CNPD

COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Rapport annuel 2012

CNPD

COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Rapport annuel 2012

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 dispositions légales qui protègent les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée à l'égard du traitement des données à caractère personnel.

Superviser et assurer la transparence par :

- L'examen préalable des traitements soumis à autorisation ;
- La publicité réalisée au moyen du registre des traitements notifiés ;
- Les investigations suite à des plaintes ou effectuées 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 des 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'orientation thématiques.

Table des matières

1 Avant-propos

Le collège :
Pierre WEIMERSKIRCH, Gérard LOMMEL, Thierry LALLEMANG

Entrée en vigueur le 1er décembre 2002, la loi du 2 août 2002 est venue remplacer la loi du 30 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques en transposant dans la législation du Grand-Duché de Luxembourg les règles de la directive européenne de protection des données du 24 octobre 1995. Sous l'impulsion du ministre délégué aux Médias et à la Communication de l'époque, M. François Biltgen, qui s'était personnellement impliqué dans l'élaboration du projet de loi, une loi-cadre était adoptée qui allait encadrer de façon transversale toutes les activités numériques des secteurs privé et public avec un souci de juste équilibre entre société de l'information et libertés individuelles. Il s'agissait également de ne pas entraver la libre circulation des données à caractère personnel et par là,

le développement de certains domaines tels que le commerce électronique.

Le gardien du respect des droits fondamentaux dans le contexte du traitement des données, tant par les acteurs du secteur privé que par l'Etat et les organismes publics, est depuis 10 ans une autorité indépendante fonctionnant sous le statut d'établissement public, la Commission nationale pour la protection des données.
Sa mission comprend, outre le traitement des demandes de vérification et des plaintes des citoyens, la veille technologique et législative et les avis à donner au gouvernement et au législateur au sujet des projets de loi et mesures réglementaires susceptibles d'avoir des effets dans son domaine de compétence.

Ces dernières années, la Commission nationale se voit confrontée à de nouvelles problématiques et doit faire face à de nombreux défis découlant de la modification des modes de vie et de communication, tels que ceux inhérents aux risques particuliers d'atteinte à la vie privée des citoyens à travers les nouvelles technologies connectées, du recours de plus en plus fréquent à la biométrie, à la géolocalisation, au traçage et au profilage, à la publicité ciblée comportementale, de l'abus de confidentialité sur les réseaux sociaux, le droit à l'oubli sur Internet, la cybercriminalité, les pertes et fuites de données nominatives.

Les progrès technologiques rapides et la globalisation sont des phénomènes qui ont modifié en profondeur la manière de collecter, de consulter et d'utiliser les données de l'individu.
Pour adapter les législations européennes et nationales à cette évolution, la Commission européenne a présenté, le 25 janvier 2012, ses propositions visant à réformer le cadre légal règlementant la protection des données dans l'Union européenne. Il est également question d'empêcher l'abus d'utilisation des données privées des utilisateurs, aussi bien par des entreprises privées que par des autorités publiques.

La modernisation du cadre juridique européen, sous l'impulsion de la Vice-présidente de la Commission européenne Viviane Reding, se fonde sur trois axes :

- le renforcement des droits individuels à la transparence et des moyens d'action pour les citoyens et consommateurs ;
- une responsabilisation accrue des acteurs (combinée avec un allègement des contraintes administratives) ;
- l'augmentation des moyens d'action – aussi sous forme de pouvoirs de sanction – des autorités chargées d'assurer le respect des dispositions légales.

Cette réforme a pour but de mettre sur un pied d'égalité les citoyens européens, à travers la mise en place de règles communes à l'ensemble des Etats membres. En effet, le règlement s'appliquera à toutes personnes, autorités publiques et entreprises traitant des données personnelles des citoyens européens.

Les grands groupes américains comme Facebook, Google ou Apple sont donc directement concernés.
Cela permettra de renforcer les droits des consommateurs, offrira une sécurité juridique aux entreprises et augmentera la confiance des citoyens dans les entreprises.

Le projet ambitieux de la Commission européenne traite un certain nombre de situations sensibles apparues seulement récemment : la responsabilité des prestataires de cloud computing, les conditions d'un consentement valable et le droit à l'oubli sur Internet, la confiance des consommateurs dans les réseaux sociaux et le commerce électronique, les obligations des entreprises en cas de faille de sécurité, etc.

1 Avant-propos

Les propositions de la Commission européenne présentées le 25 janvier 2012 sont en cours d'examen par le Conseil et le Parlement européen.

Plus de 3000 amendements sont actuellement examinés au sein de la Commission LIBE. Même s'il est hasardeux de prévoir actuellement quelles seront les formules de compromis finales sur les aspects les plus âprement débattus, on peut être confiant que le paquet législatif composé d'un règlement européen à portée générale et d'une directive spécifique pour ce qui concerne les activités de la Police et de la Justice mettra fin à la fragmentation juridique actuelle et améliorera de façon substantielle la mise en œuvre efficace des principes de base de la directive de 1995 qu'elle reprend et développe en tenant compte des nouveaux défis. Le renforcement des moyens d'action des autorités de protection des données et l'accent mis sur l'« accountability » des acteurs compteront pour beaucoup dans la valeur ajoutée attendue de ce projet législatif communautaire par nos concitoyens en termes de droits individuels et de protection des internautes.

La révision du cadre légal européen était au cœur des discussions de la conférence de printemps *(« Spring Conference »)* des commissaires européens à la protection des données, organisée par la CNPD, dont le thème était *« La réforme de la protection des données européenne confrontée aux attentes ! »*.

Cette année-ci, ce fut au Luxembourg d'accueillir cette conférence dont le lieu d'organisation alterne annuellement. Du 2 au 4 mai 2012, cet événement à rayonnement international a réuni plus de 130 délégués des autorités de 38 pays ainsi que des représentants de la Commission européenne, du Conseil de l'Europe et de l'OCDE.

Pour les collaborateurs et services de la CNPD, l'année 2012 était également marquée par un changement de locaux : elle a emménagé le 6 décembre dans le nouveau bâtiment administratif de l'Etat à Esch-Belval.

Avec l'entrée en vigueur des modifications de la loi du 30 mai 2005 sur la protection de la vie privée dans le secteur des communications électroniques, la CNPD a vu ses missions s'étendre, notamment par l'introduction de l'obligation de lui notifier les violations et incidents touchant à la sécurité des données.


© Le Fonds Belval

Au cours des années à venir, la Commission nationale mettra davantage l'accent sur les investigations et contrôles sur place, mais elle servira également de guide aux acteurs publics et privés.

Sur ce premier point, la Commission nationale intervient en général après plainte reçue ou de sa propre initiative. Ce domaine n'est pas appelé à supplanter, mais à compléter les autres formes d'action déployées pour stimuler la culture de la protection des données au Luxembourg et le respect des droits des personnes concernées.

Car le but ultime de la mission de la CNPD, c'est le renforcement de la confiance des citoyens et consommateurs dans l'attitude des acteurs qui recueillent et utilisent des renseignements les concernant, dans les outils nouveaux et les évolutions de nos vies privées et professionnelles à l'ère numérique.

Luxembourg, le 24 mai 2013

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

2 Les activités en 2012

L'année 2012 en un coup d'œil

Janvier

16 - La CNPD émet un avis sur l' « identifiant unique »
25 - La Commission européenne présente ses propositions pour réformer le cadre légal règlementant la protection des données dans l'Union européenne
28 - La CNPD participe à la Journée de la protection des données avec le slogan *« Votre vie privée n'est pas privée de droits »*

Février

2 - Le G29[1] demande une suspension des nouvelles règles de confidentialité de Google
7 - La CNPD participe au Safer Internet Day avec le thème *« Génération connectée - Découvrir l'Internet ensemble, c'est plus sûr ! »*

Mars

23 - Le G29 publie sa prise de position détaillée sur le paquet législatif de réforme de la protection des données au niveau européen
28 - Le ministre des Communications et des Médias lance une consultation nationale sur la proposition de règlement de la Commission européenne. Elle donne notamment lieu à des avis de la FEDIL et de l'ABBL

Avril

24 - Le Groupe de Berlin publie un document de travail sur le cloud computing
27 - Le G29 met en garde contre les dérives potentielles des technologies biométriques et précise ses recommandations

Mai

2-4 - La CNPD organise la conférence annuelle des autorités européennes à la protection des données à Luxembourg
18 - La CNPD émet un avis complémentaire sur le surendettement

Juin

15 - La CNPD émet un avis complémentaire sur l'exploitation d'une base de données à caractère personnel relative aux élèves
26-27 - La CNPD donne un cours de formation sur la protection des données à l'INAP

Juillet

1 - Le G29 publie des lignes directrices sur le cloud computing
13 - La CNPD émet un avis concernant la mise en place d'un système de pétition électronique à la Chambre des députés

Août

15 - Les autorités de protection des données d'Allemagne et de Norvège ouvrent des enquêtes sur la fonction de reconnaissance faciale de Facebook

[1] Groupe de travail, institué par l'article 29 de la directive 95/46/CE sur la protection des données.

DELIBERATIONS

370
Délibérations adoptées

6
Avis relatifs à des projets ou propositions de loi ou mesures réglementaires

11
Agréments pour les chargés de la protection des données

FORMALITES PREALABLES

586
Notifications reçues

706
Demandes d'autorisation

5821
Déclarants (depuis 2002)

DEMANDES DE RENSEIGNEMENT

1697
Demandes

PLAINTES ET INVESTIGATIONS

133
Plaintes
(+15% par rapport à 2011)

18
Investigations

Septembre

20-21 - La CNPD participe à la conférence de l'Académie de Droit européen intitulée *« The proposed EU general data protection regulation - strengthening the EU's data protection architecture? »*

24 - La CNPD émet un avis sur l'avant-projet de règlement grand-ducal déterminant les modalités et les conditions de fonctionnement du registre national du cancer

Octobre

10 - La CNPD émet un avis sur l'organisation du casier judiciaire et les échanges d'informations extraites du casier judiciaire entre les Etats membres de l'Union européenne

25 - La CNPD effectue des contrôles auprès de deux communes dans le cadre du processus de remplacement de cartes d'identité défectueuses

30 - La CNPD participe à la conférence de l'Institut grand-ducal *« Zwischen Datenschutz und Informationsfreiheit. Die Aufgabe der Archive im 21. Jahrhundert. »*

Novembre

21-23 - La CNPD participe à la sixième conférence annuelle de l'Association francophone des autorités de protection des données personnelles

Décembre

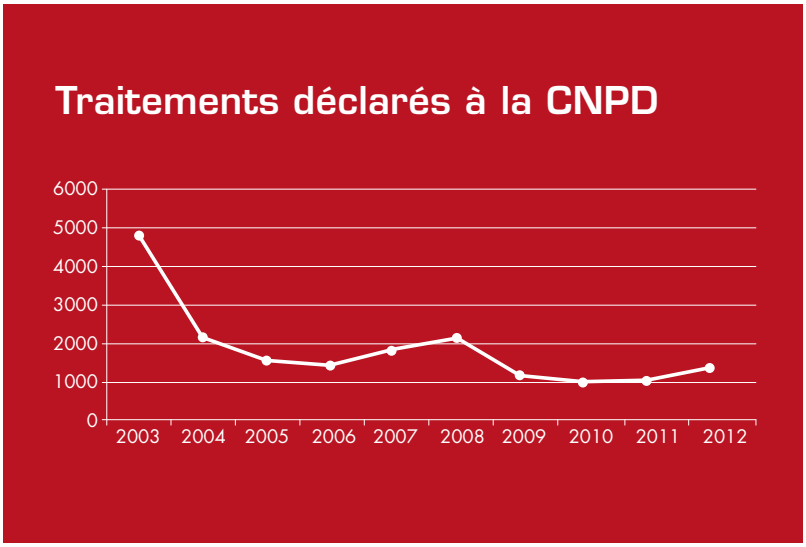
1 - La loi sur la protection des données est entrée en vigueur il y a 10 ans

6 - La CNPD s'installe dans le bâtiment administratif de l'Etat à Esch-Belval

17 - La CNPD rencontre la direction de l'agence eSanté pour discuter de l'état des lieux et de la progression des projets communs

17 - Le G29 charge la CNPD et la CNIL d'examiner les conditions contractuelles d'utilisation des services en ligne de Microsoft

2 Les activités en 2012



Le travail de la Commission nationale pendant l'année 2012 était centré principalement sur les activités suivantes :

- Le traitement des notifications et des demandes d'autorisation préalable ;
- 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

Le registre public

La loi prescrit la tenue d'un registre public par la Commission nationale. Ce registre permet au public de vérifier si telle ou telle entité a déclaré ses traitements et si elle est susceptible de détenir des informations les concernant.

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

Ne figurent pas dans le registre public les traitements de données exemptés de déclaration et ceux qui, soumis à l'autorisation préalable de la Commission nationale, n'ont pas été autorisés.

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 18.659. En tout, 5821 déclarants/responsables se sont ainsi conformés aux devoirs de déclaration imposés par la loi.

L'obligation de déclaration des fichiers et traitements de données à caractère personnel à la Commission nationale obéit à la volonté du législateur d'assurer à celle-ci une bonne visibilité des réalités sur le terrain et de permettre au public de consulter la liste des traitements déclarés dans le registre public[2].

Dès l'entrée en vigueur de la loi du 2 août 2002, la Commission nationale a reçu de nombreuses déclarations d'organisations soucieuses de se mettre en conformité avec la législation.

La diminution des traitements déclarés après 2008 peut s'expliquer par l'entrée en vigueur de la loi du 27 juillet 2007 (modifiant la loi du 2 août 2002). Celle-ci a introduit de larges exceptions au devoir de notification. Les responsables du traitement n'ont depuis lors plus besoin de notifier les traitements de données les plus courants qui comportent un risque négligeable d'atteinte à la vie privée des personnes physiques. Par ailleurs, certains traitements de données sensibles soumis à des conditions légales restrictives sont maintenant soumis à notification et n'exigent plus d'autorisation préalable.

