre du culte ou de la détermination du régime alimentaire.

La CNPD estime que le traitement des données relatives à la confession n'est légitime et proportionné qu'à la condition que le consentement du pensionnaire soit libre. Pour que celui-ci soit libre, il faudra que l'indication de la confession par le pensionnaire soit facultative et non pas obligatoire. A ce sujet, il est encore renvoyé au point 4. du présent avis. Se pose en outre la question de la validité du consentement demandé aux pensionnaires mineurs d'âge.

Par ailleurs, il est prévu de traiter dans le dossier individuel des données relatives à la santé du pensionnaire. Un dossier médical, conservé dans une farde séparé à l'infirmerie, contiendra les documents relatifs à la santé physique et mentale du pensionnaire. L'accès à ce dossier est strictement réservé au personnel médical et exceptionnellement au directeur du centre auquel est confiée la garde du pensionnaire.

L'accès au dossier médical par le directeur est susceptible de constituer une violation au secret médical. Or, les auteurs du projet de règlement grand-ducal justifient cette entorse en renvoyant aux explications d'une recommandation formulée par la médiateure. La CNPD partage l'analyse de la médiateure pour justifier la nécessité d'accéder au dossier médical par le directeur. Les dérogations au secret médical doivent obligatoirement être prévues dans un texte légal ce que les auteurs du projet de règlement grand-ducal se proposent de faire en l'espèce.

4. Origine des données

Les projets de loi et de règlement ne spécifient rien sur l'origine des données. Proviennent-elles toutes ou seulement une partie des personnes concernées elles-mêmes ? Quelles données sont le cas échéant reprises des décisions des autorités judiciaires ? Parmi les données qui sont fournies par le pensionnaire, certaines du moins sont-elles facultatives ? Les pensionnaires sont-ils informés des conséquences lorsqu'ils refusent le cas échéant de fournir une donnée considérée comme obligatoire ?

Qu'en est-il si un pensionnaire est déjà, au moment du placement, pensionnaire du centre socio-éducatif, mais non de l'unité de sécurité. Existe-t-il des dossiers semblables pour le centre socio-éducatif en général (hors unité de sécurité) dont les données sont transmises à l'unité de sécurité et puis le cas échéant complétées ?

Par souci de clarté juridique, la Commission nationale estime que l'origine des données et le caractère obligatoire ou facultatif des données devraient être précisés dans les textes sous examen.

5. Les personnes ayant accès aux données

Le personnel du centre socio-éducatif

D'après l'article 9 du projet de règlement, seuls le directeur ou son délégué auraient accès aux données. Or, le commentaire de l'article 7 du projet de règlement précise que certaines données relatives à la santé et non issues du dossier médical seraient communiquées aux membres du personnel de l'unité de sécurité pour que ceux-ci soient avertis d'avance lorsque le pensionnaire fait un malaise ou une crise suite à ses problèmes de santé. Les membres du personnel encadrant n'ont-il pas accès à d'autres données en plus dans le cadre de leurs taches professionnels ? La question mérite d'être clarifiée. De manière générale, les textes sous avis devraient préciser qui a accès à quelles données suivant le principe que chaque agent ne doit avoir accès qu'aux données nécessaires à l'accomplissement de ses tâches.

Les destinataires externes

Selon l'article 9 du projet de règlement, une série d'organismes peuvent avoir accès aux données *« pour exercer un acte de leur ministère ou de leurs fonctions après avoir justifié de leur qualité et de leur identité auprès le directeur ou de on délégué ».*

La Commission nationale estime que les modalités d'accès aux données par les différents organismes devraient être précisées dans le texte et complétées le cas échéant par un renvoi aux textes légaux définissant les missions légales respectives dans le cadre desquelles ces organismes pourraient avoir accès aux dossiers.

Par ailleurs, il nous semble recommandable que les communications de donnés à ces organismes soient retraçables et fassent donc l'objet d'une documentation. Il conviendrait dès lors de prévoir un système qui permette de retracer a posteriori qui a eu accès à quelles données, et pour quelle raison, afin que des abus éventuels puissent être évités.

6. La durée de conservation des données

Les textes sous avis ne définissent aucun délai légal de conservation des données.

L'article 7 du projet de règlement dispose ce qui suit :

« A la libération du pensionnaire son dossier individuel est classé dans les archives établis auprès le service de gestion administrative du centre pour être reproduit et continué en cas d'un nouvel placement. »

Or, l'article 4 paragraphe (1) lettre (d) de la loi modifiée du 2 août 2002 et l'article 6 paragraphe 1. lettre e) de la Directive 95/46/CE posent le principe que les données personnelles ne doivent pas être conservées pendant une durée qui excède celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées.

Par ailleurs, une conservation des données limitée dans le temps est une garantie supplémentaire en termes de protection des droits et libertés fondamentaux et de droit à l'oubli.

Etant donné que les pensionnaires sont des adolescents, il n'y a aucune raison que les données soient conservées pendant un délai trop long, après la fin des mesures de placement et du moins après avoir atteint l'âge de la majorité. Il serait dès lors nécessaire que les textes sous examen fixent une durée pendant laquelle les données peuvent être conservées dans les bases de données.

Le projet de loi dans son article I point 10° indique encore que les archives qui contiennent les dossiers individuels des pensionnaires sont strictement confidentielles et qu'ils ne peuvent pas faire l'objet d'une communication à des tiers. L'accès à ces archives est limité aux personnes directement concernées par le jugement de l'affaire en cause « ou aux autres personnes dûment autorisées par le directeur ». Dans ce contexte se pose la question de savoir qui seraient ces « autres personnes » (qui peuvent donc quand-même être des tiers) et sur base de quels critères le directeur autoriserait ces personnes à accéder aux dossiers.

7. Les mesures de sécurité

Les textes sous avis ne prévoient pas de dispositions relatives aux mesures de sécurité et de confidentialité des données. Certes, les articles 22 et 23 de la loi modifiée du 2 août 2002 relatifs à la sécurité des traitements de données à caractère personnel sont applicables aux traitements de données envisagés. Cependant vu l'ampleur de la collecte de données à caractère personnel en cause, il conviendrait de prévoir des mesures de sécurité spécifiques dans le texte du règlement grand-ducal et plus particulièrement en ce qui concerne le contrôle de l'utilisation, de l'accès et de la transmission des données.

À l'instar d'autres textes légaux[32] ces mesures devraient notamment englober des restrictions physiques précises à l'accès aux données stockés sur papier et un système de traçage des accès aux fichiers dans l'hypothèse où il est envisagé de gérer le registre général, le dossier individuel et le bulletin disciplinaires sous forme électronique.

Ainsi décidé à Esch-sur-Alzette en date du 25 juillet 2013.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

[32] p.ex. - le règlement grand-ducal du 26 septembre 008 pris en exécution de la loi du 29 août 2008 sur la libre circulation des personnes et l'immigration et déterminant les données à caracère personnel auxquelles le Ministère ayan l'immigration dans ses attributions peut accéder ;
- loi du 5 juin 2009 relative à l'accès des autorités judiciaires, de la Police, de l'Inspection générale e la Police à certains traitements de données à caractère personnel etc.

Annexes

Avis relatif au projet de règlement grand-ducal relatif aux modalités du comptage de l'énergie électrique et du gaz naturel

Délibération n°566/2013
du 13 décembre 2013

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

Par courrier du 24 octobre 2013, le Ministre de l'Economie et du Commerce extérieur, Monsieur Etienne Schneider, a invité la Commission nationale à se prononcer au sujet d'un avant-projet de règlement grand-ducal relatif aux modalités du comptage de l'énergie électrique et du gaz naturel.

En prémisse de ses commentaires passant en revue les différents articles du projet de règlement, la Commission nationale note que le déploiement des compteurs intelligents nécessite la mise en place d'un système de sécurisation des données performant et évolutif. Afin de garantir la confidentialité des renseignements à caractère personnel, le chiffrement des données et la traçabilité des connexions aux serveurs doivent être assurés, et un système d'habilitation des personnes ayant accès aux données doit être mis en place. De plus, la sécurité des données doit se faire tout au long de la chaîne de communication, au travers de tous les acteurs et de tous les moyens de communication. La Commission nationale précise que cette obligation de sécurité découle des articles 21 à 23 de la loi modifiée du 2 août 2002.

Par ailleurs, la Commission nationale tient à souligner le risque de dérives potentielles liées à l'utilisation des compteurs intelligents. Le déploiement des compteurs intelligents est un projet national ayant pour but in fine d'être installé dans l'ensemble des habitations luxembourgeoises. Par conséquent, au regard des informations précises collectées par lesdits compteurs, il sera possible de déduire les habitudes de vie (heure de lever, heure de coucher, présence ou absence au domicile,…) ou même, dans des cas spécifiques, le type d'appareils utilisés. Par

conséquent, il y a lieu de définir strictement les conditions dans lesquelles les gestionnaires de réseaux et les fournisseurs pourront utiliser les données de comptage, afin que les compteurs intelligents soient, d'une part, un minimum attentatoire à la vie privée des citoyens et, d'autre part, qu'ils améliorent la gestion de l'énergie pour les acteurs du marché de l'énergie.

Ci-après, sont passés en revue les articles de l'avant-projet qui donnent lieu à observations de la Commission nationale.

1. L'article 1

L'article 1er du projet de règlement définit à la fois les gestionnaires de réseau de distribution ainsi que, le cas échéant, les gestionnaires de réseau de transport d'électricité et de gaz naturel comme étant « responsables ». Tel que l'article est rédigé actuellement, la Commission nationale relève que la notion de « responsable » se révèle insuffisante pour qualifier les gestionnaires de réseaux. En effet, cette notion pourrait être interprétée dans le sens où les gestionnaires de réseaux seraient uniquement tenus pour responsables de mettre en application les modalités pratiques permettant le comptage intelligent de l'énergie électrique et du gaz naturel.

Or, est-on obligé de constater que « les gestionnaires de réseaux » sont également amenés à traiter des données à caractère personnel dans la mesure où les informations collectées (numéro d'identification unique du compteur, date, heure, profil de charge du compteur, alertes, informations sur le niveau du réseau, comme la tension, les coupures de courant et la qualité de l'alimentation électrique,…) permettent d'identifier de manière directe ou indirecte les habitudes des utilisateurs des compteurs intelligents.

La Commission nationale estime donc que les gestionnaires de réseaux doivent également être considérés comme « responsables du traitement » au sens de l'article 2 (n) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel définissant le responsable de traitement comme étant *« la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données à caractère personnel. Lorsque les finalités et les moyens du traitement sont déterminés par ou en vertu des dispositions légales, le responsable du traitement est déterminé par ou en vertu des critères spécifiques conformément aux dispositions légales ».*

Il est donc nécessaire de préciser que les gestionnaires de réseaux sont à considérer comme étant responsables de l'activité de déploiement des modalités de comptage mais également comme étant responsable de traitement de données au sens de l'article 2 (n) de la loi précitée.

Quant au Groupement d'intérêt économique (GIE), ce dernier doit être considéré comme sous-traitant (au sens de l'article 2 (o) de la loi modifiée du 2 août 2002) dans la mesure où il ne fait qu'agir sous l'autorité des gestionnaires de réseau. En effet, la collecte automatisée des données de comptage est effectuée via le système central commun du GIE pour l'usage des gestionnaires de réseau qui se chargeront ensuite de les transmettre aux fournisseurs choisis par les clients finals.

Les fournisseurs d'électricité et de gaz naturel sont considérés comme étant « destinataires » des données collectées au sens de l'article 2 (d) de la loi modifiée du 2 août 2002. Ces derniers seront toutefois tenus pour « responsables des traitements » à l'égard des traitements qu'ils effectueront à partir des données obtenues.

2. L'article 2

Les compteurs intelligents indiquent la consommation

d'énergie totale ainsi que l'historique des consommations dans le temps. À l'aide de telles informations, il est possible d'établir les profils de charge d'un ménage. Pour établir un tel profil, le compteur enregistre, tous les quarts d'heure pour l'électricité et toutes les heures pour le gaz naturel, la consommation d'énergie et transmet ces informations dans le système central. Les informations sont ensuite mises à disposition aux gestionnaires de réseaux compétents au moins une fois par jour.

Le recours au « quart-horaire » pour l'électricité et « horaire » pour le gaz naturel est fondé sur les pratiques commerciales présentes au niveau européen entre les gestionnaires de réseaux et les producteurs dans le cadre de leur coopération « ENTSOE[33] ». C'est en effet sur base des cadences « quart horaires » et « horaire » que s'effectuent les achats/ventes en matière d'électricité et de gaz naturel.

De plus, une telle pratique permet aux gestionnaires de réseaux d'effectuer des prévisions statistiques de l'évolution de la charge afin que la production électrique et le stockage du gaz correspondent le plus fidèlement possible aux réels besoins des entreprises et des ménages luxembourgeois. C'est en effet sur base des prévisions statistiques de la veille qu'est définie l'énergie nécessaire pour le lendemain. Cette pratique permet ainsi aux gestionnaires de réseaux de déterminer par zone géographique, la quantité nécessaire d'électricité au quart-heure près et de gaz à l'heure près.

Ces échéances et cadences permettent également d'atteindre les objectifs émis par la Directive européenne 2006/32/CE relative à l'efficacité énergétique dans les utilisations finales et aux services énergétiques qui prévoit plusieurs mesures pour parvenir à une économie d'énergie et à une efficacité énergétique parmi lesquelles *« un meilleur établissement des relevés[34] »* et *« des compteurs individuels qui mesurent avec précision leur consommation effective et qui fournissent des informations sur le moment où l'énergie a été utilisée[35] »*.

Elles permettent également aux gestionnaires de réseaux et aux fournisseurs d'électricité et de gaz naturel de réaliser les tâches qui leur incombent dans les meilleures conditions de coût et de qualité de services vis-à-vis de leurs clients. En effet, pour planifier l'approvisionnement en électricité et offrir des tarifs avantageux, il faut des pronostics de consommation précis car les surcapacités et les sous-capacités

[33] www.entsoe.eu
[34] Article 11.1 de la Directive 2006/32/CE.
[35] Article 13 de la Directive 2006/32/CE.

imprévues sont onéreuses pour les fournisseurs[36].

Au regard des explications susmentionnées, on peut estimer que les valeurs de consommation ou de production enregistrées aux cadences tels que mentionnées dans le projet de règlement sont adéquates, pertinentes et non excessives pour atteindre les finalités mentionnées à l'article 3 du présent projet.

3. L'article 3

La Commission nationale s'étonne que l'article 3 définisse uniquement les finalités pour lesquelles les fournisseurs peuvent traiter les données. En effet, les gestionnaires de réseaux collectent, conservent, et traitent également les données pour des finalités distinctes ou similaires. Par conséquent, faudrait-il à notre avis énumérer également les finalités des traitements effectuées par les gestionnaires de réseaux.

Par ailleurs, le principe de finalité repris à l'article 4 (1) de la loi modifiée du 2 août 2002 impose au responsable du traitement de ne collecter des données que pour des finalités déterminées, explicites et légitimes et de ne traiter les données ainsi collectées que de manière compatible avec ces finalités. Les finalités doivent être clairement définies : *« il ne peut être question d'englober dans une finalité un ensemble d'objectifs flous et trop nombreux[37] ».* De plus, les responsables de traitements sont également tenus d'informer les personnes concernées par la collecte des données des finalités du ou des traitement(s)[38].

Dans le projet de règlement en question, l'article 3 (3) énumère quatre finalités pour lesquelles les fournisseurs sont en droit d'utiliser les données. Toutefois, par l'utilisation du terme « notamment pour », le projet de règlement laisse à penser que d'autres finalités pourraient ultérieurement venir s'ajouter à celles existantes. La Commission nationale souligne que les finalités du traitement des données à caractère personnel doivent être énumérées de manière précise et limitative. En effet, les responsables de traitement doivent traiter les données conformément au but indiqué lors de leur collecte et les données ne peuvent faire l'objet d'un nouveau traitement en vue d'une autre finalité qui est incompatible avec la finalité pour laquelle elles ont été collectées à l'origine[39].

Par ailleurs, il ressort des conversations entretenues avec les différents acteurs du marché que les gestionnaires de réseaux et les fournisseurs souhaitent conserver les données collectées pour les besoins d'éventuels litiges. En effet, ils entendent s'assurer que chaque consommateur a effectivement payé sa consommation et *a contrario*, rechercher les consommateurs dont la consommation n'est pas conforme à la facturation (gestionnaire de réseau de distribution) et ainsi vérifier si des pertes inexplicables se produisent sur le réseau suite à un problème technique, à des activités suspectes ou illégales telles que le vol de courant. La Commission estime qu'il serait nécessaire de l'ajouter aux finalités déjà énumérées à l'article 3 (3).

4. L'article 4

Le projet sous examen entend déterminer la durée de conservation des données de comptage de l'énergie électrique et du gaz naturel à quinze ans aussi bien pour les les gestionnaires de réseaux que pour les fournisseurs d'électricité ou de gaz naturel.