La Commission européenne a d'ailleurs prévu dans son projet de règlement européen, présenté le 25 janvier 2012, de simplifier encore davantage le cadre réglementaire en supprimant certaines contraintes administratives, comme les obligations de notification pour les organismes qui traitent des données personnelles.

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 2012, 586 traitements ont été notifiés à la Commission nationale, ce qui représente une hausse par rapport à l'année précédente. 80% des notifications proviennent d'acteurs du secteur privé.

La finalité invoquée le plus souvent dans les notifications

[2] http://www.cnpd.public.lu/registre/application/index.html

Les activités en 2012

envoyées à la Commission nationale concerne l'administration du personnel et la gestion des ressources humaines. D'autres raisons citées pour traiter des données dans le cadre de notifications sont : la gestion de la clientèle, la comptabilité, la gestion des fournisseurs, les relations publiques ou encore la recherche (statistique, scientifique ou biomédicale).

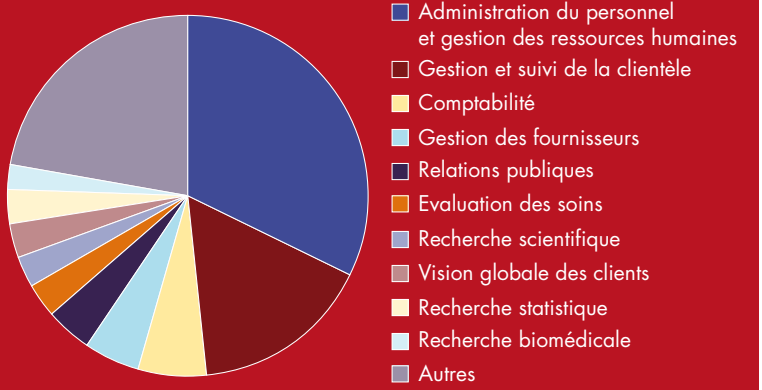
2.1.1.2 Les autorisations préalables

La loi sur la protection des données définit très précisément selon quelles modalités et dans quelles circonstances peut avoir lieu le traitement de données à caractère personnel. Le législateur a estimé que certains 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.

Les décisions de la Commission nationale visent à établir un juste équilibre entre différents intérêts, à savoir le droit des personnes concernées à jouir d'une vie privée intacte d'un côté et, de l'autre, l'intérêt légitime que peut avoir l'exploitant à mettre en oeuvre un traitement soumis à autorisation.

Le nombre des autorisations se maintient à un niveau élevé avec 706 demandes reçues en 2012. Ces dossiers nécessitent toujours une analyse détaillée et une appréciation pondérée au cas par cas.

Notifications

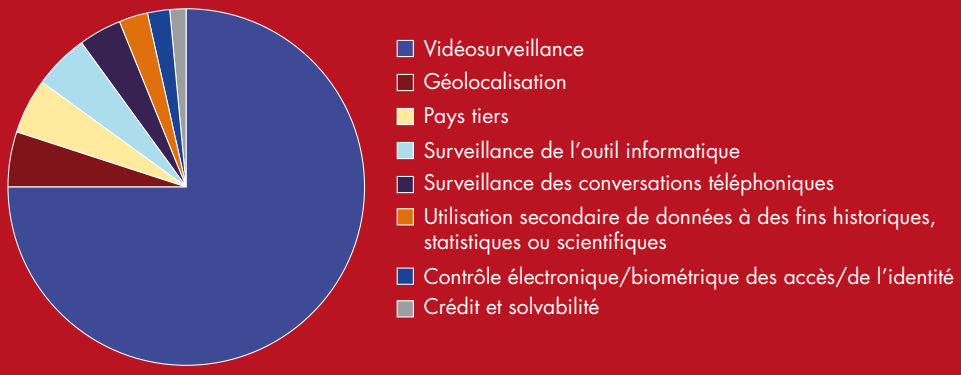


Quels sont les traitements soumis à autorisation ?

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



Parmi les autorisations préalables, la majorité des cas soumis à la Commission nationale concerne l'exploitation de caméras de surveillance. En 2012, les demandes concernant le contrôle des déplacements de véhicules et de personnes grâce à la géolocalisation ont augmenté par rapport à l'année précédente.

La loi prévoit par ailleurs 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.

En 2012, la Commission nationale a reçu 70 engagements formels de conformité.

2 Les activités en 2012

2.1.2 Transferts de données hors Union européenne

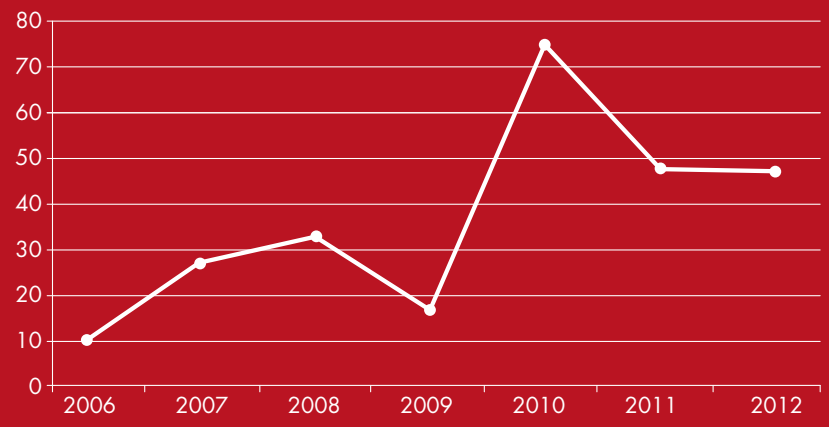
2.1.2.1 Autorisation en cas de transferts de données vers des pays tiers

En 2012, la Commission nationale a été saisie de 48 demandes d'autorisation en vue du transfert de données vers des pays tiers. Ce chiffre reste constant par rapport à l'année précédente.

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 aussi 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 lorsqu'elles externalisent leurs activités informatiques.

En 2012, la majorité des demandes émanaient d'entreprises du secteur financier. Les pays de destination étaient le plus souvent les Etats-Unis et l'Inde.

Tranferts 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), elle doit demander une autorisation préalable à la CNPD.

Cependant, 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[3] : 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.

2.1.2.2 Approbation de règles d'entreprise contraignantes

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

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

Les activités en 2012

- 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 2009, la Commission nationale a 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. L'approbation de ce code de conduite contraignant pour toutes les entités d'eBay et de PayPal à travers le monde a été préparée par la CNPD et a impliqué les autorités de protection des données de 14 autres Etats européens.

Au cours de l'année 2012, elle a passé en revue de façon approfondie les chartes de deux groupes internationaux avec siège à Luxembourg. Parmi celles-ci, la charte du groupe ArcelorMittal a été validée fin décembre par les 25 autres autorités impliquées des Etats membres où le groupe est implanté[4].

2.1.3 Les chargés de la protection des données

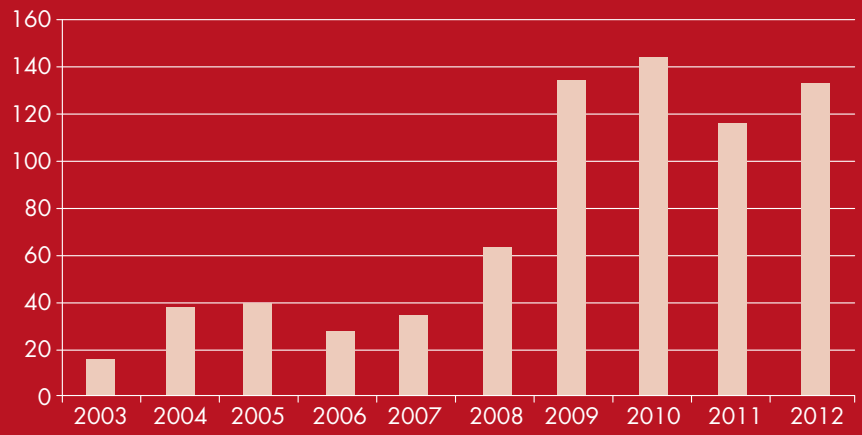
Le responsable du traitement peut nommer un chargé de la protection des données. Celui-ci a un rôle d'intermédiaire entre la CNPD et le responsable du traitement qu'ils conseillent et dont ils suivent les fichiers et procédures. Les organisations qui désignent un chargé, interne ou externe, n'ont plus besoin de notifier leurs traitements. Seuls les traitements soumis à autorisation continuent à faire l'objet de formalités auprès de la CNPD. Le chargé agit à la fois comme conseiller et investigateur. Dans certains cas, il peut, mieux que la Commission nationale, car plus près du responsable du traitement, guider celui-ci dans l'application des principes de la loi.

Depuis 2005, 68 entreprises, associations et organismes publics ont désigné un chargé de la protection des données.

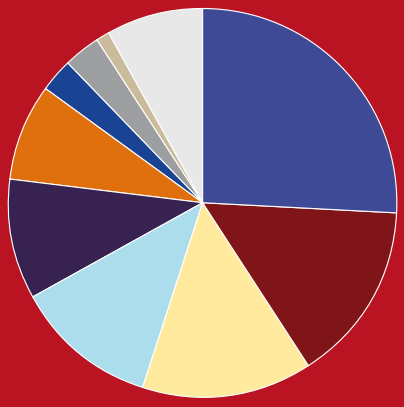
L'institution d'un chargé constitue un pas important dans le développement d'une culture de la protection des données dans les entreprises et organisations en question qui disposeront en interne des connaissances et

[4] Délibération n°1/2013 du 1er février 2013 de la Commission nationale pour la protection des données relative aux règles d'entreprise contraignantes du groupe ARCELORMITTAL.

Evolution du nombre de plaintes



Motif des plaintes



- Demande d'effacement ou de rectification non respectée
- Refus d'accéder aux données
- Transmission de données à des tiers
- Licéité de certaines pratiques administratives ou commerciales
- Vidéosurveillance
- Opposition à prospection ou plaintes contre le spam
- Licéité d'un traitement par l'employeur
- Durée de conservation
- Demande de coopération

de l'expertise nécessaires. Le projet de règlement européen actuellement discuté entend rendre obligatoire la présence d'un chargé de la protection des données au sein de chaque entreprise et organisme d'une certaine taille ou en fonction de la nature particulière des données traitées.

2.1.4 Demandes de vérification de licéité et plaintes

Le traitement des demandes de vérification de licéité et des plaintes de la part des citoyens a pris une importance croissante dans le travail de la Commission nationale. De plus en plus de citoyens font appel à la CNPD s'ils estiment qu'il y a entrave à la loi ou à l'exercice de leurs droits. En 2012, elle a été saisie de 133 plaintes.

Cette partie de son activité comporte un aspect international, dans la mesure où l'autorité de contrôle luxembourgeoise

2 Les activités en 2012

est compétente pour assurer le respect de la législation nationale par les sociétés multinationales offrant des services sur Internet et qui ont choisi d'établir leur siège européen à Luxembourg (eBay, PayPal, Skype, Microsoft, Amazon, …). La Commission nationale est ainsi fréquemment saisie de demandes émanant d'autorités de protection des données des autres Etats membres qui agissent au nom de leurs propres citoyens.

Les délais d'instruction peuvent varier de quelques jours à plusieurs mois, en fonction de la complexité du dossier et des recherches à effectuer dans le cadre de celui-ci, de la qualité des réponses apportées par le responsable du traitement en cause et des actions entreprises par la Commission nationale (contrôle sur place, mise en demeure, transmission au parquet…).

Ci-après sont énumérés quelques exemples de traitement de plaintes, demandes et questions du public qui permettent

Intervention auprès d'une commune

La Commission nationale a été saisie d'une plainte concernant l'envoi par une commune des fiches de retenue d'impôt pour l'année 2012. Un citoyen a informé la CNPD que la fenêtre de l'enveloppe faisait apparaître non seulement les nom et prénom du destinataire, mais également l'état civil, la date de mariage, le statut professionnel ainsi que le numéro de matricule.

Il en résulte que l'obligation de confidentialité des données auquel la commune est tenue n'était plus assurée, car ces données ont pu être vues par des tiers non autorisés.

Après l'intervention de la CNPD, la commune concernée a immédiatement réagi en mettant en œuvre les mesures nécessaires afin qu'une telle diffusion ne se reproduise plus.

d'illustrer l'action de la Commission nationale face aux difficultés rencontrées par les personnes concernées.

Demande d'effacement ou de rectification des données non respectée

Il s'agit des cas où la Commission nationale a été saisie par des particuliers lorsqu'ils ont rencontré des difficultés à faire supprimer ou modifier leurs données auprès d'un responsable du traitement.

Cela inclut toutes les demandes de clôture de comptes auprès de commerces ou de services en ligne, les demandes d'effacement de données (données clients, données de candidature, données bancaires, etc.) ou encore les plaintes qui concernent la transmission erronée de données à des tiers (contrats, livraisons, documents, etc.).

Refus d'accéder aux données

Dans de nombreux cas, la Commission nationale a dû prêter assistance aux plaignants, soit parce qu'ils n'ont pas réussi à faire valoir leur droit d'accès auprès du responsable du traitement, soit parce que la réponse fournie par le responsable du traitement était insuffisante.

A ce titre, la fermeture d'un compte ou l'exclusion d'un client par les commerces de biens ou de services en ligne est un problème récurrent.

Dans ces dossiers, en cas de motifs insuffisamment transparents, la Commission nationale a dû agir afin que les

Cas d'espèce concernant la prospection non sollicitée par l'entreprise des P&T pour les envois du catalogue IKEA

La Commission nationale avait été saisie d'une demande de vérification de licéité concernant l'envoi systématique par l'entreprise des Postes et Télécommunications (« EPT ») à toutes les personnes disposant d'une boîte aux lettres munie de « Keng Reklammen w.e.g. » (ou « Pas de publicité svp ») de courriers de prospection demandant aux destinataires s'ils souhaitaient commander le catalogue IKEA (en apposant une étiquette spécifique sur leurs boîtes aux lettres).

Même si la CNPD n'avait pas remis en cause la licéité du fichier général des clients des services postaux reprenant de manière spécifique les utilisateurs ayant marqué leur opposition à recevoir des envois non adressés, elle était d'avis que l'utilisation qui en avait été faite dans le cas présent constituait un détournement de finalité. En effet, la loi modifiée du 2 août 2002 prévoit que le responsable du traitement doit s'assurer que les données à caractère personnel ne soient pas traitées de manière incompatible avec les finalités initialement déclarées.

Suite à cette demande de vérification de licéité, la Commission nationale avait appelé l'EPT à s'abstenir à l'avenir de mettre en œuvre de telles pratiques, au profit d'IKEA ou de toute autre firme.

2 Les activités en 2012

personnes concernées puissent prendre connaissance de toutes les données en cause ayant servi à justifier ces décisions.

Transmission de données à des tiers

La Commission nationale a également été saisie d'une dizaine de plaintes concernant des données personnelles transmises à des tiers non autorisés.

Elle a notamment dû intervenir dans les cas suivants :

- une ONG a transmis les données personnelles de ses membres à une agence de marketing sans l'autorisation des personnes concernées ;
- un garage a transmis les numéros de téléphone de ses clients à une entreprise qui fait des enquêtes de satisfaction, sans l'accord préalable de ces clients ;
- un service en ligne a transmis un courriel à une centaine d'adresses e-mails qui étaient visibles par tous les destinataires.

Licéité de certaines pratiques administratives ou commerciales

Il s'agit des demandes de vérification de licéité adressées à la Commission nationale, qui ont trait à certaines pratiques commerciales ou administratives.

Opposition à prospection ou plaintes contre le SPAM

Lorsque les plaignants ont des difficultés à faire valoir leur droit d'opposition ou estiment ne pas avoir consenti à être prospectés, ils en réfèrent à la Commission nationale.

En effet, l'article 30 de la loi modifiée du 2 août 2002 confère aux personnes concernées le droit de s'opposer, sur demande et gratuitement, au traitement les concernant envisagé par le responsable du traitement des données à des fins de prospection. En outre, l'article 11 de la loi modifiée du 30 mai 2005 confère ce même droit aux personnes concernées pour des envois de prospection par courrier électronique.

Les règles en droit luxembourgeois en matière de prospection par e-mail sont claires. L'abonné doit préalablement consentir à cette prospection (principe de l'« opt-in »), à moins que le fournisseur n'ait obtenu les

Les propos d'un salarié enregistrés en cachette par un collègue de travail

Un syndicat avait informé la CNPD qu'au sein d'une société, un salarié avait enregistré en cachette divers propos tenus par ses collègues de travail, pour ensuite les transmettre au service des ressources humaines. Par ailleurs, les caméras vidéo installées à l'intérieur de l'entreprise n'avaient pas été autorisées par la Commission nationale. Dans cette affaire, la Commission nationale a dû rappeler au plaignant qu'un enregistrement en cachette effectué par un salarié à l'insu d'un ou de plusieurs autres salariés n'est pas à considérer comme un « traitement de données à caractère personnel » au sens de la loi modifiée du 2 août 2002, étant donné que le salarié en question n'est pas « responsable du traitement » (personne qui détermine les finalités et les moyens d'un traitement de données à caractère personnel). Par contre, l'enregistrement des images ou de sons effectué par l'employeur en tant que responsable du traitement, à des fins de surveillance sur le lieu du travail, tombe dans le champ de la loi.

De tels enregistrements sont avant tout susceptibles de violer l'article 2 de la loi du 11 août 1982 concernant la protection de la vie privée *(« Est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 euros à 5.000 euros, ou d'une de ces peines seulement, quiconque a volontairement porté atteinte à la vie privée d'autrui (…) en écoutant ou faisant écouter, en enregistrant ou faisant enregistrer, en transmettant ou faisant transmettre au moyen d'un appareil quelconque des paroles prononcées en privé par une personne, sans le consentement de celle-ci ».)*

Les activités en 2012

données de son client dans le cadre d'une vente antérieure d'un produit ou d'un service. Même dans ce cas-là, l'abonné peut toujours et en tout état de cause s'opposer à toute sorte de prospection ultérieure (principe de l'« opt-out »).

A ce titre, la Commission nationale a dû intervenir à plusieurs reprises au courant de l'année 2012 :

- dans le cas d'un garagiste qui se servait d'une clientèle de son partenaire commercial afin de prospecter des personnes non clientes à lui ;
- dans le cas d'envois de courriels non sollicités par des commerces en ligne ;
- dans les cas de non-respect d'opposition aux courriels de prospection, notamment par les commerces en ligne et, de plus en plus fréquent, par des sites de rencontres.

Licéité d'un traitement par l'employeur

La Commission nationale a été saisie de plusieurs plaintes, soit par les délégués du personnel, soit par les employés eux-mêmes qui mettaient en cause le traitement de données effectué par leur employeur, notamment en matière de surveillance sur le lieu du travail.

Une telle surveillance (vidéosurveillance, géolocalisation, accès biométriques, surveillance des outils informatiques, surveillance des conversations téléphoniques, etc.) est, sauf cas d'exception, soumise à autorisation préalable de la Commission nationale.

En 2012, la Commission nationale a dû intervenir dans plusieurs affaires de surveillance sur le lieu de travail. A ce titre, elle a constaté une légère hausse d'installations non autorisées de systèmes de géolocalisation dans les voitures de service ou l'utilisation de tels systèmes à d'autres fins que celles pour lesquelles une autorisation avait été accordée.

La Commission nationale est encore régulièrement saisie de la question des enregistrements des communications téléphoniques, notamment par les entreprises commerciales. Elle rappelle que ces enregistrements ne peuvent être effectués que dans le cadre des usages professionnels licites, afin de se ménager une preuve d'une transaction commerciale ou de toute autre communication commerciale. Ces enregistrements doivent être limités aux seuls postes téléphoniques des départements concernés et tant les salariés que les correspondants doivent en être informés au préalable.

En ce qui concerne l'utilisation des outils informatiques à titre privé par les salariés, la Commission nationale a dû rappeler à plusieurs reprises que les employeurs n'ont pas le droit de contrôler l'usage de ces outils de manière continue, sauf exception légale. L'employeur n'a pas non plus le droit de prendre connaissance des courriels marqués comme privés. En outre, quel que soit l'outil informatique, la surveillance doit toujours être graduée *(« progressive Kontrollverdichtung »)*, c'est-à-dire que l'employeur doit d'abord procéder à une surveillance ponctuelle pendant laquelle les salariés ne sont pas identifiés.

Si des indices et soupçons sont détectés, l'employeur pourra intensifier sa surveillance et faire des analyses individualisées permettant d'identifier les salariés.

2.1.5 Contrôles et investigations

La Commission nationale est dotée de pouvoirs d'investigation et d'intervention nécessaires à l'exercice de ses missions. Pour veiller au respect de la réglementation applicable en matière de protection des données, elle dispose d'un accès direct aux locaux où a lieu le traitement autres que les locaux d'habitation ainsi qu'aux données faisant l'objet du traitement.

Pour l'année 2012, la Commission nationale a sensiblement renforcé son action dans ce domaine. Cela ne vise non seulement les contrôles ponctuels qui sont pratiqués lorsque des cas d'atteinte à la législation sur la protection des données lui sont signalés, mais aussi de façon plus générale un but de prévention.

Au total, la Commission nationale a effectué 18 contrôles et investigations en 2012, notamment dans le cadre de plaintes en matière de vidéosurveillance. Elle est également intervenue suite à l'intrusion dans la base de données médico-sportive de l'Etat en janvier 2012, ou encore pour vérifier si la durée de conservation des photos a été respectée lorsque des cartes d'identité défectueuses ont dû être remplacées auprès des communes.

2 Les activités en 2012

2.1.5.1 *Investigation au « Centre Médico-Sportif »*

En janvier 2012, une personne avait pu accéder à la base de données du « service médico-sportif » du Ministère des Sports, contenant des données à caractère personnel de plus de 48.000 personnes.

En présence de Monsieur François Biltgen, ministre des Communications et des Médias, et de la Commission nationale, les trois commissions parlementaires concernées se sont penchées sur ce dossier en date du 17 février 2012.

Après investigation, le ministre a pu confirmer qu'il s'agissait en l'espèce d'une erreur humaine et non d'un acte de piratage. L'individu en question avait simplement consulté le post-it collé sur un écran contenant le login et le mot de passe d'un membre autorisé du service médico-sportif.

L'analyse de l'incident au Centre par la Commission nationale a pourtant révélé quelques insuffisances. Selon le président de la CNPD, Gérard Lommel, cette affaire « *montre bien que la sécurité des données et des infrastructures est un enjeu de tous les jours* »[5] et que cet incident « *doit être mis à profit pour davantage sensibiliser les responsables et les collaborateurs en charge de fichiers et d'infrastructures* ».

D'où la création d'un Cyber Security Board qui a recommandé au gouvernement de continuer à accélérer le plan d'action concernant la sensibilisation et la formation des agents de l'Etat en matière de sécurité informatique. Monsieur le ministre Biltgen s'est aussi prononcé en faveur d'une généralisation obligatoire du système d'authentification forte pour les applications sensibles, notamment via l'application Luxtrust. Depuis mai 2012, la banque de données du service médico-sportif fonctionne avec un tel système. Cette banque de données ne peut donc plus être accédée moyennant un simple mot de passe. En outre, les personnes autorisées à accéder à cette banque de données ont reçu une formation appropriée.

Monsieur Lommel, pour sa part, estime que « *toutes ces mesures sont tout à fait bienvenues et sont de nature à favoriser la prise en compte des risques pour une réaction rapide* ». La question de la sécurité évolue constamment et les campagnes de sensibilisation et de formation entamées par le gouvernement sont à saluer dans ce contexte.

La CNPD a également préconisé – pour certaines banques de données particulièrement grandes et sensibles – la nomination

[5] Interview avec Le Quotidien, 27 janvier 2012.

d'un chargé de la protection des données qui assurerait en interne une mission de veille. Il existe actuellement des chargés de la protection des données auprès de la Banque Centrale du Luxembourg, du STATEC, de l'entreprise des Postes et Télécommunications, du Centre de recherche public de la Santé et du CEPS.

Recensement des banques de données gérées par l'Etat et amélioration de leur sécurisation

Suite à cette intrusion dans la base de données du service médico-sportif de l'Etat, le Cyber Security Board a décidé de mettre en place un groupe de travail chargé d'une mission de recensement des banques de données gérées par l'Etat, dans le but d'en optimiser la sécurité. Par la suite, le Conseil de gouvernement avait validé cette approche.

En mai 2012, le Cyber Security Board avait envoyé à tous les ministères une liste des informations devant être fournies en relation avec l'exploitation des banques de données. Le groupe de travail est sur le point de finaliser ces travaux qui lui permettront de définir des critères sécuritaires objectifs, afin de pouvoir opérer une identification prioritaire des bases de données sensibles.

Grâce à ce ciblage stratégique, une évaluation détaillée des données figurant dans les différentes banques de données de l'Etat, ainsi que de leurs modalités de fonctionnement et d'accès pourra être opérée.

Une nouvelle mission de ce groupe de travail consiste encore dans la définition de consignes obligatoires en matière de sécurisation et quant à l'accès des gestionnaires des banques de données. Ces règles varieront en fonction du degré de sensibilité des données gérées.

A côté d'une généralisation du système d'authentification forte auprès de l'Etat et de la formation des responsables des banques de données ainsi que des utilisateurs, le Cyber Security Board a encore décidé qu'à l'avenir, la création de toute nouvelle banque de données sera accompagnée d'une charte précisant les consignes à respecter du côté du gestionnaire et des utilisateurs.

2.1.5.2 Contrôles auprès de deux communes

Par circulaire du 11 octobre 2012, le ministre de l'Intérieur et à la Grande Région avait fait savoir qu'un certain nombre de cartes d'identité délivrées entre avril 2010 et décembre 2011 présentaient un défaut de lisibilité sous la lumière UV et devaient être remplacées auprès des communes.

Avant l'envoi de cette circulaire, la Commission nationale avait été consultée par ledit ministère, alors qu'il est apparu que plusieurs communes avaient tout simplement conservé les documents (données) de base des demandes d'obtention d'un titre d'identité. La Commission nationale s'est prononcée sur la licéité de cette pratique par rapport aux dispositions de la loi modifiée du 2 août 2002, en particulier en ce qui concerne la conservation des photos étant donné que celles-ci, prises dans le cadre de cette finalité et par opposition aux simples données textuelles, constituent des données biométriques particulièrement sensibles.

Position de la CNPD

Alors qu'une conservation illimitée de ces photos n'est pas admissible, la Commission nationale a estimé que la conservation dans les dossiers en version papier pourrait se justifier pendant un certain temps pour des besoins administratifs. Une réutilisation en vue de la confection d'une nouvelle carte pour remplacer une ancienne carte défectueuse n'apparaît donc pas comme disproportionnée. Par conséquent, l'utilisation des données issues des demandes

Les activités en 2012

des cartes d'identité pour les années 2010 à 2012 est licite aux yeux de la CNPD.