Or, le principe établi par l'article 4 (1) (d) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel limite-t-il la durée de conservation des données à celle nécessaire à la réalisation des finalités pour lesquelles les données ont été collectées. Les responsables de traitements doivent donc définir de manière précise les finalités de leurs traitements pour s'assurer

[36] Préposé fédéral à la protection des données et à la transparence (PFPDT), « L'utilisation de compteurs intelligents », http://www.edoeb.admin.ch/datenschutz/00625/00724/index.html?lang=fr
[37] A . Pipers, « Le respect de la vie privée », Editions Politeia A.s.b.l., Bruxelles, 1995, cité par doc. Parl. 4735, p.30.
[38] Article 26 de la loi du 2 août 2002.
[39] Groupe 29, WP183, « Avis 12/2011 sur les compteurs intelligents ».

que la durée de conservation des données n'excède pas le temps nécessaire à la réalisation d'un objectif licite et bien spécifié.

Afin d'évaluer la durée de conservation des données, la Commission nationale se doit de mettre en balance les intérêts, d'une part, des acteurs du marché de l'énergie et, d'autre part, des personnes concernées par les données collectées. La Commission nationale estime qu'une conservation des données au « quart-horaire » pour l'électricité et « horaire » pour le gaz naturel pour une période de quinze ans permet d'obtenir un profilage extrêmement détaillé des habitudes des individus, de sorte que les intérêts et les droits et libertés de la personne concernée prévalent sur les intérêts des gestionnaires de réseaux et des fournisseurs. De plus, comme la Commission nationale l'a déjà exprimé dans le présent avis, les risques de dérives liés à l'utilisation des données ainsi collectées sont attentatoires à la vie privée des individus, de sorte qu'il y a lieu de réduire le plus possible la durée de conservation des données.

La Commission nationale est donc d'avis que le délai de conservation applicable au marché des télécommunications peut être applicable par analogie au marché de l'énergie. L'article 5 (3) de la loi modifiée du 30 mai 2005 relatives aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électronique dispose que « *les données relatives au trafic qui sont nécessaire en vue d'établir les factures des abonnées et aux fins des paiements d'interconnexion peuvent être traitées. Un tel traitement n'est possible que jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement et ne peut en tout état de cause dépasser 6 mois lorsque la facture a été payée et n'a pas fait l'objet de litige ou de contestation* ». En d'autres termes, la Commission nationale est d'avis que les gestionnaires de réseaux ainsi que les fournisseurs doivent conserver les données de comptage « quart-horaire » pour l'électricité et « horaire » pour le gaz naturel pendant une période de 6 mois lorsque la facture a été payée et n'a pas fait l'objet de litige ou de contestation. Les données de comptage doivent ensuite être agrégées afin de conserver une unique donnée de comptage par mois, et ce pendant une période de cinq ans. En effet, la prescription quinquennale prévue à l'article 2277 du code civil s'applique aux créances d'électricité.

Ainsi décidé à Esch-sur-Alzette en date du 13 décembre 2013.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

Avis relatif au règlement interne du Registre National du Cancer

Délibération n°606/2013 du 23 décembre 2013

Conformément à l'article 2 paragraphe (3) du règlement grand-ducal du 18 avril 2013 déterminant les modalités et conditions de fonctionnement du registre national du cancer, le règlement interne, qui contiendra outre la charte de sécurité, aussi les modalités de contrôle qualité à opérer et les modalités relatives à la publication des résultats est soumis pour approbation au ministre ensemble avec la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale »)

Par courrier du 14 octobre 2013, le Centre de recherche public de la santé (ci-après désigné CRP-Santé), a invité la Commission nationale à se prononcer au sujet des documents concernant le règlement interne du Registre National du Cancer. Le règlement interne, tel que soumis à la Commission nationale, est composé du document du règlement interne (version du 9 octobre 2013), de la charte de sécurité des systèmes d'information (version du 9 octobre 2013), du manuel qualité (version du 25 juillet 2013), de la procédure de diffusion des résultats (version du 9 octobre 2013) et de la brochure d'information des patients.

- Concernant le document de la charte de sécurité, la Commission nationale formule les suggestions suivantes :

1) Au chapitre 3 section « 3.2 Engagements des collaborateurs », il est précisé que « *Lors de son engagement en tant que collaborateur au sein du RNC, il bénéficie de la part du responsable opérationnel du RNC d'une formation, entre autre relative à la sécurité des données, au respect de la confidentialité, au devoir de protection des données à caractère personnel des patients et des sources, et aux procédures inhérentes à ces aspects.* ». La Commission nationale suggère d'étendre cette activité par la mise en place d'une formation continue relative à la sécurité suivant un cycle au minimum annuel. Les risques évoluent et les procédures sont changées pour s'adapter à l'évolution de l'environnement. Le feedback des collaborateurs par rapports aux risques de sécurité et la mise en application de ces procédures peuvent apporter des éléments pertinents quant à la gestion de la sécurité du système d'information. Dans

ce contexte, la Commission nationale propose d'organiser une formation mise à jour, au minimum annuellement, relative à la sécurité propre à l'environnement en question.

2) Au chapitre 4 section « II.2. Utilisation professionnelle / privée », il est indiqué que « *L'utilisation résiduelle du système d'information du RNC à titre privé est strictement interdite* ». Il est quasiment inévitable qu'un utilisateur accède à un moment ou à un autre à des sites Internet non professionnels, communique par email avec des correspondants personnels ou effectue une tâche privée avec son PC. De plus, il est de jurisprudence constante que le salarié a droit, dans une certaine mesure, même au temps et au lieu de travail, au respect de sa vie privée, ce qui ne permet pas à l'employeur d'appliquer une restriction totale quant à l'utilisation raisonnable d'un système d'information à titre privé. A ce titre, la Commission nationale recommande de mettre en place des « bornes Internet », séparées du système d'information du RNC, destinées à un usage privé (ex : utilisation de webmails privés, consultation de sites Internet non professionnels) et d'associer à cette activité une charte d'utilisation des bornes Internet.

De manière générale, la CNPD estime nécessaire d'isoler le système d'information propre au registre national du cancer de toutes autres activités nécessitant l'utilisation d'un système d'information (navigation Internet, email, gestion administrative,…)

3) Le chapitre 4 section « II.4.2 Respect des engagements de la CNPD », précise que « *Le CRP-Santé et ses partenaires s'engagent à respecter les dispositions présentées et validées par la CNPD pendant toute la durée d'exploitation du RNC* ». La Commission nationale suggère de retirer ce texte qui par l'expression « dispositions présentées et validées par la CNPD » ne permet pas de déterminer quelles sont les dispositions concernées et peuvent prêter à confusion quant à l'application de la législation sur la protection des données à caractère personnel. En effet, cette dernière est applicable dans son ensemble sous la responsabilité du CRP-Santé (accountability).

4) Le chapitre 4, article III, section « III.1. Règles de sécurité applicables » a trait, entre autres, à la gestion des mots de passes.

a. Concernant le point « *Le choix d'un mot de passe non trivial* », nous proposons de mettre en place une politique de construction de mots de passe forcée techniquement, afin que les utilisateurs soient contraints d'utiliser des mots de passe avec le niveau de complexité requis.

b. Il convient de souligner qu'au regard de la sensibilité des données traitées et du caractère national du registre, la sécurité des accès à la base de données du RNC basée uniquement sur la combinaison nom d'utilisateur / mot de passe n'est pas d'un niveau de sécurité suffisant, même si le mot de passe diffère pour l'accès à la base de données du RNC du mot de passe d'accès au terminal de l'utilisateur. Dans ce contexte la CNPD exige la mise en œuvre d'une authentification forte pour l'accès à la base de données du RNC.

En effet, depuis la survenance de l'incident dit « Medicoleak » au début de l'année 2012, le Cyber Security Board (mis en place par le gouvernement en juillet 2011) a renforcé ses efforts en vue de la mise en œuvre progressive de la politique du gouvernement en matière de cyber sécurité auprès des organismes publics qui gèrent des fichiers contenant des données sensibles. A cet effet, le Cyber Security Board s'est prononcé « *pour une généralisation obligatoire du système de l'authentification forte pour les applications sensibles notamment via l'application LUXTRUST* ». Ainsi, au fur et mesure de leur identification, les bases de données « sensibles », gérées par les administrations et établissements publics, devront obligatoirement être équipées d'une authentification forte Luxtrust.

De l'avis de la CNPD ceci devra évidemment aussi être le cas pour une base de données aussi sensible que le Registre National du Cancer dont la gestion est assurée par le Centre de Recherche Public de la Santé.

Dans cette même section, la charte de sécurité énumère un certain nombre de règles élémentaires à appliquer par le collaborateur, « *De la part du collaborateur* », pour lesquelles la Commission nationale suggère d'appliquer les mesures suivantes :

c. « *ne pas connecter aux réseaux locaux des équipements non autorisés par le CRP-Santé ou son établissement* » : nous conseillons la mise œuvre de blocages techniques pour appliquer cette mesure et ne pas en laisser le contrôle uniquement aux utilisateurs.

d. « *ne pas déposer les données relatives aux RNC…* » : la CNPD suggère de ne pas laisser aux utilisateurs la possibilité d'évaluer eux-mêmes les conséquences de tels actes. A cet effet, nous conseillons de définir une procédure précise, comprenant les instructions d'acceptation des cas où les données professionnelles peuvent être déposées en dehors du système d'information du Registre National du Cancer. Cette procédure pourra se référer au document de « Procédure de diffusion des résultats », mais elle devrait également prendre en compte les activités quotidiennes des collaborateurs pour lesquelles une exportation des données entre ligne de compte (exemples : stockage intermédiaire de données, données nécessaires pour une activité exceptionnelle ou liée à l'administration quotidienne.

e. « *assurer la protection des informations sensibles du RNC et ne pas les transporter sans protection …* » : Comme pour le point « c » ci-avant, la Commission

nationale conseille l'implémentation d'un outil qui permet le contrôle des supports mobiles (contrôle de l'utilisation et obligation du chiffrement de ces supports). Cet outil devra également être en mesure de forcer techniquement l'application de cette règle.

f. *« ne pas quitter son poste de travail… sans se déconnecter ou verrouiller sa session par un mot de passe »* : la Commission nationale recommande d'ajouter la mise en œuvre d'un blocage automatique de la station après quelques minutes d'inactivité.

5) Au chapitre 4, article III, section « III.2 Devoirs de signalement et d'information », la charte de sécurité indique que le *« collaborateur doit avertir le CRP-Santé dans les meilleurs délais en cas de découverte d'une anomalie affectant le système d'information »*. A cet effet, la CNPD propose d'indiquer aux collaborateurs un point de contact unique (SPOC – Single Point Of Contact) auquel les collaborateurs peuvent s'adresser en cas de suspicions d'incident ou d'incident avéré. Dans la continuité de ce processus, nous conseillons fortement de créer et d'implémenter une procédure de gestion des incidents dans laquelle sont, entre autres, définis les rôles et responsabilités de chacun, les flux de communication et les pouvoirs décisionnels en cas de survenance d'un incident.

6) Dans le chapitre 4, article IX « Transmission des données électroniques vers le RNC », la Commission nationale voudrait relever une erreur de syntaxe dans l'expression *« modèle de cryption par clé asymétrique »* et suggère de remplacer cette expression par « modèle de chiffrement asymétrique »

7) Dans le chapitre 4, article XII « Réalisation d'un audit de sécurité », concernant le point *« un audit externe commandité à une société indépendante qualifiée en sécurité informatique »*, il conviendrait de remplacer le terme « sécurité informatique » par « sécurité de l'information ». L'objectif étant d'éviter que ces audits externes ne soient purement techniques, mais prennent également en compte les aspects organisationnels de gestion de la sécurité de l'information.

8) La Commission nationale souhaite également relever les points suivants pouvant être ajoutés à la charte de sécurité :

a. Nous conseillons d'intégrer une section relative à l'utilisation du téléphone et d'indiquer aux collaborateurs les règles de divulgations et de collectes d'information par téléphone.

b. La même remarque vaut pour les communications liées à l'utilisation des courriels.

c. Finalement, nous suggérons également d'insérer une section sur la mise en œuvre de mesures relatives à la continuité de service et la récupération de production (BCP / DRP).

- Concernant le document de « Convention de transfert de données », la Commission nationale émet les remarques suivantes :

En ce qui concerne l'article 11 section 11.2 « Incidents », nous renvoyons aux recommandations du point 5) de la section précédente en mettant en œuvre une procédure commune de gestion des incidents.

- Concernant le formulaire de refus du patient :

La CNPD estime important et nécessaire de rajouter au formulaire de refus du patient une phrase qui informe le patient que son opposition au traitement de ses données n'entraîne aucun préjudice pour lui et ne porte pas atteinte à son droit à recevoir des soins de santé appropriés, conformément à l'article 4 paragraphe (1) 2ème alinéa du règlement grand-ducal du 18 avril 2013 déterminant les modalités et conditions de fonctionnement du registre national du cancer.

Ainsi décidé à Esch-sur-Alzette en date du 23 décembre 2013.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

7 Annexes

Participations aux travaux européens

Documents adoptés par le groupe de travail « Article 29 » en 2013

Document	Date d'adoption	Référence
Programme de travail 2014-2015	03.12.2013	WP 210
Avis 07/2013 sur le modèle d'analyse d'impact relative à la protection des données pour les réseaux intelligents et les systèmes de relevés intelligents (modèle d'AIPD) élaboré par le groupe d'experts 2 de la task-force sur les réseaux intelligents de la Commission	04.12.2013	WP 209
Document de travail 02/2013 énonçant des lignes directrices sur le recueil du consentement pour le dépôt de cookies	02.10.2013	WP 208
Avis 6/2013 sur la réutilisation des informations du secteur public (ISP) et des données ouvertes	05.06.2013	WP 207
Avis 05/2013 sur les frontières intelligentes	06.06.2013	WP 206
Avis 04/03 sur le modèle d'analyse d'impact relative à la protection des données pour les réseaux intelligents et les systèmes de relevés intelligents (modèle d'AIPD) élaboré par le groupe d'experts 2 de la task-force sur les réseaux intelligents de la Commission	22.04.2013	WP 205
Document explicatif sur les règles d'entreprise contraignantes applicables aux sous-traitants	19.04.2013	WP 204
Avis 03/2013 sur la notion de limitation de la finalité	02.04.2013	WP 203
Avis 02/2013 sur les applications destinées aux dispositifs intelligents	27.02.2013	WP 202
Avis 01/2013 apportant une contribution supplémentaire aux discussions sur la proposition de directive relative à la protection des données traitées dans les domaines de la police et de la justice pénale	26.02.2013	WP 201
Document de travail 01/2013 : Contribution au débat sur les propositions d'actes d'exécution	22.01.2013	WP 200

Groupe de travail « Article 29 » – Document de travail 02/2013 énonçant des lignes directrices sur le recueil du consentement pour le dépôt de cookies

Adopté le 2 octobre 2013

Depuis l'adoption, en 2009, du texte portant modification de la directive « vie privée et communications électroniques » 2002/58/CE, transposé dans l'ensemble des Etats membres de l'UE[40], les sites web ont élaboré une série d'applications pratiques afin de recueillir le consentement pour l'utilisation de cookies[41] ou de technologies de traçage similaires (ci-après dénommés « cookies ») employés à des fins diverses (telles l'amélioration des fonctionnalités, l'analytique, la publicité ciblée et l'optimisation des produits, etc.) par les opérateurs de sites web ou des tiers. L'éventail de mécanismes de consentement déployés par les opérateurs de sites web témoigne de la diversité des organisations et des catégories de public auquel ils s'adressent.

Il est loisible à l'opérateur du site d'utiliser différents moyens pour obtenir un consentement, pour autant que celui-ci puisse être réputé valable au titre de la législation de l'UE. Le groupe de travail examine par la suite dans le présent avis si une solution particulière mise en œuvre par l'opérateur du site web satisfait ou non à toutes les conditions de validité du consentement.

Bien que la directive « vie privée et communications électroniques » prévoie l'exigence d'un consentement pour stocker des cookies ou pour y avoir accès, la mise en œuvre pratique des obligations juridiques varie d'un opérateur de site web à l'autre dans l'ensemble des Etats membres de l'Union. Les expériences actuellement observées à cet égard reposent sur une ou plusieurs des pratiques suivantes, bien qu'il importe de relever que, même si chacune d'elles peut être un élément utile d'un mécanisme de consentement, il est improbable que le recours à une pratique isolée suffise à fournir un consentement valable, puisque tous les éléments d'un tel consentement doivent être réunis (par exemple, un mécanisme de choix effectif nécessite également d'adresser un avertissement et des informations) :

- un avertissement immédiatement visible informant que différents types de cookies[42] sont utilisés par le site web consulté et communiquant des informations selon une approche par étape, habituellement via un lien ou une série de liens, donnant à l'utilisateur davantage d'informations sur les types de cookies utilisés,
- un avertissement immédiatement visible selon lequel, en utilisant le site web, l'utilisateur consent à ce que des cookies soient installés par ce site,
- des informations aux utilisateurs sur les modalités de manifester leur volonté, puis de la retirer, en ce qui concerne les cookies, y compris des informations sur la manipulation requise pour exprimer une telle préférence,
- un mécanisme par lequel l'utilisateur peut choisir d'accepter tous les cookies ou certains d'entre eux ou de les refuser,
- une option offerte à l'utilisateur de modifier ultérieurement une préférence préalablement définie en matière de cookies.