Par contre, une conservation des photos sous format électronique au-delà du délai strictement nécessaire pour la fabrication et la vérification des titres d'identité émis ne peut pas être acceptée. Dans sa délibération n°228/2008 du 11 août 2008 relative à la demande d'autorisation préalable du ministère des Affaires étrangères quant au traitement des données biométriques, la Commission nationale s'était prononcée dans le même sens. Elle avait estimé à l'époque que les données biométriques numérisées ne peuvent être conservées plus de deux mois après la délivrance du passeport biométrique.

Le projet de loi n°6330[6], qui prévoit des photos numérisées pour les nouvelles cartes d'identité électroniques, dispose également à l'art. 16, paragraphe 3 que « *les données biométriques ne sont conservées que pendant une durée de deux mois après la délivrance de la carte d'identité* ».

Les citoyens auraient manifesté leur incompréhension, si on leur avait imposé une démarche supplémentaire pour faire de nouvelles photos, alors que les anciennes étaient toujours disponibles. La durée de validité figurant sur la nouvelle carte correspond à celle de la carte défectueuse qui est remplacée.

Contrôles du processus de remplacement des cartes d'identité défectueuses

Par la suite, la Commission nationale a effectué des contrôles auprès de deux communes pour examiner le processus de renouvellement des cartes d'identité défectueuses et pour s'assurer que ses recommandations avaient été prises en compte.

Lors de ces contrôles, la Commission nationale a recherché la présence éventuelle de photos numérisées dans les bases de données desdites communes. Elle a constaté qu'il n'avait été procédé à aucun moment à une numérisation ou une sauvegarde informatique de la photo des titulaires de cartes d'identité. Les responsables des communes contrôlées ont assuré et montré aux agents de la CNPD que les dossiers de demandes de titre d'identité étaient conservés de façon sécurisée et avec accès strictement limité. Le risque d'abus est donc beaucoup moindre que dans le cas d'un recours à des photos numérisées conservées dans des fichiers électroniques.

La prolifération des bases de données comprenant des données biométriques engendre

[6] Projet de loi relative à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité, aux registres communaux des personnes physiques.

par nature un risque accru d'interconnexion et d'utilisation abusive de données à caractère personnel. La CNPD, à l'instar des autorités de protection des données des autres pays européens, s'emploie résolument à empêcher une telle évolution.

La Commission nationale se prononcera sous peu de manière plus générale sur la question de la durée de conservation des photos au format papier et électronique.

2.1.5.3 Vidéosurveillance

La Commission nationale est intervenue à plusieurs reprises dans le cadre de plaintes en matière de vidéosurveillance.

Caméras filmant les propriétés avoisinantes ou la voie publique

Vu le nombre croissant de sociétés de sécurité, la prospection en la matière et la possibilité d'acquérir des appareils de surveillance à bon prix et faciles d'usage, de plus en plus de particuliers installent des caméras de surveillance sur leur propriété pour se protéger contre d'éventuels cambriolages ou pour faciliter la recherche d'auteurs d'actes de vandalisme ou d'autres délits.

Ces caméras peuvent toutefois porter atteinte au respect de la vie privée des passants ou voisins, lorsqu'elles filment également l'espace public ou les propriétés avoisinantes. Plusieurs citoyens ont saisi la Commission nationale parce qu'ils étaient gênés par de telles caméras, se sentaient espionnés de manière continue sur leur propre propriété et entravés dans leur liberté de mouvement.

Même si la loi modifiée du 2 août 2002 énumère de manière limitative les cas dans lesquels une vidéosurveillance peut être considérée comme légitime, et même si la loi ne s'applique pas lorsqu'un système de vidéosurveillance est mis en œuvre « *dans le cadre exclusif de ses activités personnelles et domestiques* », la Commission nationale ne saurait néanmoins tolérer qu'une personne privée filme la propriété voisine ou la voie publique.

A ce titre, lorsqu'elle est saisie de telles affaires, la CNPD décide dans la majorité des cas de procéder à un contrôle sur place, notamment lorsqu'elle ne reçoit aucune réponse de la personne ayant mis en place une telle surveillance. Si elle estime que les caméras visent bien la propriété avoisinante ou la voie publique, ou si elle constate que le responsable du traitement prétend ne pas outrepasser sa propriété mais « s'amuse » à changer les angles de vue de ses caméras, la Commission nationale n'hésitera pas à transmettre ces faits au Parquet en soulignant l'importance à faire cesser ces troubles, qui constituent dans la majorité des cas des infractions tant à la loi du 11 août 1982 concernant la vie privée qu'à la loi modifiée du 2 août 2002.

Vidéosurveillance sans autorisation

La Commission nationale a également été saisie par des

Les activités en 2012

salariés s'interrogeant sur la licéité de caméras placées dans leur entreprise.

Vérification faite, il est apparu dans plusieurs cas que la vidéosurveillance était opérée en violation des dispositions de la loi modifiée du 2 août 2002.

Dans ces dossiers, la Commission nationale a demandé aux responsables du traitement de cesser immédiatement l'utilisation de la vidéosurveillance et les a sommés de se mettre en conformité avec la loi.

2.1.6 Violations de données à caractère personnel dans le secteur des communications électroniques

La Commission nationale intervient également lorsqu'apparaissent des failles de sécurité dans le secteur des communications électroniques, notamment pour garantir la confidentialité des utilisateurs.

Depuis l'entrée en vigueur de la loi du 28 juillet 2011[7], les

[7] 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.

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 2012, la Commission nationale a adopté au cours de 27 séances 370 délibérations, dont :

- 353 autorisations ;
- 6 avis relatifs à des projets ou propositions de loi et mesures réglementaires ;
- 11 agréments pour les chargés de la protection des données.

fournisseurs d'accès à Internet et les opérateurs de téléphonie doivent avertir immédiatement la Commission nationale en cas de survenance d'une violation de la confidentialité des données. Si un tel incident est susceptible d'affecter défavorablement leurs abonnés, alors ceux-ci devront également être informés.

La loi définit la violation de données à caractère personnel comme une « *violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés de données à caractère personnel transmises, stockées ou traitées d'une autre manière en relation avec la fourniture de services de communications électroniques accessibles au public* ». En 2012, la CNPD n'a reçu aucune notification de violation des données personnelles.

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

Cette obligation s'inscrit dans un processus de responsabilisation accrue des acteurs en charge de données personnelles. Le projet de règlement européen relatif à la protection des données prévoit la généralisation de cette obligation de notification pour l'ensemble des responsables du traitement.

2.2 Avis et recommandations

L'avis de la Commission nationale est de plus en plus demandé en ce qui concerne les projets de loi ou mesures réglementaires ayant trait à la protection des données ou ayant un impact sur la vie privée des citoyens. Ces dispositions deviennent de plus en plus complexes et nécessitent une appréciation soigneuse et pondérée des intérêts en présence, et une connaissance des aspects juridiques relevant de domaines fortement différents.

En 2012, la Commission nationale a émis six avis dans le cadre de projets de loi ou de règlements grand-ducaux :

1. Avis à l'égard du projet de loi n°6330 relatif à l'identification des personnes physiques, à la carte d'identité, aux registres communaux des personnes physiques et portant modification de 1) l'article 104 du Code civil ; 2) la loi modifiée du 22 décembre 1886 concernant les recensements de population à faire en exécution de la loi électorale ; 3) la loi modifiée du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales ; 4) la loi communale modifiée du

Les activités en 2012

13 décembre 1988 ; 5) la loi électorale modifiée du 18 février 2003 (Délibération n°1/2012 du 16 janvier 2012)

2. Avis complémentaire relatif au projet de loi n°6021 portant modification : 1. de la loi modifiée du 8 décembre 2000 sur le surendettement, 2. de l'article 2016 du Code civil, 3. des articles 1er et 4 du Nouveau Code de procédure civile et 4. de l'article 536 du Code de commerce sur le surendettement et modifiant certaines dispositions légales (Délibération n°143/2012 du 18 mai 2012)

3. Avis complémentaire relatif au projet de loi n°6284 portant sur l'exploitation d'une base de données à caractère personnel relative aux élèves (Délibération n°156/2012 du 15 juin 2012)

4. Avis concernant la mise en place d'un système de pétition électronique à la Chambre des députés (Délibération n°200/2012 du 13 juillet 2012)

5. Avis relatif à l'avant-projet de règlement grand-ducal déterminant les modalités et les conditions de fonctionnement du registre national du cancer et modifiant le règlement grand-ducal du 20 juin 1963 rendant obligatoire la déclaration des causes de décès (Délibération n°239/2012 du 24 septembre 2012)

6. Avis à l'égard du projet de loi n°6418 relatif à l'organisation du casier judiciaire et aux échanges d'informations extraites du casier judiciaire entre les Etats membres de l'Union européenne et modifiant le Code d'instruction criminelle (Délibération n°245/2012 du 10 octobre 2012)

2.2.1 L'identifiant unique des personnes

En date du 16 janvier 2012, la Commission nationale s'est prononcée au sujet du projet de loi n°6330 relatif à l'identification des personnes physiques, à la carte d'identité et aux registres communaux des personnes physiques. Ce projet de loi constitue la fusion, avec des modifications, des projets de lois n°5949 (registres communaux des personnes physiques) et n°5950 (identification des personnes physiques, registre national des personnes physiques, carte d'identité).

S'étant déjà exprimée sur les deux anciens projets de loi[8], la Commission nationale a regretté

[8] La Commission nationale avait déjà rendu son avis sur le projet de loi n°5949 en date du 10 mars 2009 (délibération 48/2009), puis sur le projet de loi n°5950 en date du 14 février 2011 (délibération 11/2011).

que ses observations n'aient pas été prises en compte dans leur totalité. Dans ce dernier avis, elle a limité son analyse aux points traités dans les avis précédents et qui ont fait l'objet de modifications.

Quel numéro d'identification nationale ?

Selon le projet de loi, le numéro d'identification nationale sera composé, à partir de la date de naissance, d'une plage séquentielle unique par date de naissance et de deux numéros de contrôle.

La Commission nationale a conclu dans son avis que l'identification des personnes physiques telle qu'elle est envisagée ne présente pas les garanties appropriées, telles qu'exigées par la directive 95/46/CE. Elle a notamment regretté que le projet de loi n'ait pas répondu aux ambitions de vouloir modifier et améliorer le système complètement dépassé mis en place en 1979. En outre, elle estime que l'usage de l'identifiant unique aurait dû s'accompagner de solutions technologiques novatrices pour renforcer les garanties destinées à éviter des risques d'abus.

Il est vrai que l'utilisation d'un système reposant sur un numéro d'identification unique pour l'ensemble ou pour une partie des démarches administratives peut présenter des avantages. Chaque citoyen qui se voit attribuer un numéro d'identification peut ainsi le mémoriser, car la structure de ce numéro d'identification est connue au préalable (la date de naissance, le sexe,…). De plus, il n'a pas à se souvenir de plusieurs numéros d'identification, un numéro unique facilitant ses démarches auprès de différentes administrations.

La Commission nationale n'est pourtant pas convaincue que la plus-value liée au fait que les individus peuvent facilement se souvenir de leur numéro d'identification national soit suffisamment importante pour justifier les risques qu'elle peut comporter. En effet, n'importe qui pourra composer le numéro d'identification d'une autre personne : s'il en connaît la date de naissance, il n'a qu'à se souvenir des derniers chiffres. Le risque majeur réside essentiellement dans les interconnexions de fichiers, c'est-à-dire la possibilité de regrouper des données contenues dans divers fichiers et de retracer tous les actes de la vie courante d'un administré qui deviendrait quasiment transparent *(« Gläserner Bürger »)*.

Si la loi du 31 mars 1979[9] avait prévu des garanties adéquates dans le domaine de l'identification numérique des personnes, celles-ci sont désormais insuffisantes. Le numéro d'identification est souvent demandé et utilisé en dehors de démarches administratives, par des personnes non autorisées et/ou pour des finalités autres que celles autorisées par la loi du 31 mars 1979. De plus, le numéro d'identification permet de faire le lien entre plusieurs fichiers.

La Commission nationale a encore noté avec regret que le projet de loi ne prévoie plus le remplacement du numéro actuel faisant ressortir la date de naissance et le sexe de l'individu concerné par un numéro d'identification non parlant, comme l'envisageait le texte initial du projet de loi n°5950. Lors des nombreuses réunions avec les représentants des ministères impliqués et dans son avis écrit, elle a présenté l'évolution récente des systèmes dans des pays qui utilisaient précédemment le même type de numéro d'identification parlant et qui ont modifié récemment leur législation pour l'adapter au souci de protection de la sphère privée en l'entourant de garanties technologiques performantes. Ainsi, à titre d'exemple, l'Autriche utilise un système plus respectueux des droits des personnes tout en permettant les échanges informatiques d'informations entre administrations utilisant des numéros distincts pour une

[9] Loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales.

seule et même personne. Quant à la Suisse, elle a fait le choix de l'adoption d'une nouvelle structure d'identifiant unique à treize chiffres et totalement aléatoire, qui ne fournit donc pas d'information parlante sur son titulaire.

Demandes d'information de tiers sur les données figurant dans les registres communaux

La Commission nationale avait fait part du nombre important de demandes émanant de communes qui souhaitaient connaître les suites qu'elles devaient donner à des demandes de communication d'adresse portant sur une personne en particulier et formulées par des tiers. Elle a régulièrement dénoncé le vide juridique de la situation actuelle et elle a demandé à ce que le législateur règle cette situation en proposant un cadre légal qui présenterait les critères à réunir pour délivrer ces informations.

Le projet de loi n°5949 avait prévu une procédure d'autorisation préalable auprès de la Justice de Paix. Une telle procédure n'est pourtant plus du tout mentionnée dans le projet de loi actuel.

Par conséquent, et en faisant application des règles générales en matière de protection des données, la Commission nationale considère que la communication à des tiers de données à caractère personnel issues des fichiers communaux serait interdite, dès lors que ces fichiers communaux sont créés pour répondre à des finalités précises, mais différentes des raisons pour lesquelles les informations sont demandées. La Commission a donc estimé que le projet de loi devait être complété pour remédier à l'insécurité juridique en la matière.

2.2.2 Le surendettement

La Commission nationale s'est également prononcée au sujet de la version amendée du projet de loi n°6021 concernant le surendettement[10]. Elle avait déjà avisé ce projet le 17 juin 2011. Depuis lors, le projet de loi a été modifié de manière substantielle. Dans sa prise de position, la Commission nationale a observé avec satisfaction que certaines de ses remarques ont été intégrées dans les amendements. Quelques précisions et éclaircissements devraient pourtant encore être apportés au projet de loi.

Sanction pour diffusion de données à d'autres fins que celles prévues par la loi

La finalité de la loi concernant la diffusion des informations reçues par la consultation du répertoire des personnes surendettées est l' « *information des créanciers,*

[10] Dénomination complète : projet de loi n°6021 concernant le surendettement portant modification : 1. de la loi modifiée du 8 décembre 2000 sur le surendettement, 2. de l'article 2016 du Code civil, 3. des articles 1er et 4 du Nouveau Code de procédure civile et 4. de l'article 536 du Code de commerce sur le surendettement et modifiant certaines dispositions légales.

cautions et coobligés du débiteur surendetté sur l'état d'avancement de la procédure de règlement collectif des dettes ».

La Commission nationale a estimé dans son avis qu'il y a lieu de prévoir une disposition pénale sanctionnant la diffusion à des fins étrangères à cette finalité. Elle a suivi en cela la position du Conseil d'Etat. Une telle disposition permettrait de sanctionner les abus relatifs à l'utilisation du répertoire, dont la consultation est désormais permise à toute personne qui justifie de son identité. Il est en effet à craindre que des personnes mal intentionnées consultent le répertoire *« par simple curiosité malsaine ».*

Dans le même ordre d'idées, pour ce qui est de la consultation du répertoire par de simples particuliers, la CNPD partage aussi la proposition du Conseil d'Etat de *« limiter l'information de toute personne justifiant de son identité à la seule confirmation ou infirmation de l'inscription au répertoire ».*

Durée de conservation

Le projet de loi amendé allonge la durée de conservation des données dans le répertoire à dix années au maximum. Selon la CNPD, cet allongement des délais de conservation n'est pas motivé.

En effet, dans la première version du projet de loi, la durée de conservation dans le répertoire était de sept années pour les plans de règlement conventionnel, les plans de redressement judiciaire, les plans établis à des fins probatoires et les recommandations de la Commission de médiation. A défaut de précisions qui puissent justifier un allongement, la Commission nationale a recommandé de maintenir la durée d'inscription à sept ans pour les plans ci-dessus.

En ce qui concerne la durée de conservation de l'information relative aux débiteurs surendettés ayant bénéficié de la procédure de rétablissement personnel, qui était de cinq ans à partir de la date du jugement de clôture de la procédure, la Commission nationale a estimé qu'il est logique de prévoir un allongement de la durée de l'inscription dans le mesure où le plan judiciaire peut être établi pour une durée maximale de sept années. Il n'est toutefois pas justifié de pouvoir garder cette inscription au-delà de ce délai.

2.2.3 L'exploitation d'une base de données relative aux élèves : avis complémentaire

Dans son avis complémentaire du 15 juin 2012, la CNPD a formulé quelques observations au sujet du projet de loi n°6284 relatif aux traitements de données à caractère personnel concernant les élèves. Elle a salué les nombreuses améliorations apportées au texte du projet de loi en termes de protection des données et de la vie privée, mais a également émis des réserves, notamment en ce qui concerne l'intention de faire figurer une photographie de chaque élève

Les activités en 2012

dans un fichier centralisé et la sanction pénale prévue en cas de refus de fournir des données.

Améliorations

Parmi les améliorations apportées au texte du projet de loi, citons :

- le fait que le texte amendé prévoit désormais la désignation d'un chargé de la protection des données (tel que visé à l'article 40 de la loi modifiée du 2 août 2002) au sein du ministère de l'Education nationale et de la Formation professionnelle ;
- les dispositions relatives à la sécurité et la confidentialité des données ainsi que celles relatives à l'accès aux données ont été précisées et renforcées ;
- les données relatives aux revenus des représentants légaux des élèves ne seront pas collectées et traitées ;
- pour des considérations de transparence et de loyauté envers les personnes concernées, les représentants légaux et l'élève majeur recevront une information individuelle, écrite et exhaustive sur le traitement des données les concernant.

La photographie de l'élève stockée dans la base de données centralisée

La Commission nationale a fait remarquer qu'à l'heure actuelle, il n'existe aucun autre fichier informatique, exploité par une administration ou un service de l'Etat, qui contiendrait de façon permanente des photographies des administrés ou de seulement une partie ou catégorie de citoyens. Le projet de loi avisé constituerait dès lors un précédent, puisqu'il prévoit l'enregistrement permanent de la photographie de quelque 95.000 élèves dans un fichier centralisé à l'échelle nationale.

La CNPD s'est toujours prononcée contre l'insertion d'une donnée biométrique (qui est une donnée particulièrement sensible) dans une base de données centralisée, compte tenu des usages possibles de ces traitements et des risques d'atteintes graves à la vie privée et aux libertés individuelles.

La sanction pénale prévue en cas de refus de fournir des données

L'article 4 paragraphe (7) prévoit maintenant une amende pénale en cas de refus de fournir les données mentionnées à l'article 3 paragraphe (2). La Commission nationale est opposée à l'idée d'assortir la disposition en question de sanctions pénales

et s'est interrogée sur la compatibilité de cette disposition avec le droit d'opposition que la loi modifiée du 2 août 2002 confère à tout citoyen. Elle s'est posée, par ailleurs, la question de savoir s'il n'était pas disproportionné de prévoir une amende pénale en cas de refus de fournir des données comme par exemple l'adresse électronique ou la photographie.

Précédents avis

La Commission nationale s'était déjà exprimée à plusieurs reprises à propos de ce projet de loi, notamment dans ses avis précédents du 26 juillet 2010, du 15 avril 2011 et dans sa note du 22 mai 2012.

2.2.4 La pétition électronique

Dans le cadre de la modernisation du droit de pétition, la Chambre des députés envisage d'instaurer une nouvelle catégorie de pétition appelée « pétition publique ». Contrairement à la pétition ordinaire, toutes les démarches relatives à la pétition publique se feront exclusivement de manière électronique. L'inscription par le biais d'un formulaire figurant sur le site Internet de la Chambre des députés est suivie de la vérification de la recevabilité de la pétition. Le cas échéant, la pétition publique sera publiée pour la collecte des signatures sur ledit site Internet pendant une période de six semaines.

La signature d'une pétition publique sera réservée, sauf exception spécifique, aux résidents du Grand-Duché de Luxembourg âgés d'au moins 15 ans. Lorsqu'une pétition aura recueilli 4.500 signatures, un débat public devra obligatoirement être organisé à la Chambre des députés et la commission des Pétitions décidera du suivi à accorder à cette pétition.

Dans sa prise de position, la Commission nationale a accueilli de manière très favorable la décision de l'administration parlementaire de renoncer à la collecte du matricule dans le contexte de la pétition publique. En effet, la Commission nationale a toujours préconisé une politique visant à limiter l'utilisation du numéro d'identité, notamment au vu des nombreux risques ayant trait aux libertés et droits des citoyens.

2 Les activités en 2012

Publication des données sur Internet

La collecte des données dans le cadre d'une pétition ordinaire se fait exclusivement au moyen de signatures manuscrites sur papier.

L'accès à ces données reste limité avant tout aux initiateurs ainsi qu'aux membres de la commission des Pétitions qui la reçoivent.

Contrairement à la pétition ordinaire, la pétition publique prévoit une publication obligatoire des données d'identification, du code postal et de la localité des pétitionnaires sur Internet. La diffusion des données à caractère personnel sur le site Internet de la Chambre des députés aura encore un effet multiplicateur en raison de l'indexation des données faite par les moteurs de recherche sur Internet (par exemple Google, Bing, Yahoo, etc.).

La CNPD a considéré que la publication de ces données à caractère personnel est susceptible de poser problème à plusieurs égards.

Le signataire d'une pétition publique court ainsi le risque d'être catégorisé ou profilé philosophiquement ou politiquement. Il suffira de taper le nom d'une personne dans un moteur de recherche pour la voir associée, le cas échéant, à une pétition. Il est évident que cela constituera, surtout dans le cadre d'un sujet de pétition plus « sensible », un risque non négligeable pour la vie privée des signataires, en considérant que ces informations pourraient être utilisées dans un tout autre contexte.

Pour les raisons précitées, la Commission nationale a estimé que la publication des données des signataires devrait être plus limitée. Elle a recommandé de laisser le libre choix aux signataires de voir publier ou non leurs nom, prénom et leur localité de résidence. Alors même que les données de certains signataires ne seraient pas publiées, le système pourra toujours indiquer le nombre total de signataires pour une pétition donnée, en vue de renseigner le public sur le succès remporté.

En tout état de cause – au cas où la Chambre des députés opterait quand même pour une publication en ligne de l'identité des signataires – la Commission nationale a considéré qu'il serait préférable que les données sur les noms et la localité ne comprennent pas le code postal.

Enfin, toutes les mesures possibles devraient être prises afin d'éviter une indexation de l'identité des signataires par les moteurs de recherche.

2.2.5 Le fonctionnement du registre national du cancer

Faisant suite à la demande lui adressée par Monsieur le Ministre de la Santé en date du 6 août 2012, la Commission nationale s'est exprimée au sujet de l'avant-projet de règlement grand-ducal déterminant les modalités et les conditions de fonctionnement du registre national du cancer et modifiant le règlement grand-ducal du 20 juin 1963 rendant obligatoire la déclaration des causes de décès.

Dans l'ensemble, elle a accueilli favorablement l'avant-projet de règlement grand-ducal, mais a cependant formulé quelques observations susceptibles d'améliorer ce texte.

Légitimité de la collecte et de l'utilisation des données dans le registre national du cancer

La Commission nationale a estimé dans son avis que le traitement de données mis en œuvre dans le cadre du registre national du cancer doit être considéré comme légitime sur base du critère du « motif d'intérêt public » et non pas sur base du consentement.

L'avant-projet indique que le traitement des données du registre national de cancer est légitimé par le consentement implicite des patients. Or, lorsqu'un traitement de données de santé est basé sur le consentement, un consentement implicite ne suffit pas, car la loi modifiée du 2 août 2002 (tout comme la directive 95/46/CE) exige un consentement exprès préalable.

La CNPD comprend parfaitement que le registre national du cancer doit être aussi exhaustif que possible pour que les données soient utilisables à des fins cliniques, scientifiques et épidémiologiques, et qu'il n'est dès lors pas envisageable de recueillir systématiquement le consentement exprès des patients. Or, la directive 95/46/CE et la loi modifiée du 2 août 2002 prévoient d'autres critères de légitimation que le consentement exprès. Le traitement de données de santé peut notamment être légitime, lorsque celui-ci s'avère nécessaire pour un motif d'intérêt public. Il va sans dire que la mise en place d'un registre national du cancer répond bien à un motif d'intérêt public, et plus particulièrement en matière de santé publique.

Le droit d'opposition, une garantie appropriée qui respecte l'autodétermination du patient

Par rapport au critère de légitimation du motif d'intérêt public qui sert comme base juridique au registre national du cancer, le droit d'opposition (ou le consentement implicite) doit être considéré comme une garantie ou sauvegarde supplémentaire en termes de protection de la vie privée.

La CNPD a salué le fait que les patients puissent s'opposer préalablement ou postérieurement à ce que leurs données figurent au registre national du cancer. Pour ce qui est de l'exercice du droit d'opposition avant le début du traitement des données, le texte en projet prévoit que les données du patient ne seront pas communiquées au registre national du cancer, mais que le gestionnaire du registre national du cancer recevra néanmoins l'information que le malade s'y est opposé. La Commission nationale s'est toutefois demandée dans son avis pourquoi le gestionnaire devait être informé de l'identité du patient.

Dans ces cas, et même si le registre ne contenait pas de données sur les patients souhaitant exercer leur droit d'opposition, le gestionnaire connaîtrait cependant leur identité et disposerait en quelque sorte d'une « liste noire ».

La Commission nationale a estimé que pour des raisons statistiques, il suffira que le gestionnaire dispose uniquement du nombre des patients qui se

sont opposés. Lorsque par après un patient décidera de participer à nouveau, ses données seront communiquées au registre et il sera sans importance pour le gestionnaire de savoir que ce patient n'a pas voulu y figurer au moment du diagnostic.

Le contenu du registre

La loi modifiée du 2 août 2002 prévoit que seules les données adéquates et strictement nécessaires à la réalisation des finalités du traitement doivent être collectées et utilisées par le responsable du traitement.

A ce titre, la CNPD ne comprend pas pourquoi il serait nécessaire de collecter la date de naissance exacte (j/m/a). Elle a estimé dans sa prise de position que pour effectuer des analyses de survie, il suffit de disposer du mois et de l'année de naissance. Elle ne voit pas non plus la nécessité de vouloir collecter le code postal en plus de la localité.

Il est clair que pour pouvoir analyser les liens entre environnement et cancer, il faut disposer d'une donnée géographique. Or, la Commission nationale pense que le code postal est une donnée trop détaillée, qui n'est pas indispensable pour faire ce genre de recherche.