Compte tenu des interprétations différentes dont fait l'objet la directive « vie privée et communications électroniques » parmi les parties prenantes et des modalités respectives de mise en œuvre dudit texte, la question suivante se pose: quelle mise en œuvre serait juridiquement conforme pour un site web qui est exploité dans tous les Etats membres de l'Union ?

L'article 2, point f), et le considérant 17 de la directive 2002/58/CE définissent la notion de consentement par référence à celle énoncée dans la directive 95/46/CE. L'article 2, point h), de la directive

[40] Depuis janvier 2013.
[41] Ainsi que l'a décrit le groupe de travail dans son avis n°04/2012, le terme « cookie » recouvre des technologies certes diverses mais axées sur le cookie HTTP.
[42] Par exemple, les cookies de modules sociaux de pistage, la publicité de tiers ou l'analytique, mentionnés dans l'avis sur l'exemption de l'obligation de consentement pour certains cookies.

95/46/CE dispose ainsi que le consentement de la personne concernée au traitement de données à caractère personnel la concernant devrait être une manifestation de volonté, libre, spécifique et informée par laquelle cette personne accepte que ces données fassent l'objet d'un traitement. Conformément à l'article 7 de la directive 95/46/CE, il convient que le consentement soit également indubitable.

Dans son avis sur la définition du consentement[43], le groupe de travail admet les différences que la notion de consentement peut présenter entre les Etats membres. Ledit avis clarifie davantage les conditions de validité du consentement et les principales caractéristiques de celui-ci :

1. ***Informations spécifiques.*** Pour être valable, le consentement doit être **spécifique** et fondé sur des **informations appropriées**. En d'autres termes, un consentement général, sans préciser la finalité exacte du traitement, n'est pas acceptable.

2. ***Moment où le consentement est donné.*** De manière générale, le consentement doit être exprimé **avant le début du traitement**.

3. ***Choix actif.*** Le consentement doit être **indubitable**. Dès lors, la procédure relative à l'obtention et à l'octroi du consentement ne doit laisser **aucun doute quant à l'intention de la personne concernée**. En principe, il n'existe pas de limitations quant à la forme que peut revêtir un consentement. Toutefois, pour être valable, le consentement doit consister en **une manifestation active de la volonté de l'utilisateur**. L'expression minimale d'une manifestation de volonté pourrait être tout type de signe, suffisamment clair pour permettre d'exprimer la volonté d'une personne concernée et être compris par le responsable du traitement (cela pourrait inclure une signature manuscrite apposée au bas d'un formulaire papier ou un comportement dont on peut raisonnablement déduire un accord)[44].

4. ***Libre manifestation de volonté.*** Le consentement ne peut être valable que si la personne concernée est **véritablement en mesure d'exercer un choix** et s'il n'y a pas de risque de tromperie, d'intimidation, de coercition ou de conséquences négatives importantes si elle ne donne pas son consentement.

Dans la droite ligne des clarifications exposées ci-dessus et dans d'autres avis[45] sur la définition du consentement

[43] Avis n°15/2011 sur la définition du consentement.
[44] De même, la proposition de texte du futur règlement de l'Union relatif à la protection des données désigne le consentement comme étant signifié par un « acte positif univoque ».
[45] Clarifications apportées dans l'avis n°2/2010 sur la publicité comportementale en ligne.

valable dans tous les Etats membres de l'UE, le groupe de travail explique que, si l'opérateur d'un site web souhaitait faire en sorte qu'un mécanisme de consentement de cookies satisfasse aux conditions posées dans chaque État membre, ce mécanisme devrait présenter chacune des principales caractéristiques suivantes : **informations spécifiques, consentement préalable, manifestation de volonté exprimée par le comportement actif de l'utilisateur et capacité de choisir librement.**

1. Informations spécifiques

Le mécanisme devrait prévoir un avertissement clair, complet et visible relatif à l'utilisation de cookies, au moment et à l'endroit où le consentement est demandé, par exemple, sur la page web sur laquelle un utilisateur démarre une session de navigation (page d'entrée). Lorsqu'ils accèdent au site web, les utilisateurs doivent être en mesure d'avoir accès à toutes les informations nécessaires relatives aux différents types de cookies utilisés par le site web ou aux différentes finalités que ces derniers poursuivent. Le site web pourrait afficher de façon visible un lien vers une zone désignée dans laquelle sont présentés tous les types de cookies qu'il utilise. Les informations nécessaires concerneraient la ou les finalités des cookies et, si cela est pertinent, il serait mentionné que des cookies peuvent provenir de tiers ou résulter de l'accès de tiers aux données recueillies par les cookies utilisés sur le site web. Aux fins de l'information complète des utilisateurs, il conviendrait également de faire figurer des informations telles que la durée de conservation (c'est-à-dire la date d'expiration des cookies), des valeurs types, des éléments détaillés sur les cookies de tiers et d'autres informations techniques. Les utilisateurs doivent également être informés des modalités d'expression de leur volonté à propos des cookies, c'est-à-dire comment ils peuvent tous les accepter, n'en accepter que certains ou aucun et comment ils peuvent, à l'avenir, modifier cette préférence.

2. Moment où le consentement est donné

Ainsi que le groupe de travail l'a conclu dans l'avis susmentionné[46], le consentement doit être donné avant le début du traitement des données. Ledit avis précise que cette exigence s'applique également dans le cadre de l'article 5, paragraphe 3, de la directive « vie privée et communications électroniques ». En conséquence, aux fins de conformité dans tous les Etats membres de l'Union, il conviendrait de solliciter le consentement avant l'installation ou la lecture des cookies. Un site web devrait, dès lors, offrir une solution en matière de consentement, d'après laquelle aucun cookie n'est installé sur l'appareil de l'utilisateur (autres que ceux pour lesquels son consentement peut ne pas être exigé[47]) tant que l'utilisateur n'a pas manifesté sa volonté à propos de ces cookies.

3. Comportement actif

Le site web doit, outre les informations relatives aux types de cookies et à la finalité de ces derniers, également présenter des informations claires et complètes aux utilisateurs sur les modalités d'expression de leur consentement, informations qui figurent très probablement sur la page à partir de laquelle les utilisateurs commencent leur session de navigation.

Les outils permettant d'obtenir ce consentement peuvent inclure écrans de démarrage, bandeaux, fenêtres de dialogue modales ou encore paramètres de navigation, etc. En ce qui concerne ces derniers, le considérant 66 de la directive 2009/136/CE précise que, « lorsque cela est techniquement possible et effectif, conformément aux dispositions pertinentes de la directive 95/46/CE, l'accord de l'utilisateur en ce qui concerne le traitement peut être exprimé par l'utilisation des paramètres appropriés d'un navigateur

[46] Avis n°15/2011 sur la définition du consentement.
[47] Pour des développements plus circonstanciés sur les exemptions, voir l'avis sur l'exemption de l'obligation de consentement pour certains cookies.

ou d'une autre application ». Lorsque l'opérateur d'un site web peut avoir la certitude que l'utilisateur a été pleinement informé et qu'il a activement configuré son navigateur ou une autre application alors, si les circonstances s'y prêtent, cette configuration indiquerait un comportement actif et serait, dès lors, respectée par l'opérateur du site web. Les conditions selon lesquelles les paramètres de navigation peuvent exprimer un consentement valable et effectif sont décrites dans l'avis n°2/2010 élaboré par le groupe de travail.

Le processus par lequel les utilisateurs pourraient consentir à des cookies consisterait pour ces personnes à adopter un acte positif ou un autre comportement actif, pour autant qu'ils aient été pleinement informés de ce que cet acte représente. Dès lors, les utilisateurs peuvent exprimer leur consentement en cliquant sur un bouton ou sur un lien ou en cochant une case dans ou à proximité de la zone dans laquelle les informations sont présentées (si l'acte est effectué de manière concomitante à la fourniture d'informations sur l'utilisation de cookies) ou par tout autre comportement actif dont l'opérateur d'un site web peut conclure indubitablement qu'il est synonyme d'un consentement spécifique et informé.

Aux fins du présent document, on entend par comportement actif un acte que l'utilisateur peut accomplir, le plus souvent un acte fondé sur une demande traçable émanant de l'utilisateur-client adressée au site web, tel que le fait de cliquer sur un lien, une image ou un autre contenu figurant sur la page d'entrée du site, etc. La forme de ces types de demandes émanant de l'utilisateur est de nature à donner à l'opérateur du site la certitude que l'utilisateur a activement demandé à nouer un dialogue avec le site web et (à supposer que l'utilisateur soit pleinement informé) qu'il consent donc effectivement aux cookies, et que l'acte constitue une manifestation active de ce consentement. En tout état de cause, les actes qui exprimeront le consentement à des cookies doivent être clairement présentés à l'utilisateur. Il faut s'assurer que le choix exprimé par un comportement actif repose effectivement sur l'information claire que des cookies seront installés à la suite de cet acte. Les informations devraient être exposées de manière à ce que l'utilisateur ait de fortes chances de les reconnaître en tant que telles (et ne les confonde pas avec de la publicité, par exemple). Il est, dès lors, essentiel de faire en sorte que le bouton, le lien ou la case qui manifeste le comportement actif se trouve dans ou à proximité de la zone

dans laquelle les informations sont présentées, pour avoir la certitude que l'utilisateur peut rapporter son acte aux informations qui s'affichent. En outre, ces informations devraient être visibles sur le site web et le rester tant que l'utilisateur n'a pas exprimé son consentement. Dans ce dernier cas, l'opérateur du site web peut avoir la garantie d'avoir reçu un consentement indubitable. De plus, un seul clic sur un lien permettant d'«en savoir plus sur les cookies» ne saurait suffire à valoir consentement parce que l'utilisateur s'est expressément limité à demander un complément d'informations. L'absence de tout comportement ne saurait non plus être considérée comme un consentement valable.

Si l'utilisateur accède au site web sur lequel lui ont été communiquées des informations relatives à l'utilisation de cookies et s'il n'adopte pas de comportement actif, tel que décrit ci-dessus, mais reste au contraire sur la page d'entrée sans agir davantage, il est difficile de soutenir qu'un consentement a été indubitablement donné. L'acte de l'utilisateur doit être de nature telle que, considéré conjointement avec les informations fournies sur l'utilisation de cookies, il peut être raisonnablement interprété comme une manifestation de la volonté de l'utilisateur.

4. Choix véritable - consentement donné librement

Le mécanisme de consentement devrait offrir à l'utilisateur un choix véritable et sérieux en matière de cookies sur la page d'entrée. L'utilisateur devrait avoir la possibilité de choisir librement entre, d'une part, la possibilité d'accepter certains ou tous les cookies ou de les refuser tous ou certains d'entre eux et, d'autre part, de conserver la possibilité de modifier à l'avenir les paramètres définis en la matière.

Dans quelques Etats membres, l'accès à certains sites web peut être subordonné à l'acceptation de cookies[48] ; de manière générale, toutefois, l'utilisateur devrait conserver la possibilité de continuer à naviguer sur le site web sans recevoir de cookies ou en n'en recevant que quelques-uns, à savoir : ceux pour lesquels il a donné son consentement qui sont nécessaires au regard de la finalité pour laquelle le service est fourni sur le site concerné, et ceux qui sont exemptés de l'obligation de consentement. Il est, dès lors, recommandé de s'abstenir d'utiliser des mécanismes de consentement qui n'offrent à l'utilisateur que la possibilité de donner son consentement mais qui ne proposent aucun choix en ce qui concerne l'ensemble des cookies ou certains d'entre eux. Il est vivement recommandé d'égrener les options dont dispose l'utilisateur.

L'argumentation développée ci-dessus repose sur le considérant 25 de la directive « vie privée et communications électroniques » 2002/58/CE, selon lequel l'accès au contenu d'un site spécifique peut être subordonné au fait d'accepter, en pleine connaissance de cause, l'installation d'un témoin de connexion ou d'un dispositif analogue, si celui-ci est utilisé à des fins légitimes. Par l'accent mis sur le « contenu d'un site spécifique », il est explicité que les sites web ne devraient pas subordonner « l'accès général » au site à l'acceptation, par un utilisateur, de tous les cookies et qu'ils ne peuvent limiter que certains contenus si l'utilisateur ne donne pas son consentement pour les cookies (par exemple, pour des sites de vente en ligne dont la finalité première est de vendre des articles, le refus des cookies (non fonctionnels) ne devrait pas empêcher un utilisateur d'acheter des produits sur ces sites web).

En outre, le considérant 10 de la directive « vie privée et communications électroniques » 2002/58/CE précise que, dans le secteur réglementé par ladite directive, la directive 95/46/CE est applicable notamment à tous les aspects de la protection des droits et libertés fondamentaux

[48] La législation suédoise permet aux sites web de n'autoriser un utilisateur à accéder à leur site que s'il donne son consentement à l'utilisation de cookies. Une personne concernée qui ne donne pas son consentement devra alors choisir un prestataire de services différent. Il est dérogé à cette règle en faveur des sites web qui fournissent certains services relevant du secteur public, sur lesquels l'utilisateur pourrait être considéré comme ayant peu de possibilités, voire comme n'ayant pas d'autre possibilité que de recourir à ce service, partant comme n'étant pas véritablement en mesure d'exercer un autre choix pour ce qui est de l'usage de cookies.

qui n'entrent pas expressément dans le cadre de la directive 2002/58/CE, y compris les obligations auxquelles est soumis le responsable du traitement des données à caractère personnel et les droits individuels.
La directive 95/46/CE est donc applicable à tous les responsables de traitement de données. Puisque le stockage d'informations ou l'obtention, au moyen de cookies, des informations déjà stockées sur les appareils des utilisateurs peut aller de pair avec le traitement de données à caractère personnel[49], dans ce cas, les règles relatives à la protection des donnés sont manifestement applicables. L'un des principes qu'il convient de prendre en considération est que les données traitées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement [article 6, paragraphe 1, point c)]. Si certains cookies ne sont, dès lors, pas nécessaires au regard de la finalité de la fourniture du service par le site web, mais se bornent à offrir des avantages supplémentaires à l'opérateur du site web, l'utilisateur devrait se voir offrir un choix véritable en ce qui concerne ces cookies.

Les types de cookies susceptibles d'être disproportionnés au regard de la finalité du site web peuvent varier en fonction du contexte. Un exemple dans lequel il serait considéré comme disproportionné de solliciter le consentement pour des cookies superflus sont les sites web offrant certains services, dont on peut considérer que l'utilisateur n'a que peu de possibilités, voire n'a pas d'autre possibilité que d'utiliser ces services, de sorte qu'il n'est pas véritablement en mesure d'exercer un choix quant à l'usage de cookies. Dans la plupart des Etats membres de l'UE, cela s'applique particulièrement aux services du secteur public[50].

Les utilisateurs devraient aussi être véritablement en mesure d'exercer un choix en matière de cookies traceurs. Des cookies de ce type sont habituellement utilisés pour suivre le comportement de personnes physiques sur plusieurs sites web, créer des profils sur la base de ce comportement, en déduire leurs intérêts et prendre des décisions touchant les personnes individuellement. Lorsque des cookies traceurs sont utilisés pour repérer des personnes physiques de cette façon, il s'agit vraisemblablement de cookies contenant des données à caractère personnel. En ce qui concerne le traitement des données à caractère personnel qui accompagne la lecture et l'installation de cookies traceurs, le responsable du traitement doit obtenir le consentement indubitable de l'utilisateur. Une

[49] Ainsi que le groupe de travail l'a également précisé dans l'avis n°2/2010 sur la publicité comportementale en ligne.
[50] Dans la grande majorité des Etats membres de l'UE, il n'est pas légal de rendre conditionnel l'accès à des sites web de service public.

décision constatant une violation du principe susmentionné serait adoptée au cas par cas par l'autorité nationale compétente pour surveiller le respect de la disposition pertinente de la législation relative à la protection des données.

Fait à Bruxelles,
le 2 octobre 2013.

Pour le groupe de travail

Le président
Jacob Kohnstamm

Groupe de travail « Article 29 » – Avis 01/2013 apportant une contribution supplémentaire aux discussions sur la proposition de directive relative à la protection des données traitées dans les domaines de la police et de la justice pénale

Adopté le 26 février 2013

1. Introduction

Le 25 janvier 2012, la Commission européenne a adopté une proposition de *directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données* (ci-après, la « directive relative à la protection des données traitées dans les domaines de la police et de la justice pénale » ou la « directive »). Cette proposition a été présentée parallèlement au règlement général sur la protection des données. Tant le Conseil que le Parlement européen ont ensuite lancé leurs procédures législatives respectives pour les deux instruments, en vue d'obtenir un accord sur l'intégralité du paquet avant les élections européennes de 2014. Cependant, le débat législatif sur la directive progresse lentement.

Le groupe de travail « Article 29 » a transmis sa première réaction générale à la proposition de la Commission dans son avis du 23 mars 2012, dans lequel il soulignait les points qu'il estimait préoccupants et faisait des suggestions d'améliorations.