2.2.6 La réforme du casier judiciaire

La Commission nationale a avisé le projet de loi n°6418 relatif à l'organisation du casier judiciaire et aux échanges d'informations extraites du casier judiciaire entre les Etats membres de l'Union européenne et modifiant le Code d'instruction criminelle.

Réorganisation du casier judiciaire

Parmi les modifications qu'a apportées le projet de loi, citons :

- l'extension du casier judiciaire aux personnes morales ;
- la suppression de la référence aux condamnations à des peines de police ;
- l'amélioration des échanges d'informations entre Etats membres ;
- la simplification du système du casier judiciaire en réduisant le nombre de bulletins (qui est actuellement de trois) à deux bulletins
  - Le bulletin n°1 contient le relevé intégral des condamnations applicables à la même personne,
  - Le bulletin n°2 ne contiendra plus que le relevé intégral des condamnations applicables à

Le casier judiciaire est un fichier destiné à recevoir l'inscription des condamnations prononcées par les juridictions répressives luxembourgeoises et, sous certaines conditions, étrangères.

L'Union européenne s'est donné pour objectif d'offrir aux citoyens un niveau élevé de protection dans un espace de liberté, de sécurité et de justice. Cet objectif suppose que les autorités compétentes des Etats membres échangent des informations extraites du casier judiciaire.

une personne, à l'exception des condamnations assorties d'un sursis de moins de 6 mois et des condamnations prononcées par des juridictions étrangères et notifiées à des fins autres qu'une procédure pénale.

Avis de la Commission nationale

Le 10 octobre 2012, la Commission nationale a eu l'occasion de présenter ses observations à la commission juridique de la Chambre des députés. Dans sa prise de position, elle a limité ses réflexions aux dispositions relatives à la délivrance du bulletin n°2 du casier judiciaire et au traitement des données résultant des extraits du casier judiciaire par les administrations, autorités et organismes publics et par les employeurs du secteur privé.

Communication du bulletin

Actuellement, il existe un traitement inégalitaire au sujet de la communication du bulletin lorsqu'il s'agit d'un employeur du secteur public ou du secteur privé. L'arrêté ministériel modifié du 22 novembre 1977 détermine la liste des organismes publics pouvant réclamer le bulletin n°2. Par contre, l'employeur privé ne bénéfice pas du droit d'exiger la délivrance d'un casier judiciaire, mais doit demander à son futur salarié qu'il lui délivre un extrait (bulletin n°3). S'y ajoute le fait que l'employeur privé n'a pas le droit de soumettre ledit extrait à un traitement au sens de la loi modifiée du 2 août 2002. En d'autres mots, il a le droit de prendre connaissance du contenu des bulletins produits par les candidats, sans pour autant pouvoir en faire mention dans des dossiers structurés ou fichiers informatiques.

Or, il s'avère que les pratiques effectives ne sont pas toujours conformes au cadre légal exigé. La Commission nationale soutient la mise en place d'une base légale claire et précise (à l'endroit de l'article 8 du projet de loi) autorisant l'employeur, privé ou public, à pouvoir consulter et traiter les informations contenues dans l'extrait du casier judiciaire de son personnel et de pouvoir les conserver pour une durée limitée à deux ans au maximum.

Droit d'accès de l'intéressé

Le citoyen peut parfaitement obtenir l'accès et consulter sur place l'intégralité des inscriptions le concernant en se présentant au guichet du casier judiciaire, alors même qu'il ne peut obtenir délivrance d'un extrait que sous la forme du bulletin n°3 (et à l'avenir du bulletin n°2 après la suppression du bulletin n°3). Son avocat y a également accès dans le cadre de toute procédure judiciaire pénale.

Il est vrai que ni le texte du règlement grand-ducal du 14 décembre 1976 portant réorganisation du casier judiciaire, ni celui du projet de loi en question ne mentionnent un tel accès.

La Commission nationale estime qu'il serait souhaitable que cette faculté soit expressément prévue et qu'elle soit en outre portée à la connaissance du public dans les guichets (y compris sur la page web du guichet électronique) du casier judiciaire.

2 Les activités en 2012

Condamnations mentionnées sur le bulletin délivré à l'intéressé

Les condamnations mentionnées au bulletin n°2 comprennent désormais celles pour contraventions de police (de 1re et 2e classe) et pour les infractions à la législation relative à la circulation routière (à l'exception des contraventions en matière de stationnement), alors que le bulletin n°3 délivré actuellement ne renseigne que les condamnations à des peines privatives de liberté pour crime et délit, sauf condamnations conditionnelles avec ou sans mise à l'épreuve.

L'adoption du projet de loi engendrera par conséquent une visibilité substantiellement élargie de l'employeur sur les condamnations du candidat ou de son nouveau salarié. La Commission nationale n'est pas convaincue qu'il faille absolument englober ces condamnations pour des infractions à la législation sur la circulation routière et pour des infractions engendrant des peines de police.

Transparence et information des personnes concernées en cas de délivrance d'un extrait

Même si la délivrance directe des extraits du casier judiciaire aux autorités, administrations et organismes publics peut être justifiée, il s'avère néanmoins nécessaire de mettre en place un minimum de mesures de sauvegarde destinées à prévenir et à détecter des abus. Il s'agit de veiller à ce que les extraits du casier judiciaire ne soient demandés que dans les seuls cas prévus par une disposition législative ou réglementaire, et uniquement en cas de nécessité dûment justifiée.

Il paraît également impératif de prévoir, dans le texte même de la loi, l'information systématique et obligatoire des personnes concernées par toute demande et délivrance d'un extrait les concernant, avec la mention de l'organisme demandeur.

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.

2.3.1 Actions de sensibilisation du public

Le 28 janvier 2012, à l'occasion de la Journée de la protection

des données, la Commission nationale a mené une campagne publique placée sous le slogan *« Votre vie privée n'est pas privée de droits »*. Organisée annuellement depuis 2007 par le Conseil de l'Europe et 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 des données. L'édition 2012 a pris une importance toute particulière, alors que les textes légaux au niveau du Conseil de l'Europe, de l'Union européenne et de l'OCDE étaient en cours de révision.

Ouverte à la signature le 28 janvier 1981, la « Convention 108 » du Conseil de l'Europe 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 de données le concernant, et à assurer la transparence quant à l'utilisation des fichiers et des traitements effectués à partir de ses données personnelles.

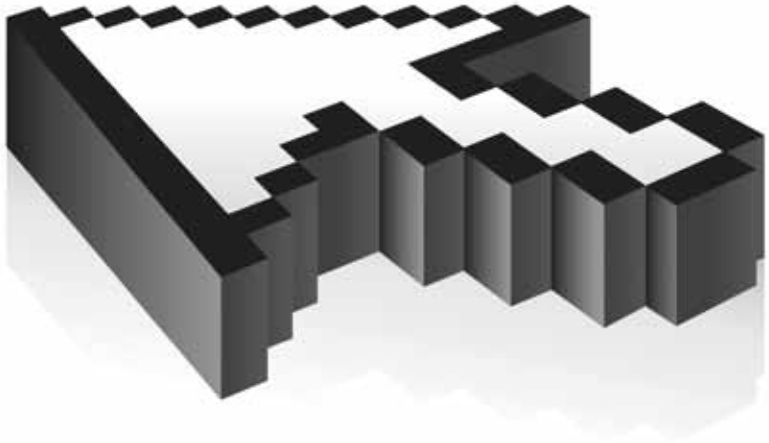
La Commission nationale a également participé au Safer Internet Day, qui a été lancé à l'initiative de la Commission européenne et organisé dans le monde entier par INSAFE le 7 février 2012. Cette année, le mot d'ordre était *« Génération connectée – Découvrir l'Internet ensemble, c'est plus sûr ! »*. Au Luxembourg, BEE SECURE a initié et coordonné de nombreuses activités, dont l'objectif était de mobiliser le plus grand nombre d'acteurs et d'institutions. Des conférences et formations ont eu lieu toute la semaine du 6 au 10 février.

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

Au cours de l'année 2012, la Commission nationale est intervenue régulièrement dans les médias pour se prononcer sur des sujets ayant trait à la protection des données et de la vie privée. Le Président et les membres effectifs ont accordé plus de 30 interviews aux organes de presse.

Parmi les thèmes traités par les médias, citons : la coopération de la CNPD avec l'Université du Luxembourg, la journée de la

Les activités en 2012



protection des données, le vol de données au Centre médicosportif (« Medicoleak »), la révision de la législation européenne sur la protection des données, la base de données relative aux élèves et le cloud computing.

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 2012, elle a reçu 43% 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

Pierre Weimerskirch présentant un exposé lors de l'événement dédié à la tendance « BYOD »

Gérard LOMMEL à la table ronde « Internet, amplificateur de libertés ? »

et obligations respectifs. Les internautes intéressés peuvent donc 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

Directement sollicitée par de nombreux organismes, sociétés ou institutions pour conduire des actions de formation ou de sensibilisation de publics plus spécialisés aux enjeux de la protection des données, la Commission nationale organise régulièrement des formations, conférences et séminaires.

Le Président de la CNPD, Gérard Lommel, a participé au séminaire intitulé « *The proposed EU general data protection regulation - strengthening the EU's data protection architecture?* ». Organisée par l'Académie de Droit européen en collaboration avec le Contrôleur européen de la protection des données, cette manifestation s'est déroulée à Trèves les 20 et 21 septembre. Le programme a porté sur les principales nouveautés et modifications actuellement en discussion au niveau du Parlement européen et du Conseil, suite aux textes proposés le 25 janvier 2012 par la Commission européenne. L'événement s'adressait non seulement aux magistrats des juridictions européennes et nationales, aux autres juristes du secteur public et aux professionnels du secteur privé ou associatif, mais aussi aux chargés de la protection des données, intéressés par l'évolution du cadre légal européen dans cette matière. « *Towards a less bureaucratic, but more effective*

Les activités en 2012

supervision of Data Protection in a better integrated EU legal framework », tel était le titre de l'exposé de Monsieur Lommel qui portait plus particulièrement sur deux défis importants pour les autorités de protection des données européennes : le développement de l'efficacité des règles relatives à la protection des données et une amélioration du respect et de la mise en œuvre des règles à travers l'UE.

Par ailleurs, Pierre Weimerskirch, membre effectif de la Commission nationale, a fait un exposé lors d'un événement organisé par Telindus dédié à la tendance « BYOD » (Bring Your Own Device) le 27 septembre. Grâce aux nouvelles technologies, les employés d'une société peuvent aujourd'hui travailler de n'importe où, à tout moment et depuis n'importe quel outil. Les risques associés à cette nouvelle pratique sont bien réels. Comment rendre alors « compliant » cette façon de travailler ? Comment contrôler les accès aux données de l'entreprise depuis ces terminaux ? Comment réussir à disposer d'un inventaire des utilisateurs et de leurs appareils ? Comment éviter la fuite des données ? Comment établir une barrière entre les données personnelles et « corporate » ? Telles sont seulement quelques-unes des questions auxquelles cette conférence a essayé de répondre.

Le 26 septembre, la Commission nationale a également participé à une table ronde dédiée aux défis créés par les technologies de la communication dans le domaine de la sécurité de l'information. Cette table ronde s'est déroulée dans le cadre de la conférence « La sécurité au cœur de l'information » organisée par le groupement d'intérêt économique « Security made in Lëtzebuerg ». Les participants ont eu l'occasion de s'informer sur la protection des données à caractère personnel appliquée au domaine de la sécurité de l'information.

Le Président de la Commission nationale a également participé à une table ronde organisée par l'ASBL Liberté, intitulée « *Internet, amplificateur de libertés ?* » en date du 23 octobre. Les participants étaient Charles Goerens (Député européen), Thierry Reisch (Avocat à la Cour), Roland Arens (Responsable digital media du groupe Saint-Paul) et Sven Clement (Président du Parti Pirate).

Gérard Lommel a également fait un exposé dans le cadre de la conférence sur « *The future of data protection in Europe* », organisée par l'Information Commissioner's Office (autorité de protection des données anglaise) les 28 et 29 mars à Londres.

Entrevue le 16 octobre 2012 avec la direction de l'Union Luxembourgeoise des Consommateurs (ULC)

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 26 et 27 juin, et ils sont intervenus auprès des étudiants de l'Université du Luxembourg en date du 17 décembre.

2.4 Conseil et guidance

2.4.1 Concertation avec les organisations représentatives sectorielles, les principaux acteurs économiques, l'Etat 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 pour encadrer les acteurs privés et publics dans leurs efforts de mise en conformité.

La Commission nationale n'intervient pas seulement en amont de la mise en place des traitements de données à caractère personnel par le biais des formalités préalables, des demandes d'avis ou encore des demandes de conseil. Elle accompagne aussi de façon permanente les différents acteurs en mettant à leur disposition son expertise juridique et technique, en participant à des conférences ou en organisant des entrevues sectorielles et ciblées.

Avec la réforme des règles européennes en matière de protection des données, la Commission nationale prépare d'ores et déjà les entreprises, organismes publics et autres organisations aux nouvelles règles qui impliquent une responsabilité accrue (« accountability ») des acteurs traitant des données à caractère personnel.

Aux côtés des acteurs publics et privés

En 2012, la Commission nationale a participé à plus de 71 réunions avec les acteurs du secteur public et 61 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 en matière d'allocations familiales et d'aide pour les études supérieures ;
- Institut luxembourgeois de régulation : smart metering, vie privée dans le secteur des communications électroniques ;
- Ministère de la Santé : registre national du cancer, médecin-coordinateur ;

2 Les activités en 2012

- Ministère de la Justice : casier judiciaire, projet de directive PNR européen, surendettement ;
- Ministère des Affaires étrangères : surveillance de la navigation maritime ;
- Service des Communications et des Médias : réforme du cadre européen sur la protection des données, protection de la vie privée dans le secteur des communications électroniques, coopération en matière de protection des consommateurs, registre de baptême ;
- CTIE (Centre des technologies de l'information de l'Etat) : dossier médico-sportif ;
- CASES du Ministère de l'Economie et du Commerce extérieur : sécurité de l'information

La Commission nationale est 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, Microsoft et ArcelorMittal.