Le groupe se félicite de l'approche globale (« paquet ») adoptée par les rapporteurs du Parlement européen dans leurs projets de rapports destinés à la commission LIBE. Il est convaincu que tous les groupes politiques continueront à tenir dûment compte de tous les éléments du paquet et à veiller à la cohérence absolument nécessaire entre les deux propositions afin de les améliorer encore. Le groupe se félicite également de l'intensification du débat législatif au Conseil, à l'instigation des présidences chypriote et irlandaise.

Après avoir adopté le 5 octobre 2012 son premier avis apportant une nouvelle contribution aux discussions sur le règlement, le groupe formule dans le présent avis d'autres orientations relatives à plusieurs éléments particuliers de la directive proposée sur la protection des données traitées dans les domaines de la police et de la justice pénale. Bien que d'autres

questions puissent encore être examinées, le groupe a décidé, vu l'état d'avancement des négociations, de se concentrer sur quatre éléments actuellement considérés comme les plus importants. Il s'agit de l'utilisation des données concernant des personnes non suspectes, des droits des personnes concernées, de l'utilisation des analyses d'impact sur la vie privée et des pouvoirs des autorités chargées de la protection des données, notamment en ce qui concerne les informations confidentielles ou classifiées.

2. L'utilisation des données concernant des personnes non suspectes

L'article 5 de la proposition de directive fait obligation au responsable du traitement d'établir une distinction claire entre les données à caractère personnel concernant différentes catégories de personnes et définit cinq catégories de personnes concernées. Le considérant 23 indique que cette distinction découle nécessairement du traitement des données à caractère personnel dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière. Le groupe souligne que cette distinction est également indispensable pour garantir la bonne application des principes relatifs au traitement des données à caractère personnel définis à l'article 4.

L'article 5 établit une distinction entre plusieurs catégories de personnes ayant un lien direct ou un lien indirect (éventuel) avec une infraction pénale particulière ou des suspects [catégories a) à d), les autres personnes constituant la catégorie e)]. Compte tenu de la description donnée du lien qu'ont les personnes visées aux points a) à d) avec une infraction pénale ou une enquête, il est manifeste que les personnes relevant de la catégorie e) peuvent être qualifiées de personnes n'ayant aucun lien connu avec une infraction ou des suspects, lien mentionné pour les autres catégories.

C'est précisément à l'égard de ce groupe de personnes que les autorités européennes chargées de la protection des données ont souligné, en 2005[51] déjà, qu'il y avait lieu de faire une distinction entre le traitement de données à caractère personnel concernant des personnes non suspectes et le traitement des données relatives à des personnes liées à une infraction particulière. Le traitement de données concernant des personnes non soupçonnées d'avoir commis une infraction pénale (autres que les victimes, témoins, informateurs, contacts et complices) « ne devrait être autorisé que dans certaines

[51] Document de synthèse sur les services répressifs et l'échange d'informations dans l'UE, adopté par la Conférence de printemps des autorités européennes de protection des données, Cracovie (Pologne), 25-26 avril 2005.

conditions spécifiques et pour autant qu'il soit absolument nécessaire à une finalité légitime, clairement définie et particulière ». Par ailleurs, ce traitement devrait (de l'avis des autorités de protection des données) « être limité à une période déterminée et l'utilisation ultérieure de ces données à d'autres fins devrait être interdite ». Parallèlement, la directive devrait préciser que des restrictions et des garanties supplémentaires s'appliquent aux victimes et autres tiers, visés à l'article 5, paragraphe 1, point c), de la proposition actuelle. La législation doit reconnaître qu'il y a lieu de distinguer entre le traitement de données à caractère personnel concernant des personnes déclarées coupables d'infractions pénales et celui de données relatives à des victimes de telles infractions, en particulier dans les bases de données créées à des fins préventives ou pour faciliter les poursuites à l'encontre des auteurs de futures infractions.

L'évolution des techniques et méthodes répressives au cours de la dernière décennie indique clairement que tous les groupes de personnes relevant de la catégorie générale des « personnes non suspectes » doivent bénéficier d'une protection particulière. Cela est d'autant plus vrai lorsque le traitement n'est pas effectué dans le cadre d'une enquête ou de poursuites pénales particulières. La question qui se pose est celle de la distinction entre les informations que les services répressifs « doivent connaître » et les informations « souhaitables ».

Pour protéger les personnes non suspectes, le groupe recommande vivement qu'un nouvel article *7 bis* soit inséré, en complément de l'article 5. Ce nouvel article *7 bis*, dont le libellé est proposé ci-dessous, garantirait que la différenciation des catégories de données ne représente pas une charge administrative et ne constitue pas une fin en soi, comme la proposition actuelle semble le laisser entendre. Il y a lieu de faire en sorte que les Etats membres ne puissent procéder au traitement de données relatives à des personnes non suspectes que si certaines conditions sont remplies et qu'une protection supplémentaire est exigée lorsque de telles données sont soumises à un traitement. Par conséquent, il est plus pertinent d'insérer une nouvelle disposition dans le contexte de l'article *7* qui régit la licéité des traitements. Le groupe est conscient de la nature particulière des traitements de données effectués dans un contexte répressif et comprend que le traitement de données concernant des personnes non suspectes peut se révéler nécessaire dans certains cas.

La proposition tient également compte des divers motifs pour lesquels les services répressifs peuvent traiter les données de personnes non suspectes et propose notamment des règles strictes applicables aux cas dans lesquels le traitement ne sert pas à une enquête ou à des poursuites particulières. Il s'agit des cas dans lesquels des données concernant des personnes non suspectes ne peuvent être traitées que si leur traitement est indispensable dans un but légitime, clairement défini et spécifique, se borne à apprécier la pertinence des données pour l'une des catégories indiquées à l'article *7 bis*, paragraphe 1, points a) à d), et est limité à une période déterminée, l'utilisation ultérieure de ces données étant interdite. Afin d'éviter les discussions sémantiques sur la distinction entre « nécessaire » (employé dans la proposition de directive et « absolument nécessaire » (employé dans le document de synthèse établi à Cracovie), le groupe a utilisé l'adjectif « indispensable » dans sa proposition d'amendement. Le libellé de la disposition vise à prendre en compte la nécessité de subordonner à une condition plus stricte le traitement des données concernant une personne non suspecte en raison de l'absence de lien, direct ou indirect, entre cette personne et une enquête ou une infraction pénale spécifiques.

Annexes

Amendement proposé relatif à un nouvel article

Article 7 bis - Différentes catégories de personnes concernées

1. Les Etats membres prescrivent que les autorités compétentes ne peuvent traiter des données à caractère personnel, aux fins visées à l'article 1er, paragraphe 1, qu'en ce qui concerne les différentes catégories de personnes concernées suivantes :

a. les personnes dont il y a raisonnablement lieu de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale ;

b. les personnes reconnues coupables d'une infraction pénale ;

c. les victimes d'une infraction pénale ou les personnes à l'égard desquelles certains faits portent à croire qu'elles pourraient être victimes d'une infraction pénale ;

d. les tiers à l'infraction pénale, tels que les personnes pouvant être appelées à témoigner lors d'enquêtes en rapport avec des infractions pénales ou des procédures pénales ultérieures, ou une personne pouvant fournir des informations sur des infractions pénales, ou un contact ou un associé de l'une des personnes mentionnées aux points a) et b) ;

2. Les données à caractère personnel concernant d'autres personnes que celles visées au paragraphe 1 ne peuvent faire l'objet d'un traitement

a. que dans la mesure où ce dernier est nécessaire à l'enquête relative à une infraction pénale spécifique ou aux poursuites y afférentes, afin d'apprécier la pertinence des données pour l'une des catégories indiquées au paragraphe 1, ou

b. que si ce dernier est indispensable à des fins préventives ciblées ou à des fins d'analyse criminelle, si et aussi longtemps que ces fins sont légitimes, clairement définies et spécifiques et que le traitement se limite strictement à apprécier la pertinence des données pour l'une des catégories indiquées au paragraphe 1. Cette condition fait l'objet de réexamens réguliers, au moins tous les six mois. Toute utilisation ultérieure des données est interdite.

3. Les Etats membres prescrivent que des restrictions et des garanties supplémentaires s'appliquent, dans le respect de leur droit national, aux traitements ultérieurs des données à caractère personnel concernant des personnes visées au paragraphe 1, points c) et d).

3. Les droits des personnes concernées

Les divers éléments de la législation relative à la protection des données s'articulent autour de trois grands acteurs : les responsables du traitement (et leurs sous-traitants), les autorités de contrôle et les personnes concernées. Tant le règlement que la directive accordent à cette dernière catégorie de personnes une série de droits qui peuvent être exercés sur demande, notamment le droit à l'information, le droit d'accès aux données et le droit de rectifier ou de supprimer des données erronées ou traitées illégalement. Dans le règlement, ces droits font l'objet d'une mise en œuvre relativement libérale, le nombre d'exceptions possibles étant limité. Dans la directive, la situation est différente, également en raison de la nature du secteur répressif concerné. On comprend aisément que les autorités policières et judiciaires ne puissent pas toujours afficher une parfaite transparence quant à leurs modes de traitement des données et quant aux types de données à caractère personnel figurant dans leurs fichiers, car les enquêtes en cours pourraient être compromises.

Le groupe estime parallèlement que les exemptions et restrictions actuellement applicables aux droits des personnes concernées sont trop larges. Il n'est en particulier pas défendable que, sans autre explication, les Etats membres soient autorisés à soustraire au droit d'accès des catégories entières de données à caractère personnel. En conséquence, il conviendrait de supprimer l'article 11, paragraphe 5, et l'article 13, paragraphe 2. Le groupe insiste sur le fait que toute restriction des droits de la personne concernée devrait toujours être décidée au cas par cas, en tenant compte des circonstances particulières dans lesquelles s'inscrit la demande. La décision prise pourrait, par exemple, ne consister qu'en un refus partiel de la demande. Par ailleurs, le groupe reste d'avis que les dérogations à un droit fondamental devraient toujours faire l'objet d'une interprétation restrictive.

4. L'utilisation des analyses d'impact sur la vie privée dans le secteur répressif

Dans sa première réaction à la proposition de directive, le groupe a déjà vivement recommandé au législateur européen d'insérer dans la directive des dispositions exigeant la réalisation d'analyses d'impact sur la protection des données, y compris pendant la procédure législative. La réalisation de ce type d'analyses est d'autant plus importante à l'égard des traitements de données à caractère personnel effectués à des fins répressives, notamment au vu des risques accrus que comportent ces traitements pour les personnes. Le groupe ne comprend pas en quoi le secteur répressif se distinguerait fondamentalement des autres secteurs visés dans le règlement, dans lesquels des analyses d'impact sur la protection des données sont exigées pour apprécier les risques de nouvelles opérations de traitement envisagées. Dans ce domaine, il est extrêmement important de prévoir des garanties globales applicables au traitement des données à caractère personnel et ces garanties devraient donc être envisagées et mises en œuvre avant le début du traitement.

Le groupe est par conséquent satisfait des amendements 27, 28, 110 et 113 proposés par le rapporteur du Parlement européen, qui imposent au secteur répressif des obligations en matière d'analyse d'impact sur la protection des données, largement comparables aux obligations déjà instaurées dans le règlement. Cette mesure importante pour assurer aux personnes une meilleure protection de leurs droits fondamentaux, même dans un environnement bien informé comme le secteur répressif, devrait également être incluse dans l'approche générale

du Conseil à l'égard de la proposition de directive.

Il y a toutefois un point sur lequel l'avis du groupe diverge de celui du rapporteur. Dans ses amendements du considérant 41 et de l'article 25, paragraphe 2, le rapporteur introduit une obligation, imposée aux autorités de protection des données, d'évaluer toutes les analyses d'impact sur la protection des données et de formuler «des propositions appropriées afin de remédier à [toute] non-conformité». Le groupe considère que les autorités de contrôle ne devraient procéder que s'il y a lieu à une évaluation des analyses d'impact sur la protection des données.

5. Les pouvoirs des autorités de protection des données

La décision-cadre en vigueur, qui relève du troisième pilier, contient peu de dispositions consacrées aux missions et aux pouvoirs des autorités de protection des données, ainsi qu'aux possibilités et/ou obligations de coopération dans l'exercice des missions de contrôle et de répression. La proposition de directive représente à cet égard une grande avancée. Elle contient non seulement des dispositions soulignant la nécessité de disposer d'une autorité indépendante pour contrôler toutes les opérations de traitement des données qui se déroulent dans le cadre de la directive, mais aussi un chapitre spécifique sur la coopération entre ces autorités. Le groupe est favorable à l'esprit général de ces dispositions.

Malheureusement, les dispositions de la directive sont bien moins précises que celles de la proposition de règlement. Dans son avis général sur le paquet législatif, le groupe de travail « Article 29 » a donc déjà indiqué la nécessité de permettre aux autorités de contrôle d'avoir accès à tous les locaux. Il a également souligné la nécessité de rapprocher les dispositions des deux instruments pour assurer la cohérence du cadre juridique de la protection des données. Cet aspect est particulièrement important à l'égard de la nécessaire coopération entre les autorités chargées de la protection des données. Si ces autorités ne possèdent pas des pouvoirs similaires dans toute l'Union européenne, il pourrait être très difficile de préserver les droits des citoyens. Il pourrait arriver qu'une autorité soit habilitée, en vertu de sa législation d'exécution nationale, à entrer dans les locaux d'un service répressif pour y effectuer une inspection sans avoir préalablement obtenu le consentement de ce service, tandis qu'une autre autorité d'un pays voisin pourrait ne pas avoir

ce pouvoir et donc se voir refuser l'accès à ces locaux.

En ce qui concerne la situation des autorités de protection des données en matière d'information, la coopération pourrait se révéler d'autant plus compliquée si les pouvoirs de ces autorités restent non harmonisés, comme c'est le cas actuellement. Une étude menée par le groupe de travail « Article29 » indique que certaines autorités chargées de la protection des données ont accès, en application d'une disposition particulière de droit national, à l'ensemble des informations et documents qu'elles demandent, qu'ils soient publics, confidentiels ou classifiés, afin d'accomplir leurs missions de contrôle des traitements de données effectués à des fins répressives. Dans le cas d'autres autorités, un tel accès n'est accordé à leur personnel que s'il a obtenu une habilitation de sécurité délivrée par les services de renseignement compétents. D'autres autorités encore ne disposent d'absolument aucun accès aux informations confidentielles et/ou classifiées.

Par conséquent, si la directive impose aux autorités chargées de la protection des données de coopérer, il importe que toutes aient accès aux mêmes informations. Dans le cas contraire, elles pourraient ne pas avoir une vue d'ensemble des circonstances d'une affaire particulière et ne pas tirer la même conclusion, peut-être au détriment des intérêts de la personne concernée. Le groupe de travail « Article 29 » propose donc que la directive mentionne les types d'informations dont l'accès doit être accordé aux autorités chargées de la protection des données pour l'exercice de leurs missions de contrôle. Cette proposition n'a pas pour but d'abaisser les seuils d'accès aux informations classifiées dont bénéficient actuellement les autorités de protection des données.

Plus généralement, le groupe accueille favorablement les propositions faites par le rapporteur du Parlement européen sur les pouvoirs des autorités chargées de la protection des données et approuve la description plus détaillée de ces pouvoirs qu'il propose. L'amendement ci-après doit être envisagé comme un complément à ces propositions.

Amendement proposé

Article 46 - Pouvoirs (paragraphes à ajouter)

1. *Les Etats membres veillent à ce que chaque autorité de contrôle possède un pouvoir d'enquête lui permettant d'obtenir du responsable du traitement ou du sous-traitant l'accès à tous ses locaux, y compris à tous les équipements et moyens de traitement des données.*

2. *Les Etats membres veillent à ce que chaque autorité de contrôle se voit communiquer l'ensemble des informations et des documents nécessaires à l'exercice de ses pouvoirs d'enquête. Aucune obligation de confidentialité ne peut être opposée aux demandes des autorités de contrôle, à l'exception de l'obligation de secret professionnel visée à l'article 43.*

3. *Les Etats membres peuvent, conformément à leur droit national, subordonner à une enquête de sécurité supplémentaire l'accès aux informations classifiées à un niveau correspondant à « CONFIDENTIEL UE » ou à un niveau supérieur. Si aucun autre contrôle de sécurité n'est requis au titre de la législation de l'État membre de l'autorité de contrôle, ce fait doit être reconnu par tous les autres État membres.*

Fait à Bruxelles,
le 26 février 2013.

Pour le groupe de travail

Le président
Jacob Kohnstamm

Annexes

International Working Group on Data Protection in Telecommunications: Working Paper on Privacy and Aerial Surveillance

54th Meeting, 2-3 September 2013, Berlin (Germany)

Background

Surveillance is the monitoring of behavior, activities, or other changing information, for the purpose of influencing, managing, directing, or protecting someone or something. It often involves observation of individuals or groups by government organizations, although there are some exceptions, such as disease surveillance, which monitors the progress of a disease in a community without directly observing or monitoring individuals.