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

La Commission nationale a poursuivi sa coopération avec la Fédération des Hôpitaux Luxembourgeois (ancien nom : Entente des Hôpitaux Luxembourgeois) pour promouvoir les bonnes pratiques qui ont émergé ces dernières années au niveau des différents aspects de 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.

Elle a aussi collaboré avec l'Association des Médecins et Médecins-Dentistes (AMMD) sur les droits et obligations des patients, et avec la fondation Stëftung Hëllef Doheem sur le dossier électronique. Elle a encore participé aux travaux de l'agence « e-santé ».

Dans le domaine de la recherche, elle était en lien avec le Comité National d'Ethique et de Recherche (CNER), le CEFIS (Centre d'étude et de formation interculturelles et sociales) ou encore le STATEC.

Entrevues sectorielles

La Commission nationale a eu des réunions avec les organisations représentatives sectorielles, dont l'Association des Banques et Banquiers du Luxembourg (ABBL), l'Union luxembourgeoise des Consommateurs (ULC), l'Association des Compagnies d'Assurances (ACA), la FEDIL (Business Federation Luxembourg), la Chambre de Commerce et la Chambre des Salariés.

Réforme du cadre juridique européen sur la protection des données

La Commission nationale a soumis aux services du ministre des Communications et des Médias ses observations et recommandations relatives au nouveau paquet législatif sur la protection des données présenté par la Commission européenne dans le cadre de la consultation lancée par le gouvernement. Lors d'échanges de vues réguliers, elle a accompagné la préparation des travaux du Conseil et émis ses préconisations au fur et à mesure. Par ailleurs, elle a reçu les députés européens pour discuter de la réforme du cadre juridique européen.

2.4.2 Demandes de renseignements

La Commission nationale reçoit annuellement entre 1500 et 2000 demandes de renseignement. Dans la majorité des cas, il s'agit de questions juridiques ou de requêtes relatives aux formalités à accomplir pour mettre en œuvre un traitement de données.

En 2012, la Commission nationale a répondu à 1697 demandes de renseignement, dont 1424 par téléphone et 273 par écrit. Si la plupart des demandes émanent d'entreprises, les administrations publiques, avocats et citoyens 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 sur 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 l'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 à définir des solutions « made in Luxembourg » qui pourront servir d'exemples pour faire face aux nouveaux défis dans ce domaine, et cela 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

Les activités en 2012

sa complexité. La Commission nationale, représentée par un ou plusieurs de ses membres, a participé en 2012 à 43 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 » ;
  - « Health Data » ;
  - « Règles d'entreprise contraignantes » ;
  - « Financial Matters » ;
  - « Biometrics and E-government » ;
  - « Future of Privacy » ;
  - « Key provisions of directive 95/46/CE » ;
- du Comité consultatif de la Convention 108 du Conseil de l'Europe (T-PD) ;
- du « Groupe de Berlin », dédié à la protection des données dans le secteur des communications électroniques ;
- du séminaire européen d'échanges d'expériences dans le traitement des cas pratiques (« Case Handling Workshop ») ;
- 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.

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 27 Etats membres de l'Union européenne.

Parmi les sujets traités par le groupe de travail en 2012, citons :

- la réforme de la protection des données européenne ;
- la biométrie ;
- la reconnaissance faciale ;
- la modification des paramètres de la vie privée de Google ;
- le nouveau code de la « World Anti-Doping Agency » ;
- l'« Internet Corporation for Assigned Names and Numbers » (ICANN, en français : Société pour l'attribution des noms de domaine et des numéros sur Internet) ;
- les applications mobiles ;
- les « Binding Corporate Rules » (BCR, en français : règles d'entreprise contraignantes) ;
- le cloud computing.

2.6.1.1 Programme de travail 2012-2013

Le groupe de travail a fixé ses priorités dans son programme de travail pour la période 2012-2013.

Un de ses objectifs est d'assurer une mise en œuvre cohérente et correcte du cadre juridique actuel et de continuer à préparer le futur cadre juridique proposé par la Commission européenne le 25 janvier 2012.

Le groupe va également essayer de répondre aux défis technologiques émergents posés par le cloud computing, la reconnaissance faciale, les systèmes de suivi par capture d'empreintes numériques ou encore les smartphones.

De plus, le groupe entend préciser et renforcer le rôle de tous les acteurs dans le domaine de la protection des données : personnes concernées, responsables du traitement des données et autorités chargées de la protection des données. Le groupe se penchera par ailleurs sur le domaine de la liberté, de la sécurité et de la justice, afin d'y assurer une approche cohérente et efficace en matière de protection des données.

2.6.1.2 Prises de position détaillées sur la réforme européenne de la protection des données

En 2012, le groupe de travail a avisé à deux reprises le paquet de la Commission européenne concernant la réforme de la protection des données.

Dans sa prise de position du 23 mars, le groupe a analysé en détail les deux propositions législatives présentées par Madame Viviane Reding 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.

Un avis favorable avec des réserves

Le G29 a accueilli favorablement les propositions visant à renforcer les droits des individus, à donner plus de responsabilité aux détenteurs de données et plus de pouvoirs aux autorités nationales et internationales chargées de la protection des données.

Le groupe s'est également félicité de l'inclusion de dispositions motivant les responsables du traitement à respecter la vie privée des personnes dès le début (p.ex. en effectuant des « Privacy Impact Assessments » et en respectant les principes de « Privacy by Design » et de « Privacy by Default »).

De plus, le G29 a soutenu la proposition de la Commission européenne d'harmoniser les pouvoirs et compétences des autorités de contrôle pour assurer de façon plus effective le respect de la législation, notamment en ayant la possibilité d'imposer des amendes importantes.

Les activités en 2012

Besoin d'amélioration et de clarification

En dépit de son avis favorable, le groupe de travail a noté que certaines parties des propositions devaient être améliorées et clarifiées.

Avec le nouveau règlement, les entreprises n'auront, en principe, à traiter qu'avec l'autorité de contrôle du pays de l'Union européenne où se trouve leur siège principal (principe du « guichet unique »). Le groupe considère qu'il faudra clarifier la méthode en vue de déterminer le lieu d'implantation du siège principal d'une entreprise multinationale. Cet aspect jouera un rôle essentiel dès qu'il s'agira de désigner l'autorité « chef de file » dans un cas particulier ou pour une entreprise donnée. En outre, les répercussions sur les compétences des autres autorités de contrôle devront être précisées.

En ce qui concerne la directive pour le domaine de la police et de la justice, le groupe de travail a regretté le niveau d'ambition de la Commission européenne et a souligné le besoin de dispositions plus fortes. Il a critiqué notamment l'absence de principes de la protection des données comme la limitation des périodes de conservation, la transparence et l'exactitude des données à caractère personnel. De plus, le groupe a émis des réserves quant au champ d'application de la directive et sa cohérence avec le règlement.

Avis complémentaire

Le 5 octobre, le groupe de travail a adopté un deuxième avis relatif au paquet législatif de la Commission européenne.

L'avis est plus détaillé que celui du 23 mars, qui constituait une première réponse générale aux propositions de la Commission européenne. La prise de position tient compte des discussions actuelles au Parlement et au Conseil de l'Union européenne et fournit des explications supplémentaires sur certains concepts clés tels que la définition des données personnelles, la notion du consentement et des actes délégués.

Le groupe de travail a notamment souligné que ce serait une erreur de modifier des aspects clés des données à caractère personnel ainsi que la notion du consentement, comme certains l'ont proposé. Pour mieux protéger la confidentialité des données et la pérennité du règlement, il est nécessaire d'adopter une définition élargie des données à caractère personnel et de veiller à ce que toute procédure fondée sur un

consentement soit une procédure de qualité.

Dans son avis, le groupe a constaté que des doutes ont été émis quant au réalisme du mot « explicite » dans le contexte du consentement. Or, le G29 est d'avis que l'inclusion de ce mot constitue une importante clarification du texte, qui est nécessaire pour permettre aux personnes concernées d'exercer véritablement leurs droits, en particulier en ce qui concerne l'Internet, où l'usage du consentement actuel est trop souvent abusif. Il serait très peu souhaitable que cette importante clarification du texte en soit supprimée.

La proposition de la Commission relative à un nouveau règlement prévoit un volume considérable d'actes délégués et d'actes d'exécution. Même si, dans certains cas, ces actes supplémentaires peuvent être un instrument précieux pour apporter un meilleur niveau d'harmonisation et d'orientation, le groupe de travail Article 29 émet des réserves sur la mesure dans laquelle la Commission serait habilitée à adopter de tels actes.

2.6.1.3 Publication de lignes directrices sur le cloud computing

Le groupe « Article 29 » a adopté un document de travail sur le cloud computing, qui comporte des précisions sur le cadre juridique applicable aux fournisseurs de tels services et à leurs clients. Il a notamment analysé les questions relatives à la protection des données et les obligations incombant aux responsables du traitement actifs sur le territoire de l'Espace économique européen (EEE). Le cloud computing désigne l'utilisation à distance de ressources informatiques qui étaient auparavant stockées localement sur les serveurs et ordinateurs des entreprises, organisations ou particuliers. Les applications et les données ne se trouvent alors plus sur l'ordinateur local, mais comme « dans un nuage » (d'où l'expression « cloud computing »). De nombreux services de cloud computing, fournis et facturés à la demande, sont désormais disponibles. Ils permettent notamment aux entreprises (surtout aux PME) de mutualiser leurs coûts informatiques et d'hébergement et d'utiliser des services informatiques auxquels

ils n'avaient pas accès jusqu'alors pour des raisons financières.

Risques du cloud computing en matière de protection des données

Malgré ses avantages économiques et pratiques, le recours croissant au cloud computing dans le traitement des données à caractère personnel soulève certains problèmes. Le G29 a notamment cité le manque de contrôle qu'on peut exercer sur les données personnelles. En transférant ses données vers un service « cloud », un client rencontrera davantage de difficultés lorsqu'il s'agira de déployer les mesures techniques et organisationnelles nécessaires pour assurer la disponibilité, l'intégrité, la confidentialité, la transparence, l'isolement et la portabilité des données.

Une information insuffisante sur les modalités du traitement des données par un service « cloud » comporte également un risque important. En l'absence de transparence, le client peut rencontrer des difficultés en essayant de remplir ses obligations en tant que responsable du traitement. Il se pourrait p.ex. qu'il ne soit pas au courant du fait que le traitement des données inclut plusieurs responsables du traitement et sous-traitants ou que les données sont transférées hors de l'EEE vers un pays n'assurant pas un niveau de protection adéquat.

Le client d'un service « cloud » doit savoir par qui et pour quelle raison ses données sont utilisées. Dans son avis, le G29 a même demandé aux prestataires de fournir à leurs clients des informations relatives à leurs sous-traitants et aux emplacements des serveurs dans lesquels les données sont traitées.

Recommandations du G29

Un des conseils-clés de cet avis aux entreprises et administrations est de faire une analyse des risques avant d'adopter un service de cloud computing et de s'assurer que la sécurité, la transparence et la légalité des traitements sont garanties.

Le G29 a d'ailleurs recommandé aux clients de choisir un fournisseur garantissant que les traitements effectués seront conformes à la législation européenne sur la protection des données, notamment en ce qui concerne les transferts de données vers des pays tiers.

2.6.1.4 La reconnaissance faciale sur Internet et les services mobiles

En date du 22 mars 2012, le G29 a adopté un avis relatif à

l'utilisation de la reconnaissance faciale sur les sites Internet et les services mobiles.

La technologie de reconnaissance faciale est aujourd'hui non seulement utilisée dans des casinos pour reconnaître les joueurs avec interdiction d'accès, mais aussi dans de nombreux outils utilisés au quotidien tels que les appareils de photos numériques équipés d'une telle fonction ou lors de l'ouverture d'une session sur un ordinateur portable.

Un nombre croissant d'applications en ligne, dont le plus grand réseau social Facebook, utilisent également la reconnaissance faciale pour identifier, authentifier ou catégoriser des individus. Concrètement, si vous êtes un utilisateur de Facebook et qu'un de vos « amis » ajoute de nouvelles photos dans lesquelles vous semblez apparaître, le réseau social lui proposera automatiquement de « marquer » ces photos avec votre nom. Pour effectuer cette « suggestion d'identification », Facebook se base sur toutes les photos sur lesquelles vous avez déjà été identifié auparavant.

Dans son avis, le groupe de travail a rappelé que les photos sur lesquelles le visage d'un individu est clairement visible et identifiable sont considérées comme des données à caractère personnel. Etant donné que ces photos comportent des données biométriques, elles doivent faire l'objet d'une protection renforcée. De ce fait, le G29 a proposé de rendre obligatoire le consentement de la personne identifiée sur une photo et ce, préalablement à sa publication. Afin que le consentement soit valide, l'individu doit également être informé de manière appropriée sur le traitement.

Parmi les autres risques posés par de tels systèmes, le groupe a cité, entre autres, les traitements de données illégaux, les failles de sécurité lors d'un transfert et le manque de précision de la reconnaissance faciale. Le groupe de travail a fait plusieurs recommandations afin de minimiser ces risques. En l'occurrence, le responsable du traitement doit toujours s'assurer d'avoir le consentement de la personne concernée et prendre les mesures nécessaires pour assurer la sécurité lors d'un transfert de données. Il doit, par ailleurs, donner les moyens appropriés aux personnes concernées pour qu'elles puissent exercer leur droit d'accès.