Aerial surveillance is the gathering of surveillance, usually visual imagery or video, from an airborne vehicle. Since the International Conference of Data Protection and Privacy Commissioners first discussed issues of aerial surveillance by satellites in 1992[52], there have been far-reaching technological developments. Whereas satellite-based services such as Google Earth at present do not pose particular risks to individual privacy as long as only snapshots with limited resolution of imagery are collected, the situation is different with regard to low flying surveillance platforms such as drones. Whereas the use of drones for military (combat) purposes is the subject of some limited – due to classification - public debate, similar debate about civilian uses of this technology for information collection purposes and their consequences has so far been neglected. The history of satellite technology since 1989 shows however that reconnaissance technology formerly restricted to military use can eventually become available for civilian use as well.

Surveillance platforms can be used for a wide range of purposes, including:

a) Remote sensing: the use of a variety of sensors (visual, infrared or near infrared spectrum, gamma ray, biological and chemical) to detect the presence of chemicals, microorganisms and other biological factors, radioactive materials, weapons and so on;
b) Commercial aerial surveillance: livestock monitoring, wildfire mapping, pipeline security, home security, precision farming, road patrol and anti-piracy[53];
c) Resource exploration: perform geophysical surveys in order

[52] Cf. Report of the Working Group on Data Protection in Telecommunications on problems relating to the secrecy of telecommunications and satellite communications and Common Statement of the 14th International Conference of Data Protection and Privacy Commissioners, 29 October 1992, Sydney, in: International Documents on Data Protection in Telecommunications and Media 1983 – 2006, p. 51; http://www.datenschutz berlin.de/attachments/334/IWGDPT_WP_brochure.pdf

[53] The US-companies Skybox Imaging and Planet Labs are planning to deploy fleets of lightweight microsatellites to engage in Live Earth Screening. They are allowing private investors to buy and downlink imagery, cf. http://www.nytimes.com/2013/08/11/business/microsatellites-what-big-eyesthey-have.html?_r=0 (seen on 20 October 2013).

to predict the location of oil, gas and mineral deposits, monitoring the integrity of oil and gas pipelines and related infrastructure, comparing the real size of farmland for which subsidies have been received with claims in the corresponding application forms[54];

d) Scientific research: weather observations, including close monitoring of dangerous weather systems such as hurricanes, or use in severe climates such as the Antarctic;
e) Search and rescue: searching for missing persons, damage assessment following a natural (or man-made) disaster; and
f) Conservation: monitoring movements of animals, detecting and monitoring hazardous material spills, forest fire detection, fishery protection, etc.

Surveillance Platforms

A variety of platforms[55], or vehicles, has been or can be used for aerial surveillance, including:

a) Fixed Wing: a fixed-wing aircraft is an aircraft capable of flight using wings that generate lift caused by the vehicle's forward airspeed and the shape of the wings. The wings of a fixed-wing aircraft are not necessarily rigid; kites, hang-gliders and aeroplanes using wing-warping or variable geometry are all regarded as fixed-wing aircraft;
b) Rotary Wing: the term rotary wing describes an airfoil that rotates about an approximately vertical axis, as that supporting a helicopter or autogiro in flight;
c) Unmanned Aircraft Systems (UAS): an unmanned aircraft (UA), commonly known as a drone, is an aircraft without a human pilot on board. Its flight is either controlled autonomously by computers in the vehicle, or under the remote control of a pilot on the ground or in another vehicle. UAS can either be fixed or rotary wing craft; and may be operated singly or in swarms (communicating with each other and with the ground under centralized control) or
d) Other: an aerostat is a craft that remains aloft primarily through the use of buoyant lighter than air gases, which impart lift to a vehicle with nearly the same overall density as air. Aerostats include free and/or moored balloons, airships or dirigibles and may be powered or unpowered.

Each of these platforms will have different operating characteristics such as operating altitude, speed, range, endurance (i.e., how long can the platform remain aloft), ability to loiter, and payload capacity.

Surveillance Technologies

A variety of surveillance technologies can be carried by the above-mentioned platforms, the exact payload being dependent on a number of factors including mission, weather, payload capacity, the range of the sensor, its field of view and resolution, and so on. Sensors include (but aren't necessarily limited to):

a) Visible spectrum: these sensors are typically in the form of cameras, including high-definition and full motion video systems[56]; they allow for continuous live surveillance and storage of the entire video footage;
b) Infra-Red (IR): these types of sensors detect energy emitted or reflected from the target. Most IR sensors are passive, although they may be used in conjunction with an IR illumination source. They can "see" through smoke, fog, haze and other atmospheric obscurants better than a visible light camera;
c) Night Vision: the ability to see in low light conditions, based on a combination of sufficient spectral range (i.e., how much of the electromagnetic (EM) spectrum the device can detect) and sufficient intensity range (i.e., how much light is needed to form a useful image). Night vision

[54] Cf. the European Integrated Administration and Control System (IACS) <http://ec.europa.eu/agriculture/direct-support/iacs/index_en.htm> aimed at preventing fraud in agricultural subsidies. IACS includes satellite surveillance.

[55] A different categorization appears on page 2 of Stanley, J and Crump. C., "Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft", ACLU Report dated December 2011 (available online at http://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf)

[56] The U.S. Army recently acquired a 1.8 gigapixel camera for use on its drones. This camera (Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System - ARGUS IS) offers 900 times the pixels of a 2 megapixel camera found in some cell phones; it was built at low cost using 368 camera chips from cell phones. It can track objects on the ground 65 miles away from an altitude of 20,000 feet. Cf.US Army unveils 1.8 gigapixel camera helicopter drone, BBC NEWS (29 December 2011), http://www.bbc.com/news/technology-16358851. An instructive video can be seen at: http://www.youtube.com/watch?v=QGxNyaXfJsA> accessed on 2 April 2013.

technologies can be broadly divided into three main categories:

1) Image intensification: these technologies work on the principle of magnifying the amount of received photons from various natural sources such as starlight or moonlight. Examples of such technologies include night glasses and low light cameras;
2) Active illumination: these technologies work on the principle of coupling imaging intensification technology with an active source of illumination in the near infrared (NIR) or shortwave infrared (SWIR) band. Examples of such technologies include low light cameras; and
3) Thermal imaging: these technologies work by detecting the temperature difference between the background and the foreground objects.

d) Radar: radar uses very high frequency radio waves to determine the range, altitude, direction or speed of an object. Radar can also be used to identify and track objects, such as vehicles, on the ground (using, for instance, Side Looking Airborne Radar (SLAR)); and
e) Specialized sensors: a range of specialized sensors (e.g., to detect traces of chemical, biological, nuclear, radiological and explosive materials; license plate scanners; acoustic sensors, etc.) can also be carried by aerial surveillance platforms. Combinations of these sensor types can provide organizations with the capability to conduct aerial surveillance under almost any conditions.

Privacy Implications

There are a number of aspects of surveillance that raise privacy concerns, including the surveillance being hidden, intrusive, indiscriminate and/or continuous.[57] Although these aspects were articulated in the context of electronic surveillance, they are also applicable to aerial surveillance:

a) Hidden: depending on size, operating altitude, sensor capabilities and so on, it may not be possible to detect aerial surveillance (either the platform itself or the sensors being used). Those subject to surveillance would have to rely on self-disclosure by the organization conducting the surveillance or disclosure by a third party. Those subject to hidden surveillance are less able to hold the organization conducting the surveillance accountable;
b) Intrusive: the range of possible operating conditions for

[57] Freiwald, Susan, "A First Principles Approach to Communications Privacy", published in the Stanford Technology Law Review (2007 STAN. TECH. L. REV. 3), dated 2007. Available online at http://stlr.stanford.edu/pdf/freiwald-first-principles.pdf.

aerial surveillance platforms and the capabilities of their associated sensors increase the intrusiveness of aerial surveillance (they can "see" almost anything and everything);

c) Indiscriminate: aerial surveillance generally covers an area that includes individuals and activities that do not warrant being subject to surveillance, resulting in an over-collection of information; and

d) Continuous: emerging aerial platforms combine increasing endurance and the ability to "stare" at an area to effectively create continuous surveillance of any given area[58].

These characteristics give rise to some specific privacy concerns[59]:

a) Mission creep: although most people would likely support the use of aerial surveillance (e.g. for detecting and monitoring natural disasters), or for use in specific, limited law enforcement circumstances, it seems inevitable that other privacy-invasive uses would be found for such technology;

b) Tracking: the ability to maintain surveillance over an extended area for an extended period of time raises the possibility that individuals and vehicles could be tracked on an on-going basis;

c) Proliferation as the cost of UAS technology is rapidly falling. UAS may be bought or built by private individuals for use as "personal" or "DIY" UAS.

More privacy intrusive than CCTV

The privacy implications of CCTV have been a subject of debate for years, and many privacy authorities have issued guidelines on the necessary safeguards regarding its use. As explained above, aerial surveillance systems have the potential to be much more privacy intrusive than CCTV systems, for several reasons including:

- Aerial surveillance systems may use many more different sensors than CCTV systems.
- The installation of CCTV usually requires access to and control of the premises concerned, which is not required for aerial surveillance systems, in particular for outdoor locations.
- Depending on flight height and other factors (e.g. miniaturization) aerial surveillance systems may be more difficult - if not impossible - to detect by the persons observed than most CCTV systems.
- Aerial surveillance systems may be deployed without any delay, not requiring installation or configuration on site.

This clearly indicates that the safeguards in place for CCTV, while indicating a minimal standard, cannot be considered sufficient in the context of aerial surveillance systems and have to be adapted and complemented by specific measures appropriate for the different aerial surveillance systems and usage scenarios.

Therefore certain new essential safeguards should be adopted by regulators on a national level taking into account possible differences between the public and the private sector. Furthermore, since aerial surveillance does not stop at national borders international agreements will be necessary to prevent a "global panopticon" from emerging.

Recommendations

Whether operated by law enforcement or other public sector agencies, by private sector companies, or flown recreationally by citizens, the increasing use of aerial forms of surveillance will likely intensify concerns about how to preserve and protect individual and collective privacy as people go about their daily lives. If aerial surveillance becomes an increasingly common fixture in today's society, and society accepts that presence as normal, it is conceivable that society's expectations of privacy in public could seriously erode. It is important to secure an

[58] The U.S. Air Force has developed the "Gorgon Stare" technology, a spherical array of nine cameras fitted to a drone which is able to capture motion imagery of whole cities ("With Air Force's Gorgon Drone 'we can see everything'", http://www.washingtonpost.com/wpdyn/content/article/2011/01/01/AR2011010102690.html

[59] A discussion of different potential privacy concerns/issues appears on page 11 of Stanley, J and Crump. C., "Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft", ACLU Report dated December 2011 (available online at http://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf).

appropriate balance between the needs of law enforcement, public safety, etc. on the one hand and the legitimate privacy interests of individuals on the other.

With that in mind, the Working Group makes the following recommendations:

a) the use of aerial surveillance should be limited to specific purposes[60] (e.g., searching for missing persons, border surveillance, legitimate private purposes such as access to information by journalists);
b) the use of personal data such as images collected from the air by government agencies should require a judicial warrant;
c) to the maximum extent possible, the public should be notified about the use of aerial surveillance; this requires e.g. that any UAS with the ability to collect and transmit information over a data link reports a GPS location, capabilities and ownership (e.g., government agency, company or private individual responsible for the particular platform or vehicle), in real time, to a competent authority and that this authority makes location information available, as open data, in real time;
d) surveillance should be restricted to as confined an area as possible (by limiting sensor fields of view), in order to minimize the likelihood of "over-collection";
e) stringent controls over how aerial surveillance information can be used and who has access to that information should be implemented. Exceptions can be made for emergencies (e.g., searching for missing persons); and
f) there should always be a "man in the loop" so that if there are any problems or unusual circumstances (e.g., the UAS starts to drift into a residential area), these can be addressed in as timely a manner as possible.

In view of the rapidly evolving technology, the Working Group will continue to monitor developments in this field closely.

[60] The ACLU describe the following constraints on the use of drones:
a) USAGE LIMITS: Drones should be deployed by law enforcement only with a warrant, in an emergency, or when there are specific and articulable grounds to believe that the drone will collect evidence relating to a specific criminal act;
b) DATA RETENTION: Images should be retained only when there is reasonable suspicion that they contain evidence of a crime or are relevant to an ongoing investigation or trial;
c) POLICY: Usage policy on domestic drones should be decided by the public's representatives, not by police departments, and the policies should be clear, written, and open to the public; and
d) ABUSE PREVENTION & ACCOUNTABILITY: Use of domestic drones should be subject to open audits and proper oversight to prevent misuse. See http://www.aclu.org/blog/tag/domestic-drones; see also the resources listed by EPIC at http://www.epic.org/privacy/drones mentioning several bills addressing these issues currently before the U.S. Congress.

International Working Group on Data Protection in Telecommunications: Working Paper on the Human Right to Telecommunications Secrecy

54th Meeting, 2-3 September 2013, Berlin (Germany)

In view of recent reports on the activities by intelligence services the Working Group recalls that it has on several occasions stressed the importance of telecommunications secrecy as a human right[61]. Most telecommunications today is taking place across borders therefore the distinction between national and international telecommunications has become obsolete.Telecommunications and in particular the Internet are essential technologies for individuals and societies in the 21st century. Both depend on the legitimate expectation of users that communications in principle are free from surveillance and interception. This applies to contents as well as metadata and other digital traces. If this confidentiality by default is threatened the very fabric of free societies is at risk. Interception of communications by government agencies in general[62] and intelligence services in particular can be necessary for legitimate reasons but it must be the *exception*, not the rule. To comply with principles of openness, transparency and accountability, there should be mechanisms to re-assure the public that interception powers are being used lawfully, appropriately and proportionally.

The Working Group therefore urges governments:

1. To recognize telecommunications secrecy as an essential part of the globally acknowledged human right to privacy;[63]
2. To strengthen telecommunications secrecy as a human right in an international convention. Restrictions should be limited to what is strictly necessary in a democratic society;
3. To agree on international rules limiting government access to data stored by Internet service providers and signals intelligence on the Internet;
4. To provide for greater transparency and public accountability of government agencies as to the results of lawful interceptions[64]; this includes transparent rules on classification and declassification[65];
5. To ensure that every data subject regardless of nationality has the right to be notified ex post, to have his data deleted and corrected and of access to justice;
6. To allow and encourage citizens to freely research, create, distribute and use tools for secure communications; no citizen should be monitored simply on the ground that he or she is using such tools;
7. To ensure effective and independent oversight with regard to surveillance activities carried out by police and intelligence agencies or on their behalf by private processors[67].

---

[61] Common Statement on Cryptography (12.09.1997) – http://www.datenschutzberlin. de/attachments/172/crypt_en.pdf ; Common Position on Public Accountability in relation to Interception of Private Communications, 23rd meeting, 15 April 1998, Hong Kong – http://www.datenschutz-berlin.de/attachments/904/inter_en.pdf; Ten Commandments to protect Privacy in the Internet World – Common Position on Incorporation of telecommunications-specific principlesin multilateral privacy agreements, 28th meeting, 14 September 2000, Berlin – http://www.datenschutz-berlin.de/attachments/216/tc_en.pdf ; Working Paper on TelecommunicationsSurveillance, 31st meeting, 27 March 2002, Auckland – http://www.datenschutzberlin.de/attachments/912/wptel_en.pdf; The Granada Charter of Privacy in a Digital World, 47th meeting, 15./16 April 2010, Granada – http://www.datenschutzberlin.de/attachments/794/675.40.11_Endfassung.pdf. The European Court of Human Rights in its jurisprudence has interpreted Art. 8 of the European Human Rights Convention along similar lines, see Case of Weber and Saravia v. Germany, Decision of 29 June 2006, with further references.

[62] For the diverse legal situation globally cf. International Data Privacy Law, Vol. 2 No.4 (2012), Special issue on Systematic Government Access to Private Sector Data.

[63] The right to private correspondence is specifically mentioned in Article 12 of the UN Universal Declaration of Human Rights, Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and Article 8 of the European Convention on Human Rights (ECHR).

[64] The European Court of Human Rights in the case of Youth Initiative for Human Rights v. Serbia, Judgment of 25 June 2013 has clarified that intelligence agencies are within the scope of freedom of information legislation.

[65] See Principles 11-17 of the Tshwane Global Principles on National Security and the Right to Information of 12 June 2013.

[66] See Principle 6 of the Tshwane Global Principles.

7 Annexes

International Working Group on Data Protection in Telecommunications: Working Paper on Web Tracking and Privacy: Respect for context, transparency and control remains essential

53rd meeting, 15-16 April 2013, Prague (Czech Republic)

Introduction

1. This paper is based on a foundation of respect for the fundamental rights and freedoms of Web users. Although it does not focus on specific technical remedies the paper does assume that the technical action of Web tracking must be lawful, appropriate and that it must operate within a strict framework of those rights. The principles of choice and control - claimed by much of industry - sit at the core of this framework, and those principles must be enacted with precision upon the pillars of clarity, transparency and accountability. The justification for the imposition of Web tracking is not self evident and thus industry and other tracking exponents must continually strive to explore solutions that bring this activity not just squarely within the framework of fundamental rights and privacy, but also in line with the imperative of Privacy by Design.

2. In this working paper, the Working Group addresses the issue of Web Tracking and Privacy. Although no clear definition exists, we will refer to a definition of Web Tracking[67] as the collection, analysis and application of data on user activity from a computer or device while using various services of the Information Society (hereinafter: the Web)[68] in order to combine and analyze it for different purposes, from charitable and philanthropic to commercial. We consider various forms of market research to fall within this definition of Web Tracking, for example outreach measurement (the degree to which users are served with ads across the Web), engagement measurement (the degree to which users interact with services across the Web) and audience measurement (the degree to which micro profiles can be derived from users interacting with services across the Web).[69]

Scope of the Working Paper

3. The paper is addressed to all providers of web sites as well as software developers and service providers offering or using tracking technology. This paper discusses the development of tracking technologies and their possible impact on the privacy of

[67] Cf. van Eijk (2012), The DNA of OBA: unique identifiers, URL: http://www.campusdenhaag.nl/crk/publicaties/robvaneijk.html#definition-of-web-tracking.

[68] Note that with IP-based technology becoming the backbone of the information society, and integrating many other former "stand alone" technologies ("Convergence"), this may well encompass the use of a telephone (IP telephony), television (IPTV), reading digital newspapers, or any other media consumption using digital technologies (including reading an e-book). For a detailed discussion of the resulting privacy risks cf. theWorking Paper on Privacy Issues in the Distribution of Digital Media Content and Digital Television (Berlin, 4./5.09.2007) of this Group; URL: http://www.datenschutz-berlin.de/attachments/349/digit_en.pdf

[69] JICWEBS Reporting Standards, URL: http://www.abc.org.uk/PageFiles/50/Web Traffic Audit Rules and Guidance Notes version2 March 2013 master.pdf

citizens. This paper deals with digital traces left behind when using various services of the Information Society with a Web Browser, including unique identifiers derived from non-cookie based techniques.[70] This includes Web Browsers on other devices, for example smart mobile devices and smart televisions.

4. This paper does not deal with specific additional risks which may stem from the advent of apps on mobile devices.[71] Nevertheless the principles in this paper should also be applied for tracking mechanisms used in other services.
5. This paper is not about how protective measures can be implemented (e.g., legal requirements for consent). Note that while in some jurisdictions, depending on the purpose of Web Tracking, explicit consent (opt-in) is required, in other jurisdictions, an opt-out for Web Tracking will be considered valid to satisfy the legal framework if certain conditions are met. These include, among other things: adequate notification of processing; transparency in the notification; notification at or before the time of collection; and simple, effective and persistent opt-out methods. A number of restrictions may also be in place, including limiting the processing sensitive information such as information on health, information on political or philosophical beliefs and the prevention of the tracking of children.

Background

6. The technical possibilities of monitoring the activities of users on websites have multiplied over the past decade and the emerging "Information Society" has seen several sea changes since then.[72] Web tracking developed from very modest beginnings - when single providers of online services started to monitor their users to find out whether a particular user had been there before and what this user had been doing - into an almost panoptical vision of marketers more recently. In this vision, the marketer seems to be able to monitor every single aspect of the behaviour of an identifiable user across websites. This could potentially become a complete history of the entire Internet usage of a data subject (literally from the cradle to the grave), and could be enriched with profile data from the former "offline world" (including any aspect of our lives data brokers have information about, including financial information as well as information on, for example, leisure, health, political and/or religious opinions, location information).[73]
7. This development - while greeted and fostered by marketers and other interested parties from the broader business community, and assisted by some policymakers at the national and regional levels - holds an unprecedented risk for the privacy of all citizens in an information society. The worst case scenario is that it would turn the world as we know it into a global panopticon. The offline equivalent would be to have somebody unknown to us constantly looking over our shoulders no matter where we are (in the streets or in the seeming privacy of our homes), or what we do (watching TV, shopping online, reading newspapers, and even more intimate activities), and without knowing when he is looking, and when he isn't.[74]
8. The possible repercussions of such a development are evident and not to be underestimated with respect to their potential gravity. It may annul and do away with some of the core principles of privacy - and notably transparency and control for the individual.[75] To put it more bluntly, this might be the end of the (privacy) world as we know it.

---

[70] For example, passive fingerprinting techniques based on hashing the HTTP user agent and/or the IP address of the originating browser.

[71] See, for example, Opinion 02/2013 on apps on smart devices WP 202 issued by the Article 29 Working Party (Art. 29 WP), URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2013/wp202_en.pdf

[72] The literature review on Web privacy measurement, which has been produced as an outcome of the Conference on Web Privacy Measurement (WPM) gives a more elaborate view on the technologies used for tracking, URL: http://www.law.berkeley.edu/12633.htm

[73] In Customer Relationship Management (CRM) the common terms are Customer Lifetime and Customer Lifetime Value.

[74] To make things even worse, this modernist version of the panopticon would record every single move of any given individual at any given moment in time no matter whether the guard is watching or not.

[75] Tracking as a technology is not transparent. At the technical level, in many cases, the pixels (e.g., web beacons) and mini webpages (e.g., iFrames) are invisible to the human eye.

9. The promoters of this vision, on the other hand, claim that these risks either do not exist at all, or that they have tried to address and mitigate these risks at least in part. There is strong resistance from some stakeholders from industry against recognizing that unique identifiers in Web data are personal information. One claim often put forward is that much of the data in use has been de-identified (i.e., anonymised), and that once this has been done, the data is no longer about a person and would therefore not pose a risk to the privacy of citizens. It is also claimed that any behavioural data are linked to machines only and can - this is the claim - in very many instances not be traced back to an individual at all.
10. However, these claims have no scientific proof whatsoever, and ignore the fact that machines - and especially smart phones - are becoming more and more personal devices and allow for an easy link to any given individual user. Traces can also increasingly be linked across different devices. There is also scientific proof that many seemingly anonymous data (e.g., location information of cell phones) can be traced back (i.e., be de-anonymised) to any given user if the database and the timeframe are sufficiently broad. Even worse, more recent academic work suggests that it is impossible in principle to keep "anonymous" data from being de-anonymised if the time slice depicting any given behaviour is sufficiently big (i.e., it is conceptually impossible to guarantee that "anonymous" data cannot be traced back to an individual over time). If this holds true, it is a game changer and will make a couple of core assumptions about how uses of different types of data may or may not affect the privacy of individuals useless.[76]
11. In addition, and on a slightly different note, practical daily knowledge also adds to questioning the claims made by industry. While ads may well be addressed to a machine at the technical level, it is not the machine which in the end buys the proverbial beautiful pair of red shoes - it is an individual. Thus, the claim that the processing of behavioural data for marketing is directed "only" at machines in the first place may well be seen as an attempt to blur our vision as societies on the gravity of the problem, when in reality the individual and not the machine is the only instance that can make all

[76] Cf. Ohm, Paul: Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, August 2009. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006

such tracking operations a "success" for its proponents (i.e., when the red shoes are finally being bought).

A short history of monitoring technologies

12. In trying to trace back the development described above to its modest beginnings, one mmilestone we find is the development of "cookie technology" almost 20 years ago. HTTP Cookies were introduced in 1994, first and foremost to solve the "small" problem of reliably implementing a virtual shopping cart. Due to the mostly stateless nature of the Hypertext Transfer Protocol (HTTP), user agents were not able to retain state information until then. Retaining state information was crucial for the virtual shopping cart in order to remember selected items during the shopping experience. Transparency was already then a privacy issue, because the use of cookies was not conveyed to the ordinary user. At the time, cookies were enabled by default in the browser settings and the user was not notified about the use of cookies.[77]
13. To mitigate the privacy and security risk of leaking cookie information to other sites the same origin policy was implemented. This policy meant that cookies could only be read by the same domain that set them. However, it is important to note that recommendations through the World Wide Web Consortium (W3C) propose a new standard, Cross Origin Resource Sharing (CORS)[78] which will permit the sharing of information across specified domains. Although CORS is a voluntary standard, it conflicts with the same origin policy.
14. In 1998, this group[79] addressed various privacy issues connected to the systematic collection or use of personal data on the Web.[80] In its working paper, it addressed P3P (Platform for Privacy Preferences Project), a protocol developed by W3C, which was designed to block third party cookies unless the website the user visited offered a user acceptable P3P policy.[81] However, only one major browser manufacturer implemented the standard. As a result, P3P has not been adopted widely on the Web.
15. Third party cookies have become the lifeblood of the complex digital ad industry. In 2008 marketing executives of Web Tracking companies discussed the future of analytics and site statistics. The future, five years ahead, was envisioned to be an integration of traditional sitevisit statistics (hereinafter: First and Third Party Analytics) and analytics data from other services on the Web including, for example, video, widgets, social networking, gaming and search engines (hereinafter: Web Analytics).[82]
16. Today, Web Analytics Data represents a new form of economic value. While this group does not question the benefits that measuring consumer behaviour may bring for (real-time) online behavioural advertising (OBA), it firmly believes that such practice must not be carried out at the expense of individuals' rights to privacy and data protection.

Web Tracking

17. Web Tracking involves the collection and subsequent retention, use or sharing of data on individual online behaviour across multiple websites by the use of cookies, JavaScript or any kind of device fingerprinting. Web Tracking technology enables a constant flow of real-time information about users, such as registration data, search activities, behavioural data, site visit statistics and conversion

---

[77] RFC 2109, HTTP State Management Mechanism, URL: https://tools.ietf.org/html/rfc2109. Note that current flavors of cookie storage technology include for example flash cookies and the LSOs (Local Shared Objects) used in HTML5 with matching values.

[78] Cross-Origin Resource Sharing, URL: http://www.w3.org/TR/cors/; W3C "Candidate recommendation" status since 29 January 2013 (viewed on 30 May 2013).

[79] International Working Group on Data Protection in Telecommunications.

[80] Common Position on Essentials for privacy-enhancing technologies (e.g. P3P) on the World Wide Web (Hong Kong, 15.04.1998), URL: http://www.datenschutz-berlin.de/attachments/178/priv_en.pdf

[81] The Platform for Privacy Preferences Project (P3P) enables Websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents. P3P user agents will allow users to be informed of site practices (in both machine- and human-readable formats) and to automate decision-making based on these practices when appropriate. Thus users need not read the privacy policies at every site they visit. , URL: http://www.w3.org/P3P/

[82] Omma Global Measurement 3.0, URL: http://www.webmetricsguru.com/archives/2008/09/measurement- 30-on-the-next-5-years-omma-global-day-2/

data reflecting how a user responded to individual offers. These data can be used to infer users' interests, political opinions or medical conditions. These data can be processed with the purpose to evaluate, treat in a certain way or influence the status or behaviour of an individual. Data about individual behaviour drives business decisions based on customer profiles. Buying intent may be derived from a person's presumed digital identity. The value of a potential customer is related to the chance to convince him to buy a product.

18. Web Tracking technology is present on mobile devices. A smart mobile device is unlikely to be shared between individuals, therefore making the link between the device and the individual stronger than with, for instance, desktop computers. Mobile devices contain unique device identifiers such as advertising specific identifiers,[83] the Unique Device ID (UDID), Media Access Control (MAC) address, Bluetooth MAC address, Near Field Communications (NFC) MAC address, International Mobile Subscriber Identifier (IMSI, a unique SIM card number) and the International Mobile Equipment Identifier (IMEI). These identifiers cannot be changed by ordinary users. In addition to unique identifiers, smart mobile devices may contain a rich set of data such as user name, password, age, gender, and address book. Smart mobile devices can expose accurate behavioural data on the whereabouts of a user. Precise geolocation data is readily accessible for browsers on smart mobile devices.
19. Web Tracking technology is deployed in various ways. A digital data trail may result from unintentional or unwilling disclosure of data, and may result in unnecessary disclosure of (personal) data. There are multiple ways to generate a digital data trail. For example, a campaign manager for digital ads could assign a unique identifier to the user, browser or device. Another way is to personalize referral information by adding audience segment information (micro profiles) while surfing the Web, so other sites participating in the campaign can track the user, browser or device too. A third example is by correlating unique identifiers with data collected from past visits on a specific site. A fourth example is that Web Tracking for a campaign can also take place by combining

[83] For example, to be able to perform frequency capping (control of the number of times a user has seen an ad), to deliver behavioral ads, and to measure the reach and effectiveness of an advertising campaign.

new tracking data (about a user, browser or device data) with data previously collected on a specific site, or data obtained from another (third) party. A final example involves the use of cookie matching services tha connect digital trails from the same user, browser or device with the use of different parts of the Web.[84]

20. Web Tracking consists of several automated steps, starting with the collection of Web data, the retention of these data, and the use of the data. By recombination, correlation and decontextualization, Web data can be used to construct very detailed predictive profiles of individual behaviour. Finally, Web Tracking leads to the actual application of the profile to an individual.[85]
21. Data can be stored in graph databases by various services on the Web.[86] The graph structure enables the emergence of behavioural patterns that would otherwise remain undetected. Web Tracking data in a graph can create meaningful patterns about user behaviour by itself or when combined with other data from various sources. For example, while individual unique identifiers connected directly or indirectly to a user or computer may expose little information about the casual surfer, the collection of unique identifiers reveals a pervasive view of someone's habits and browsing behaviour on the Internet. The collection of unique identifiers can be used to construct a digital identity.

Web tracking and the right to privacy and data protection of the individual

22. A key principle across a broad range of international legislative frameworks is the right to privacy that the Internet user has regardless of technology. Key elements are transparency, control and respect for context. The fact that users are unaware that they are being tracked is a privacy risk. Web Tracking as a process utilises a number of technical tools which limit the opportunity for users to be notified. For example, pixels (e.g., web beacons) and mini web pages (e.g., iFrames) are invisible to the human eye and inclusion in a web page will initiate an automatic HTTP request including the opportunity to set and access cookies containing unique identifiers.
23. Many web tracking technologies have been developed and deployed in business without providing information to the users whose data is being collected and without giving them any choice. User signals that could be understood as expressing objection to tracking have been disregarded and technical mechanisms against some tracking mechanisms have been actively circumvented, for example, by re-spawning deleted cookies, (passive) fingerprinting, and circumventing browser settings. Only when these behaviours were detected and were publicly criticized did the interested parties accept their obligation to respect users' free will. In such cases, sometimes opt-out schemes have been added after the fact, often leading to clumsy mechanisms of limited usefulness for the user. These cases have caused greatdamage to the users' trust in the reliability and honesty of all web service providers and undermine the healthy development of innovative web services.
24. Web Tracking constitutes processing of personal data in many jurisdictions due to the fact that the technology enables the individualization or identification[87] of users and/or making automated decisions about them. An example of such practice might be automatic decisions

[84] See for example URL: https://developers.google.com/ad-exchange/rtb/cookie-guide#what-is

[85] Cf. also Recommendation CM/Rec(2010)13 of the Council of Europe on the protection of individuals with regard to automatic processing of personal data in the context of profiling.

[86] A graph is based on graph theory which is a mathematical approach to model pairwise relations between objects. A graph database stores graphs which are essentially structures with nodes, edges, and properties. Theproperties may contain meta information about the nodes and edges.

[87] Recital 26 of the general Data Protection Directive 95/46/EC: Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person (...), URL: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

engines with algorithms in real time bidding platforms for personalized behavioural advertising.

25. There is strong resistance from some interested stakeholders against classifying unique identifiers in Web data as personal information. One claim often put forward is that once data has been de-identified[88], the data is no longer about a person. It should, however, be clear that a "purpose" element can also be responsible for the fact that information "relates" to a certain person or is about a person.[89]

The potential impact (or lack of impact) of "Do Not Track" (DNT) - a case study

26. In September 2011, the W3C chartered the Tracking Protection Working Group[90]. The group is working on a Do Not Track (DNT) standard. All major browsers have committed themselves to implement the standard (and most have already so implemented the HTTP header), however there remains, amongst those stakeholders who will honour the DNT:1 request[91], an open discussion on parts of the voluntary standard. Some stakeholders have indicated they will not honour the DNT flag for various reasons. The overall success of DNT is tied to the actual honouring of the DNT flag by receiving organizations and the factual adoption of the DNT standard throughout the Web by all stakeholders.
27. The default settings of DNT and the default actions by the Web Tracking organisation remain crucial once again. For DNT to be an effective instrument to provide user control, it is crucial that those performing Web Tracking can be certain that the DNT signal which they receive is a true indication of the user's wishes. In the absence of fully informed user choice, a Web Tracking organisation must assume that a user is not aware of Web Tracking and therefore assume the default position as if they had received a DNT:1 signal, which indicates a wish from the user not wanting to be tracked.
28. Any technology used for Web Tracking purposes must be proportionate. Data protection principles used worldwide are based on the notion that data should be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Data processing should be adequate, relevant and not excessive in relation

[88] De-identification means deleting, modifing, aggregating, anonymizing or otherwise manipulating data.
[89] Opinion 4/2007 on the concept of personal data (WP136), p. 10 URL: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2007_en.htm
[90] The mission of the Tracking Protection Working Group is to improve user privacy and user control by defining mechanisms for expressing user preferences around Web tracking and for blocking or allowing Web tracking elements, URL: http://www.w3.org/2011/tracking-protection/charter
[91] In the current draft DNT standard, sending "0" signals that tracking is fine, while "1" indicates a wish NOT tobe tracked.

to the purposes for which they are collected and/or further processed.

29. Finally, any technology must be "court-proof" if it is to contribute to serving the protection of privacy. DNT is in danger of remaining a tool through which a user may express wishes to service providers in the information society, without being an effective granular dialogue instrument. This leaves the user himself or any public (or private) body being chartered with enforcing those wishes or rules (and including corresponding legal obligations to honour any such choices made by an individual) empty handed vis-à-vis those providers. Some industry stakeholders try to defend the position that DNT does not constitute an obligation to respect such a wish. While this interpretation is more than doubtful, the fact remains that it is difficult to prove whether such a wish has been respected and or been disregarded.[92]

In other words, from an enforcement perspective, DNT could remain a sugar pill instead of being a proper cure and would as such be useless.

Recommendations

30. Unchecked Web Tracking may change the balance between service providers and individuals, including with respect to privacy protection. The Working group underlines that context, transparency and control remain crucial elements in the context of Web Tracking.

31. In order to contribute to addressing the risks for the privacy of the individual, the Working Group makes the following recommendations to the different stakeholders who have a part to play in the Web Tracking ecosystem.

Re-introduce respect for context and purpose limitation as core principles for any use of personal data:

- incorporate precautionary principles in any (automated) data collection, processing and sharing practices, so that data collected in one context cannot be applied in another context; and
- inform about the purpose of data collection in advance and do not change the purpose without renewed information and choice.

Bring back transparency:

Refrain from the use of invisible tracking elements;

- As a minimum, notify the user in an intelligible way when the user agent is about to send/receive a Web Tracking identifier to/from the origin/destination server;
- Display an indicator noticeable enough to the user[93] whenever Web Tracking is in progress; and
- Make an indication that Web Tracking is in progress also available to special groups of users, including the visually impaired.

Put the user back into control:

- implement mechanisms that allow users to exercise their right to privacy and data protection on the Web and do not deploy any (new) tracking mechanisms that do not have a user control mechanism; offer users an explicit choice regarding tracking - when browser software is to be installed, activated or updated, there must be a user choice;
- if the browser does not provide a user interface, the default setting should be such that the user is not tracked;
- give users the opportunity to reconsider their choice and change settings after the initial decision and at any time; let the user examine the (automated) choices that have been made with regards to Web Tracking in an easy way; and remind the user that choices regarding the (automated) settings for Web Tracking can be revoked at any time and make sure that

[92] External audit might play an important role in addressing at least parts of the problems described above, but would on the other hand add even further complexity to the ecosystem.

[93] Special consideration must be given to ensure that no group of web users are treated less favourably or are otherwise discriminated against, for example, as a result of a disability.

a revision of any such choices is technically possible in an easy way that does not put any undue burden on the individual;
- honour requests when the user agent is signalling that it does not want to be tracked;
- refrain from (passive) fingerprinting, for example by mining user generated data (such as service configurations, or user agent strings) in order to derive a unique user identifier (device fingerprint) when a user has expressed not wanting to be tracked; and
- ensure that the application of any technology devised to let users make choices is auditable and can be enforced by the competent private or public bodies chartered with enforcing rules, and especially those enshrined in the different existing legal frameworks which provide the foundation of the protection of privacy of the individual in many jurisdictions across the globe.

La protection des données dans la jurisprudence de la Cour européenne des droits de l'homme

Discours du Président Dean Spielmann (Cour européenne des droits de l'homme) prononcé lors de la célébration du 10e anniversaire de la Commission nationale pour la protection des données à Esch/Belval le 28 janvier 2013

Monsieur le Ministre,

Mesdames, Messieurs,

C'est avec beaucoup de plaisir que j'ai accepté de participer à cette journée, qui me permet de saluer l'activité essentielle de la Commission nationale pour la protection des données à l'occasion de son 10e anniversaire. Les Commissions telles que la votre existent dans un certain nombre de pays et elles y jouent un rôle tout à fait essentiel. Ma présence parmi vous témoigne de l'importance que j'y attache personnellement.

Au niveau européen, on sait que le Conseil de l'Europe a été, en quelque sorte, un pionnier en la matière puisque, dès 1973 et 1974, des recommandations furent adoptées dans le domaine de la protection des données et que, surtout, le 28 janvier 1981, la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, dite convention 108, fut ouverte à la signature des Etats membres du Conseil de l'Europe.

La pierre apportée par la Cour européenne des droits de l'homme est loin d'être négligeable et c'est ce que je vais m'efforcer de vous démontrer dans mon exposé. Si on remonte au temps lointain de l'élaboration de la Convention européenne des droits de l'homme, force est de constater qu'elle ne contient aucune référence à la nécessité de protéger les données personnelles. Cela n'est guère surprenant : dans l'immédiat après-guerre, les préoccupations dans ce domaine ainsi que les avancées technologiques étaient limitées. Cela explique donc que cette question fût largement ignorée des rédacteurs du texte.

En revanche, la Charte des droits fondamentaux de l'Union européenne, beaucoup plus récente puisque proclamée à Nice en décembre 2000, n'ignore pas ces questions et son article 8, qui s'intitule « Protection des données à caractère personnel », dispose que :

« 1. Toute personne a droit à la protection des données à caractère personnel la concernant.
2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.
3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante. »

On ne sera cependant pas surpris qu'une Cour telle que la nôtre, qui se veut proche des évolutions et des préoccupations de nos sociétés, se soit, en définitive, rapidement intéressée à ces questions qui sont désormais largement traitées par la jurisprudence.

L'interprétation « évolutive » des différentes exigences de la Convention à laquelle la Commission et la Cour européenne des droits de l'homme se sont livrées, depuis plus de cinquante ans, a permis de prendre en compte l'évolution de nos sociétés telle qu'elle résulte des nouvelles technologies. Le souci de protéger les données personnelles des citoyens a également et naturellement été pris en compte.

A titre liminaire, il importe de rappeler que le traitement et l'utilisation automatisés de données à caractère personnel, s'ils sont récents, correspondent à un phénomène mondial dont les effets sont largement bénéfiques.

Nous en sommes les acteurs et les témoins dans tous les actes de notre vie quotidienne. La réservation de billets de train ou d'avion, les demandes de remboursements de frais médicaux, les démarches relatives à l'obtention de documents d'identité sont des exemples non exhaustifs des circonstances très nombreuses dans lesquelles nous sommes conduits à divulguer à autrui, notamment aux administrations, des informations de nature tout à fait privée, voire intime. Toutes ces données sont non seulement collectées, ce qui, en soi, ne soulève pas de difficulté majeure, mais elles peuvent surtout être traitées, croisées, conservées, tout cela sans que nous en soyons même informés. Ceci a été grandement facilité par les progrès de la technologie dont nous sommes les principaux bénéficiaires en raison de l'amélioration que cela amène dans notre vie quotidienne. Cependant, il arrive que nous en soyons les victimes.

Il n'est pas surprenant que les autorités nationales aient très rapidement compris l'usage qui pouvait être fait de ces données personnelles multipliées à l'infini et à partir desquelles un portrait très complet de chacun d'entre nous peut être effectué. Certes, les raisons pour lesquelles les Etats démocratiques font usage des données personnelles sont principalement liées à la lutte contre le terrorisme et la criminalité, mais également à l'exercice efficace par l'État de ses fonctions administratives, objectifs auxquels nous ne pouvons que souscrire. Toutefois, il s'agit clairement d'ingérences dans notre vie privée.

C'est à la **collecte des données** que je consacrerai la première partie de mon intervention. Je parlerai, dans un second temps, de **la conservation et de l'exploitation des données**. Puis, j'évoquerai, plus brièvement, la question de la divulgation des données et l'accès des personnes **aux données** qui les concernent.

Avant d'évoquer la collecte des données à proprement parler, je souhaite rappeler qu'en l'absence de dispositions spécifiques dans la Convention européenne des droits de l'homme, c'est par le biais de l'article 8 et par une extension de son champ d'application que la Cour est intervenue. On sait que l'article 8 contient un premier paragraphe dans lequel est défini le droit protégé, puis un second qui énonce les restrictions qui peuvent être légitimement appliquées au droit. La jurisprudence s'est donc construite en tenant compte de la nécessité de protéger la vie privée des individus, mais aussi de prendre en considération les limitations ou restrictions opposées par les Etats. La Cour accepte ces ingérences,

mais exige que celles-ci soient prévues par la loi (une loi accessible et prévisible dans ses effets) ; qu'elles poursuivent un but légitime ; qu'elles soient nécessaires dans une société démocratique.

La collecte des données

Nous ne cessons, et en pleine connaissance de cause, de communiquer des données qui nous concernent. Toutefois, c'est souvent à notre insu que des données personnelles peuvent être collectées. Un exemple particulièrement flagrant de données collectées sans que l'intéressé en soit conscient concerne les écoutes téléphoniques, pratique fréquemment utilisée par les services de sécurité.

Les arrêts rendus en matière d'écoutes téléphoniques sont nombreux. Parfois, la Cour a d'emblée sanctionné l'absence de légalité de la mesure. Dès l'affaire *Klass c. Allemagne*[94], il fut entendu que les communications téléphoniques étaient protégées par l'article 8 de la Convention et que leur interception par les services de police et de sécurité s'analysait comme une ingérence, laquelle devait être prévue par la loi et nécessaire dans une société démocratique. L'arrêt *Malone c. Royaume-Uni*[95] qui portait également sur l'interception de communications téléphoniques le compléta utilement, dans la mesure où il donna des indications sur la notion de loi au sens de la Convention. Pour être considérée comme compatible avec la Convention, la loi doit être compatible avec la prééminence du droit et le pouvoir d'appréciation de l'exécutif doit être défini avec une netteté suffisante, compte tenu du but légitime poursuivi, pour fournir à l'individu une protection adéquate contre l'arbitraire. C'est précisément l'absence de bases légales qui conduisit la Cour dans l'affaire Malone à conclure à la violation de la Convention. Elle confirmera cette jurisprudence à l'encontre de la France dans les affaires *Kruslin et Huvig*[96] qui seront d'ailleurs à l'origine de la loi du 10 juillet 1991, relative au secret des correspondances émises par la voie des télécommunications. Par la suite, la Cour continuera d'examiner à chaque fois si la loi, en vertu de laquelle l'autorité publique mémorise les données personnelles, remplit les conditions telles qu'elles résultent de l'arrêt Malone précité. Parmi les affaires importantes, on peut notamment citer *l'arrêt Amann c. Suisse* du 16 février 2000[97] : il concernait un appel téléphonique passé au requérant depuis une ambassade pour lui commander un appareil dépilatoire qu'il commercialisait. Cet appel fut intercepté par le ministère public, qui fit établir sur le requérant une fiche par les services de renseignements. La Cour parvint à un constat de violation de l'article 8 en raison de l'enregistrement de l'appel téléphonique et car l'établissement de la fiche, comme sa conservation, n'étaient pas « prévus par la loi », le droit suisse étant imprécis quant au pouvoir d'appréciation des autorités dans ce domaine.

En ce qui concerne les écoutes téléphoniques et l'exigence de base légale, on peut citer aussi *l'arrêt P.G et J.H. c. Royaume-Uni*[98] L'affaire concernait l'enregistrement de la voix des requérants – arrêtés car soupçonnés d'être sur le point de commettre un vol – dans les locaux d'un commissariat. La Cour parvint à un constat de violation de l'article 8, car il n'existait à l'époque des faits aucun système légal permettant de réglementer l'usage des dispositifs d'écoute cachés par la police dans ses propres locaux.

On peut également citer les interceptions qui ont lieu dans un autre contexte, celui des établissements pénitentiaires. Dans l'affaire *Wisse c. France*[99], qui concernait le dispositif d'interception des conversations tenues lors des « parloirs » accordés aux proches des requérants détenus dans des maisons d'arrêt, la Cour a conclu à la violation de l'article 8. Elle

[94] Arrêt Klass et autres du 6 septembre 1978.
[95] Arrêt Malone c. Royaume-Uni du 2 août 1984.
[96] Arrêts Kruslin et Huvig c. France du 24 avril 1990.
[97] Arrêt Amann c. Suisse du 16 février 2000.
[98] Arrêt P.G et J.H. c. Royaume-Uni, du 25 septembre 2001.
[99] Arrêt Wisse c. France, du 20 décembre 2005.

a estimé, en effet, qu'en ce concerne les enregistrements des conversations tenues dans les parloirs des prisons, le droit français n'indiquait pas avec assez de clarté la possibilité d'ingérence par les autorités dans la vie privée des détenus, ainsi que l'étendue et les modalités d'exercice de leur pouvoir d'appréciation dans ce domaine.

Elle est parvenue à une conclusion analogue dans une affaire *Vetter c. France*[100] particulièrement intéressante. Dans cette affaire, à la suite de la découverte du corps d'une personne abattue par arme à feu, la police judiciaire, qui soupçonnait le requérant d'être l'auteur de cet homicide, sonorisa l'appartement d'une personne chez qui celui-ci se rendait régulièrement. La Cour a conclu à la violation de l'article 8, car elle a estimé que dans le domaine de la pose de micros, le droit français n'indiquait pas avec assez de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités.

Enfin, on peut citer, mais cette liste est loin d'être exhaustive, l'arrêt *Taylor-Sabori c. Royaume-Uni*[101] qui concernait l'utilisation par la police de messages de bipeur : les messages qui étaient adressés au requérant – accusé d'association de malfaiteurs pour la fourniture de drogues illicites – étaient interceptés au moyen d'un « clone » de son bipeur. La Cour a conclu à la violation de l'article 8, car aucune disposition légale ne réglementait l'interception de messages reçus sur des bipeurs et transmis par l'intermédiaire d'un système de télécommunications privé.

Autre moyen de collecter les données et qui figure parmi les méthodes de lutte contre la criminalité très utilisées dans nos sociétés, les systèmes de vidéosurveillance extrêmement sophistiqués qui se sont considérablement développés ces dernières années. L'article 8 s'applique ici tout naturellement. Dans ce domaine, on peut citer l'arrêt *Peck c. Royaume-Uni,*[102] qui indique dans quelles conditions de telles méthodes peuvent être autorisées et sur lequel je reviendrai un peu plus tard en évoquant la question de la divulgation des données personnelles.

Si la collecte des données ne soulève pas, en soi, de difficulté majeure, la conservation des données personnelles est une question autrement plus délicate.

La conservation des données personnelles

Dans nos sociétés démocratiques, l'existence de services de sécurité et de renseignement est parfaitement légitime. Nous sommes pleinement conscients

[100] Arrêt Vetter c. France du 31 mai 2005.
[101] Arrêt Taylor-Sabori c. Royaume-Uni du 22 octobre 2002.
[102] Arrêt Peck c. Royaume-Uni du 28 janvier 2003.

que, pour défendre l'ordre, prévenir les infractions pénales ou protéger la sécurité nationale, de tels organes conservent les données personnelles qui ont été collectées. Notre Cour ne peut tolérer ce pouvoir de surveillance que sous certaines conditions et toujours avec le souci de sauvegarder les institutions démocratiques.

La Cour apprécie les intérêts en présence et les arguments avancés par les autorités pour justifier la conservation des données. Ainsi, dans l'affaire *Segersted-Wiberg c. Suède*[103], la Cour a relevé en particulier, que, selon l'article 33 de la loi de 1998 sur les données de la police, des informations personnelles pouvaient être consignées dans le fichier de la Sûreté lorsque ces informations concernaient une personne soupçonnée d'une activité criminelle menaçant la sécurité nationale ou d'une infraction terroriste, ou faisant l'objet d'un contrôle de sécurité, ou lorsqu'il existait « d'autres raisons spéciales, eu égard au but de la tenue du fichier ». Si la Sûreté disposait d'une certaine latitude quant à l'appréciation de l'existence de « raisons spéciales », cette latitude n'était pas illimitée. Par exemple, en vertu de la Constitution suédoise, un citoyen ne pouvait faire l'objet d'une entrée dans un registre public exclusivement en raison de ses opinions politiques à moins qu'il y ait consenti. L'article 5 de la loi sur les données de la police interdisait également de manière générale la consignation de données sur la base des opinions politiques. Dans ces conditions, la Cour a estimé que l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités étaient définies avec suffisamment de clarté, compte tenu du but légitime poursuivi par la mesure en question, pour fournir à l'individu une protection adéquate contre l'arbitraire.

La question de la mémorisation des données collectées dans un registre secret et de sa durée est également importante. Elle est au coeur de l'affaire *Rotaru c. Roumanie*[104], dans laquelle la Cour a constaté une violation de la Convention en raison du manque de prévisibilité de la base légale invoquée par les autorités nationales. Il convient de noter que, dans cette affaire, la Cour a également été sensible au fait que la législation ne fixait pas de limite quant à l'ancienneté des informations conservées et à la durée de leur conservation. Il n'y avait pas non plus de disposition relative aux personnes pouvant consulter les dossiers, à la nature desdits dossiers, à la procédure à suivre pour les consulter. En se montrant plus exigeante pour ce qui concerne les données relatives au « passé lointain » d'un requérant, la Cour réaffirme que chacun a, en quelque sorte, un droit à l'oubli. Ceci était d'autant plus le cas en l'espèce que certaines des informations recueillies étaient fausses et de nature à porter atteinte à la réputation du requérant.

De manière générale, ce que la Cour cherche à assurer c'est un juste équilibre entre les intérêts qui se trouvent en concurrence. Dans une des premières affaires dont elle ait eu à connaître en la matière, l'affaire *Klass c. Allemagne*[105], elle a rappelé que les sociétés démocratiques se trouvaient menacées de nos jours par des formes très complexes d'espionnage et par le terrorisme, de sorte que l'État devait être capable, pour combattre efficacement ces menaces, de surveiller en secret les éléments subversifs opérant sur son territoire. Mais, consciente du risque « de saper, voire de détruire, la démocratie au motif de la défendre » que fait courir toute mesure de surveillance secrète par les mesures de sécurité, la Cour affirmait « que les Etats ne sauraient prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelle mesure jugée par eux appropriée ». Toutefois, dans l'affaire Klass, et malgré cette position de principe très ferme, la Cour conclut à la non-violation de l'article 8 au motif que la loi contestée par les requérants (portant restriction

[103] Arrêt Segersted-Wiberg c. Suède du 6 juin 2006.
[104] Arrêt Rotaru c. Roumanie du 4 mai 2000.
[105] Arrêt Klass c. Allemagne du 6 septembre 1978.

du secret de la correspondance, des envois postaux et des télécommunications) était considérée comme nécessaire, dans une société démocratique, à la sécurité nationale, la défense de l'ordre et la prévention des infractions pénales (article 8 § 2). Elle a donc clairement pris en considération les intérêts en présence.

Dans l'affaire *Leander c. Suède*[106], le requérant se plaignait du fait que des données liées à ses activités syndicales passées aient été mémorisées et se soient trouvées à l'origine de sa perte d'emploi, car ledit emploi se trouvait situé à proximité d'une zone militaire et avait été classé comme dangereux pour la sécurité. La Cour a mis cette affaire à profit pour compléter et préciser sa jurisprudence. Tout d'abord en énonçant que la mémorisation dans un registre secret et la communication de données relatives à la vie privée d'un individu entraient bien dans le champ d'application de l'article 8 § 1 de la Convention européenne des droits de l'homme. Puis, la Cour fit application des restrictions prévues par l'article 8 § 2 et du fait que, dans une société démocratique, l'existence de services de renseignement et la conservation des informations peuvent s'avérer légitimes et prévaloir sur l'intérêt des citoyens, à condition de poursuivre des buts légitimes, à savoir la défense de l'ordre, la prévention des infractions pénales ou la protection de la sécurité nationale. Elle parvint donc à un constat de non-violation de l'article 8 au motif que les garanties dont s'entourait le système suédois de contrôle du personnel remplissaient les exigences de l'article 8. La Cour a estimé que le gouvernement suédois était en droit de considérer que les intérêts de la sécurité nationale prévalaient en l'occurrence sur les intérêts individuels du requérant.

Qui dit conservation des données dit fichage. Or, le fichage d'une certaine catégorie de la population peut parfois s'avérer nécessaire. Ainsi, dans les affaires *Bouchacourt c. France, Gardel c. France et M.B. c. France*[107], tout en réaffirmant le rôle fondamental de la protection des données personnelles soumises à un traitement automatique, surtout à des fins policières, la Cour a conclu que l'inscription des requérants au Fichier judiciaire national automatisé des auteurs d'infractions sexuelles, telle qu'elle leur avait été appliquée, n'était pas contraire à l'article 8. En effet, elle a considéré qu'elle ne saurait mettre en doute les objectifs de prévention du fichier en question, que les sévices sexuels constituent

[106] Arrêt Leander c. Suède du 26 mars 1987.
[107] Arrêts Bouchacourt c. France, Gardel c. France et M.B. c. France du 17 décembre 2009.

incontestablement un type odieux de méfaits et que les en ants et autres personnes ulnéra les ont droit la protection e icace de l'État dans ce domaine.

Toutefois, elle parvient parfois à la solution inverse. Ainsi, dans l'affaire *Khelili c. Suisse*[108] qui concernait la classification d'une ressortissante française comme « prostituée » dans la base de données informatique de la police de Genève pendant cinq ans. Dans son arrêt, la cour a noté que la mention « prostituée » comme profession avait été supprimée de la base de données informatisée de la police, mais que cette expression, jointe aux affaires pénales en relation avec les plaintes déposées contre la requérante, n'avait pas été corrigée. Cette expression figurait donc toujours dans les fichiers informatiques de la police. La Cour a donc conclu que la mémorisation, dans le dossier de police, d'une donnée à caractère personnel, prétendument erronée, avait violé le respect de la vie privée de Mme Khelili et elle a estimé que le maintien de la mention « prostituée » pendant des années n'était ni justifié, ni nécessaire dans une société démocratique.

Cette multiplication des fichiers est une constante des sociétés contemporaines. A chaque fois qu'un crime est commis par un récidiviste (notamment dans les a aires de moeurs), on entend les commentaires de ceux qui déplorent l'absence de fichiers permettant d'identifier les coupables potentiels. D'où l'apparition de fichiers de plus en plus complets contenant, par exemple, des données biométriques. Une des affaires importantes à cet égard est l'affaire *S. et Marper c. Royaume-Uni*[109], qui concernait la conservation par les autorités des empreintes digitales, échantillons cellulaires et profils ADN des requérants après la conclusion, respectivement par un acquittement et par une décision de classement sans suite, des poursuites pénales menées contre eux.

Les empreintes digitales des requérants avaient été relevées dans le cadre de procédures pénales pour être ensuite enregistrées dans une base de données nationale, en vue de leur conservation permanente et de leur traitement régulier par des procédés automatisés à des fins d'identification criminelle.

La Cour a admis que la conservation des données relatives aux empreintes digitales et génétiques visait un but légitime, à savoir la détection et, par voie de conséquence, la prévention des infractions pénales. Elle a relevé que des empreintes digitales, des profils ADN et des échantillons cellulaires, constituaient toutes des données à caractère personnel au sens de la Convention du Conseil de l'Europe de 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Selon la Cour, la législation interne doit ménager des garanties appropriées pour emp cher toute utilisation de données caract re personnel ui ne serait pas con orme au garanties prévues à l'article 8 de la Convention. La nécessité de disposer de telles garanties se fait d'autant plus sentir lorsqu'il s'agit de protéger les données à caractère personnel soumises à un traitement automatique, en particulier lorsque ces données sont utilisées à des fins policières.

Quels sont les principes généraux dégagés par la Cour ?

L'intérêt des personnes concernées et de la collectivité dans son ensemble à voir protéger les données à caractère personnel, et notamment les données relatives aux empreintes digitales et génétiques, peut s'effacer devant l'intérêt légitime que constitue la prévention des infractions pénales. Cependant, compte tenu du caractère intrinsèquement privé de ces informations, la Cour se doit de procéder à un examen rigoureux de toute mesure prise par un État

[108] Arrêt Khelili c. Suisse du 18 octobre 2011.
[109] Arrêt S. et Marper c. Royaume-Uni du 4 décembre 2008.

pour autoriser leur conservation et leur utilisation par les autorités sans le consentement de la personne concernée.

Dans l'affaire S. et Marper, la Cour s'est donc penchée sur le point de savoir si la conservation des empreintes digitales et données ADN des requérants, qui avaient été soupçonnés d'avoir commis certaines infractions pénales, mais n'avaient pas été condamnés, était nécessaire dans une société démocratique. Elle a relevé que l'Angleterre, le pays de Galles et l'Irlande du Nord étaient les seuls ordres juridiques au sein de Conseil de l'Europe à autoriser la conservation illimitée des empreintes digitales et des échantillons et profils ADN de toute personne, quel que soit son âge, soupçonnée d'avoir commis une infraction emportant inscription dans les fichiers de la police.

Elle est parvenue à la conclusion que la protection offerte par l'article 8 serait affaiblie de manière inacceptable, si l'usage des techniques scientifiques modernes dans le système de la justice pénale était autorisé à n'importe quel prix et sans une mise en balance attentive des avantages pouvant résulter d'un large recours à ces techniques, d'une part, et des intérêts essentiels s'attachant à la protection de la vie privée, d'autre part. Tout État qui revendique un rôle de pionnier dans l'évolution de nouvelles technologies porte la responsabilité particulière de trouver le juste équilibre en la matière.

Dans cette affaire, la Cour a été frappée par le caractère général et indifférencié du pouvoir de conservation en vigueur en Angleterre et au pays de Galles. En particulier, les données en cause pouvaient être conservées quelles que soient la nature et la gravité des infractions dont la personne était à l'origine soupçonnée et indépendamment de son âge ; la conservation n'était pas limitée dans le temps ; et il n'existait que peu de possibilités pour un individu acquitté d'obtenir l'effacement des données de la base nationale ou la destruction des échantillons.

La Cour a estimé particulièrement préoccupant le risque de stigmatisation, qui découlait du fait que les personnes dans la situation des requérants, qui n'avaient été reconnus coupables d'aucune infraction et étaient en droit de bénéficier de la présomption d'innocence, étaient traitées de la même manière que des condamnés. Certes, la conservation de données privées concernant les requérants n'équivalait pas à l'expression de soupçons. Néanmoins, l'impression qu'avaient les

intéressés de ne pas être considérés comme innocents se trouvait renforcée par le fait que les données les concernant étaient conservées indéfiniment, tout comme celles relatives à des personnes condamnées, alors que celles concernant des individus n'ayant jamais été soupçonnés d'une infraction devaient être détruites.

En conclusion, la Cour a estimé que le caractère général et indifférencié du pouvoir de conservation des empreintes digitales, échantillons biologiques et profils ADN des personnes soupçonnées d'avoir commis des infractions mais non condamnées, tel qu'il a été appliqué aux requérants en l'espèce, ne traduisait pas un juste équilibre entre les intérêts publics et privés concurrents en jeu, et que l'État défendeur avait outrepassé toute marge d'appréciation acceptable en la matière. Dès lors, la conservation en cause s'analysait en une atteinte disproportionnée au droit des requérants au respect de leur vie privée et ne pouvait passer pour nécessaire dans une société démocratique. La Cour a conclu à l'unanimité qu'il y avait eu en l'espèce violation de l'article 8.

La divulgation des données

Une fois les données collectées et conservées, se pose une troisième question qui est celle de la divulgation de ces données. Elle est particulièrement sensible dans le domaine de la santé.

Une affaire importante à cet égard est l'affaire *Z c. Finlande*[110] à l'occasion de laquelle un tribunal avait condamné une personne, révélant par là même occasion la séropositivité de son épouse. La Cour a conclu à la violation de la Convention, en raison du rôle fondamental que joue la protection des données à caractère personnel dans le domaine de la santé. D'où l'importance de respecter le caractère confidentiel des informations qui y ont trait. Il y va de la confiance que les personnes accordent à leurs médecins et au système de santé en général. Dans le cas de l'affaire précitée, le caractère sensible de l'information divulguée rendait d'autant plus nécessaire le respect de la confidentialité, d'où le constat de violation auquel la cour est parvenue.

L'affaire *M.S. c. Suède*[111] a également permis à la Cour de rappeler que « la protection des données à caractère personnel, et spécialement des données médicales, revêt une importance fondamentale pour l'exercice du droit au respect de la vie privée et familiale garanti par l'article 8 de la Convention. Le respect du caractère confidentiel des informations sur la santé constitue un principe essentiel du système juridique de toutes les Parties contractantes à la Convention. Il est capital non seulement pour protéger la vie privée des malades, mais également pour préserver leur confiance dans le corps médical et les services de santé en général. La législation interne doit donc ménager des garanties appropriées pour empêcher toute communication ou divulgation de données à caractère personnel relatives à la santé qui ne serait pas conforme aux garanties prévues à l'article 8 de la Convention ». Toutefois, dans cette affaire, la Cour n'a pas constaté la violation de l'article 8. D'abord elle a noté que le dossier médical de Mme M.S. avait été communiqué par un organe public à un autre organe public, chargé d'apprécier si l'intéressée remplissait les conditions légales pour l'obtention d'une prestation qu'elle avait elle-même sollicitée. Elle a estimé que, pour décider s'il y avait lieu d'accueillir la demande d'indemnisation en cause, la Caisse avait un besoin légitime de vérifier les informations soumises par la requérante et de les confronter à celles que possédait le service de gynécologie. En l'absence d'informations objectives de la part d'une source indépendante, la Caisse aurait eu des difficultés à juger du bien-fondé de la demande. Par ailleurs, eu

[110] Arrêt Z.c. Finlande du 25 février 1997.
[111] M.S. c. Suède du 27 août 1997.

égard aux circonstances, la mesure litigieuse était soumise à des limitations importantes et assortie de garanties effectives et satisfaisantes contre les abus. Dans l'affaire Peck précitée, qui concernait la vidéosurveillance, la Cour est parvenue à un constat de violation de l'article 8 en raison de la divulgation dans les médias d'une séquence enregistrée dans la rue par une caméra de télévision en circuit fermé de la mairie, laquelle montrait le requérant en train de se trancher les veines.

L'effet horizontal de la jurisprudence impose d'ailleurs aux Etats de prendre des mesures pour renforcer la confidentialité des données personnelles en matière médicale. Ainsi, dans les affaires *Biriuk et Armonas c. Lituanie*[112], la Cour a insisté sur le fait qu'il est indispensable que le droit interne garantisse la confidentialité des informations concernant les patients et empêche toute divulgation de données personnelles, eu égard tout particulièrement à l'impact négatif de telles divulgations sur la propension d'autres personnes à se soumettre volontairement à des tests de dépistage du HIV et aux traitements appropriés.

L'accès aux données

Cet exposé ne serait pas complet si la question du droit d'accès de toute personne aux données la concernant n'était pas abordée. Cette question se trouve au centre de l'affaire *Gaskin*[113]. Dans cette affaire, le requérant avait été placé suite au décès de sa mère, sous l'assistance de la commune de Liverpool. Aux termes du Règlement de 1955 sur le placement des enfants, l'autorité locale se trouvait tenue de conserver certains dossiers confidentiels relatifs au requérant. Ce dernier, qui se plaignait d'avoir été maltraité, demanda la communication des notes et des dossiers établis par l'autorité locale pendant la période durant laquelle il fut pupille de l'assistance. Le gouvernement s'y opposait et déclarait, notamment, que le fonctionnement adéquat du service d'assistance à l'enfance dépendait des informations fournies par un certain nombre de personnes et qu'il était nécessaire de préserver l'anonymat de ces informateurs si on souhait qu'ils continuent de collaborer. La Cour a estimé qu'un système qui subordonnait l'accès aux dossiers à l'acceptation des informateurs, comme au Royaume-Uni, pouvait en principe être tenu pour compatible avec l'article 8 (art. 8), eu égard à la marge d'appréciation de l'État. Toutefois, quand un informateur n'est pas disponible ou refuse abusivement son accord, il doit sauvegarder les intérêts de quiconque cherche à consulter des pièces relatives à sa vie privée et familiale; il ne cadre avec le principe de

[112] Arrêts Biriuk et Armonas c. Lituanie du 25 novembre 2008.
[113] Arrêt Gaskin c. Royaume-Uni du 7 juillet 1989.

proportionnalité que s'il charge un organe indépendant, au cas où un informateur ne répond pas ou ne donne pas son consentement, de prendre la décision finale sur l'accès. Or il n'en allait pas ainsi dans l'affaire Gaskin. D'où le constat de violation opéré par la Cour.

Toutefois, le droit d'accès aux données personnelles n'est pas absolu et une marge d'appréciation a pu être laissée à l'État, lorsque le fichier auquel l'accès était sollicité avait pour objet de protéger la sûreté de l'État ou la prévention des infractions. Ainsi, on peut citer l'arrêt *Segersted-Wiberg c. Suède*[114] dans lequel les requérants demandaient tous en vain à consulter l'intégralité des dossiers les concernant détenus par la Sûreté suédoise. Leurs demandes furent rejetées au motif que le fait de leur donner accès à leurs dossiers pouvait compromettre la prévention des infractions pénales ou la protection de la sécurité nationale. Se fondant sur le chapitre 5, article 1 § 2, de la loi de 1980 sur le secret, les autorités et les juridictions nationales estimèrent qu'il était « difficile de déterminer si les informations [pouvaient] être révélées sans compromettre le but des mesures prises ou prévues, ou nuire à des opérations futures ». La Cour a reconnu qu' « un refus d'accès intégral à un fichier de police secret au niveau national est nécessaire lorsque l'État peut légitimement craindre que la communication de telles informations risque de compromettre l'efficacité du système de surveillance secrète destiné à protéger la sécurité nationale et à lutter contre le terrorisme ».

Mesdames, Messieurs,

Que ce soit au niveau national ou au niveau européen, la protection des données personnelles aura été considérablement améliorée depuis le début des années soixante-dix. Des instances et des mécanismes de protection ont été créés et des conventions ont été adoptées.

Je considère que le rôle joué par des commissions telles que la vôtre est crucial. Mais la Cour européenne des droits de l'homme y contribue également par les développements de sa jurisprudence. J'espère que mon exposé vous l'aura démontré. Je vous remercie.

[114] Arrêt Segerstedt-Wiberg c. Suède du 6 juin 2006.

brain&more

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