Les activités en 2012

2.6.1.5 *Mise en garde face aux dérives potentielles des technologies biométriques*

Dans son avis du 27 avril 2012, le groupe « Article 29 » a commenté les développements récents dans le domaine des technologies biométriques.

Les dispositifs biométriques sont particulièrement sensibles, parce qu'ils permettent d'identifier une personne par ses caractéristiques physiques, biologiques voire comportementales.

La biométrie peut présenter un certain nombre d'avantages : sécurité accrue des données, protection et lutte contre la fraude ou le vol d'identité, non transmissibilité des données, identification positive et davantage de confort. De plus, les données biométriques sont utilisées avec succès et de manière efficace dans le domaine de la recherche scientifique et pour les systèmes de contrôle d'accès.

Il faut cependant rester prudent quant aux utilisations qui peuvent être faites de la biométrie, car l'information biométrique est surtout une caractéristique propre à tout être vivant, comme les empreintes des doigts, la configuration des veines ou l'ADN, et elle ne peut pas être effacée ou modifiée. C'est pour cette raison que les technologies biométriques posent un risque par rapport à la protection de la vie privée des personnes concernées.

L'évolution technologique a encore amplifié ce risque en permettant la création de galeries d'images en ligne et de réseaux sociaux avec des millions de photos. Les lecteurs d'empreintes digitales et les systèmes de vidéosurveillance sont désormais beaucoup plus accessibles. Même les tests d'ADN sont devenus abordables et peuvent être effectués rapidement.

Selon le G29, l'ajout de systèmes de reconnaissance faciale, basés sur les banques de données des réseaux sociaux, aux dispositifs de vidéosurveillance ou aux smartphones pourrait mettre fin à l'anonymat et au droit des individus d'aller et de venir librement.

2.6.1.6 *Recommandations concernant l'utilisation de « cookies »*

Le groupe « Article 29 » a examiné l'impact de la révision de la directive « e-privacy »[11] sur l'utilisation des « cookies ». Selon cette directive, révisée en 2009 et transposée en droit national par la loi du 28 juillet 2011[12], il est possible de placer des cookies sur l'ordinateur

[11] Directive 2002/58/CE

[12] portant modification de la loi modifiée du 30 mai 2005 concernant la vie privée dans le secteur des communications électroniques.

de l'utilisateur à condition de recevoir son consentement explicite. Dans sa prise de position, le groupe a analysé en particulier les exceptions à ce principe d'opt-in.

Les « cookies », c'est quoi exactement ?

Le « cookie » ou témoin de connexion est un petit fichier texte au format alphanumérique déposé sur le disque dur de l'internaute par le serveur du site visité ou par un serveur tiers (régie publicitaire, service de web analytique, etc.). Dans l'ordinateur, c'est le navigateur (Internet Explorer, Firefox, Chrome, Safari, etc.) qui gère les cookies et qui permet à l'internaute de les contrôler. En principe, les cookies servent à faciliter l'utilisation ultérieure d'un site par la même personne. Ainsi, il permet notamment de reconnaître un visiteur lorsqu'il revient sur un site web, de se rappeler de la langue que l'internaute avait choisie lors de sa visite précédente ou des produits qu'il avait déposés dans son panier lors d'une session de shopping antérieure.

Toutefois, l'utilisation de cookies pourra avoir une implication importante sur la vie privée des internautes, s'ils sont employés à d'autres fins comme par exemple la gestion publicitaire, le profilage ou le traçage des internautes. Dans son avis 2/2010 (WP 171) sur la publicité comportementale en ligne, le groupe de travail avait analysé en détail cette problématique. Requêtes dans un moteur de recherche, clics et autres informations sont analysés pour proposer des publicités personnalisées aux internautes. Dans ces cas, les cookies sont placés par une partie tierce différente de l'éditeur du site et on parle de « third party cookies ».

Exceptions au principe du consentement explicite

Selon l'article 5, paragraphe 3 de la Directive « e-privacy », il est possible de placer un « cookie » sans le consentement explicite de l'internaute dans les deux cas suivants :

(1) le cookie vise « *exclusivement à effectuer ou à faciliter la transmission d'une communication par la voie d'un réseau de communications électroniques* » ;

(2) le cookie est « *strictement nécessaire à la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur* ».

Ainsi, sous certaines conditions, cela inclut les « user-input cookies » ou « session-id cookies » (lorsque l'utilisateur remplit un formulaire ou un panier d'achats), les « multimedia player session cookies » (qui enregistrent les données techniques nécessaires pour consulter des contenus vidéo et audio) ainsi que les « user interface customization cookies » (permettant notamment de se rappeler de la langue choisie par l'utilisateur lors d'une visite antérieure).

En ce qui concerne les cookies utilisés pour mesurer l'audience statistique d'un site (« Analytics »), le groupe de travail a estimé qu'ils ne posaient pas de risque par rapport à la vie privée lorsqu'ils sont directement placés par le site visité (et non par une partie tierce) à des fins statistiques et lorsque les visiteurs sont informés clairement sur leur utilisation dans les règles de confidentialité. Il faut cependant demander le consentement de l'utilisateur avant de placer ce type de cookie.

De nombreux réseaux sociaux proposent des « plugins sociaux » qu'un opérateur de site web peut intégrer sur son site, notamment pour permettre aux visiteurs de partager des contenus avec leurs « amis ». Ces plugins, lorsqu'ils sont utilisés, permettent

aux réseaux sociaux d'accéder aux cookies pour identifier leurs membres. Dans ce cas, il faut distinguer les membres connectés de ceux qui ne le sont pas ou qui ne sont tout simplement pas membres du réseau social. S'il s'agit d'un membre connecté d'un réseau social, il n'est pas nécessaire de demander son consentement explicite. Le groupe de travail a noté toutefois que l'utilisation des plugins sociaux de tiers pour toute autre fin que de fournir un service expressément demandé par l'utilisateur nécessite l'obtention de son consentement. Ainsi il est strictement interdit d'utiliser ces « social plugins » pour observer le comportement de l'utilisateur à travers de multiples sites ou pour sauvegarder les données de non-membres sans leur accord.

2.6.1.7 *Google dans la ligne de mire des autorités de protection des données pour la modification de ses règles de confidentialité*

En octobre 2012, les autorités de protection des données européennes ont sommé Google de modifier ses nouvelles règles de confidentialité entrées en vigueur le 1er mars 2012. L'autorité française CNIL a publié les conclusions communes de plusieurs mois d'enquête sur le sujet. Les 27 autorités européennes ont préconisé une information plus claire des personnes et ont demandé à Google d'offrir aux utilisateurs un meilleur contrôle de leurs données. Enfin, elles ont recommandé à Google de modifier les outils utilisés afin d'éviter une collecte excessive de données.

Dans le courrier adressé à Google, les autorités européennes ont estimé que le géant de l'Internet devait *« prendre des mesures effectives et publiques pour se mettre en conformité rapidement »*.
De plus, elles ont demandé à la société américaine de leur *« indiquer comment et dans quel délai elle va mettre à jour sa politique de confidentialité et ses pratiques pour intégrer ses recommandations »*.

Enquête menée par la CNIL sur les nouvelles règles de confidentialité de Google

Le G29 avait d'ailleurs vivement critiqué la nouvelle politique de Google en février 2012. Cette politique simplifiée permet au géant américain d'unifier les règles de confidentialité de tous ses services, comme Gmail, Google+ ou YouTube, et par conséquent de partager plus aisément les données des utilisateurs.

Face aux nombreuses questions soulevées par ces changements, le G29 a mandaté la CNIL pour conduire une enquête. Google n'a pas fourni de réponses satisfaisantes à deux questionnaires de la CNIL sur des points essentiels comme la description de tous les traitements ou la liste précise des plus de 60 politiques de confidentialité qui ont été fusionnées dans les nouvelles règles.

Selon le G29, l'analyse menée ne permettait pas de s'assurer que Google respectait les principes essentiels des règles européennes en matière de protection des données personnelles que sont la limitation de finalité, la qualité et la minimisation des données, la proportionnalité et le droit d'opposition.

En effet, les nouvelles règles de confidentialité suggèrent l'absence de toute limite concernant le périmètre de la collecte et les usages potentiels des données personnelles. Google a « *également refusé expressément de répondre sur une durée maximale de conservation des données* » a indiqué la présidente de la CNIL, Isabelle Falque-Pierrotin.

Manque de transparence

Google ne fournit pas suffisamment d'informations aux utilisateurs sur ses traitements de données personnelles. Les utilisateurs sont incapables de déterminer quelles sont les données personnelles utilisées pour ce service et les finalités exactes pour lesquelles ces données sont traitées.

En l'occurrence, les règles de Google ne font pas de différence de traitement entre le contenu anodin d'une recherche et les communications téléphoniques de l'utilisateur. Toutes ces données peuvent être utilisées indifféremment pour toutes les finalités mentionnées dans les règles.

Pas de contrôle sur la combinaison des données entre les différents services

Toute activité en ligne liée à Google (l'utilisation de ses services, de son système Android ou la consultation de sites tiers utilisant des services Google) peut être rassemblée et combinée. Le G29 a relevé que cette combinaison poursuit des finalités autres que la fourniture du service demandé par la personne, le développement de nouveaux produits, la sécurité, la publicité, la création du compte Google ou encore la recherche académique.

Google doit disposer d'une base légale pour réaliser la combinaison de données pour chacune de ces finalités.
La collecte doit également demeurer proportionnelle aux finalités poursuivies. Or, pour certaines de ces finalités, notamment la publicité, Google ne peut pas s'appuyer sur le consentement de la personne, l'intérêt légitime de Google ou l'exécution d'un contrat. L'entreprise américaine doit donc modifier ses pratiques en accordant aux utilisateurs plus de contrôle sur leurs données.

2.6.1.8 Document de travail sur epSOS (Dossier médical électronique)

Le groupe « Article 29 » a élaboré un document de travail sur le projet pilote epSOS (European Patients Smart Open Services), qui propose des services transfrontaliers de santé en ligne aux citoyens européens. Son objectif est de mettre en place un cadre pratique de « e-Santé » et une infrastructure qui permette d'accéder à des informations sur la santé des patients, provenant de différents systèmes européens de soins de santé. Il vise à améliorer la qualité de ces soins pour les citoyens qui voyagent d'un pays européen à l'autre.

Deux usages sont prévus pour le projet epSOS :

- un dossier du patient contenant des données médicales et accessible aux professionnels de la santé en vue du traitement du patient ; et

- l'utilisation transfrontalière des prescriptions électroniques.

Dans son document de travail, le G29 a abordé les questions suivantes :

- la base juridique du traitement des données dans le cadre du projet, y compris le principe de proportionnalité et la limitation des finalités ;

- les questions d'organisation ;

- la transparence ; et

- la sécurité des données.

2.6.2 Le 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 2012, le T-PD s'est penché principalement sur la révision de la Convention 108. Son processus de modernisation a débuté à l'occasion de la 5e édition de la Journée de la Protection des Données (28 janvier 2011), lorsque le Secrétaire Général du Conseil de l'Europe a lancé une consultation publique visant à recenser les préoccupations des gouvernements, de la société civile et du secteur privé.

Quelque 50 réponses ont été reçues (soit environ 400 pages) de tous les secteurs concernés : gouvernements, autorités de la protection des données, ONG, secteur privé, associations professionnelles y compris de nombreux contributeurs non-européens, essentiellement des Amériques et d'Afrique.
Ces réponses ont été analysées et prises en compte dans les propositions de modernisation.

La révision du processus poursuit deux objectifs majeurs :

- gérer les défis par rapport à la vie privée qui résultent de l'utilisation des nouvelles technologies de l'information et de la communication ;

- renforcer le mécanisme de suivi de la Convention.

Un large consensus s'est dégagé sur les objectifs à poursuivre, qui sont également clairement

ressortis de la consultation publique, à savoir :

- maintenir la nature générale et technologiquement neutre des dispositions de la Convention, avec des textes sectoriels plus détaillés, au moyen d'instruments juridiques non-contraignants (avis et recommandations) ;

- assurer la cohérence et la compatibilité avec le cadre juridique de l'Union européenne ;

- réaffirmer la vocation universelle et le caractère ouvert de la Convention.

La modernisation de la Convention devrait permettre aux particuliers de mieux superviser leurs données et responsabiliser davantage les Etats et entreprises qui traitent des données à caractère personnel.

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 télécommunication et sur Internet.

Lors de deux réunions en 2012 à Sopot (Pologne) et Berlin (Allemagne), le groupe a adopté un document de travail sur le cloud computing. D'autres sujets abordés lors de ces réunions étaient l'utilisation du protocole Internet IPv6, le « droit à l'oubli », le traçage sur Internet et les réseaux sociaux.

Le cloud computing

Le Groupe de Berlin a adopté un document de travail dans lequel il a examiné les traitements de données à caractère personnel dans des environnements de cloud computing. Ce papier se limite au cas où des entreprises ou administrations publiques utilisent le cloud computing et ne s'applique donc pas à son utilisation par des particuliers.
Le cloud computing peut présenter de nombreux avantages. Il désigne un concept qui consiste à accéder à des données et services sur un serveur distant. L'entreprise n'utilise pas sa propre infrastructure pour héberger ses données, mais un serveur distant se trouvant « dans un nuage » (« cloud »). Il existe désormais de nombreux services de cloud computing, fournis à la demande. Ils peuvent proposer le même service à un grand nombre d'utilisateurs, et donc amortir les coûts de fonctionnement sur toute la base d'utilisateurs.

De nombreuses entreprises (surtout les PME) peuvent ainsi faire des économies en utilisant ce type de services auxquels ils n'avaient pas accès avant.

En dépit de ses avantages, l'usage du cloud computing pour traiter des données à caractère personnel peut comporter des risques. Le Groupe de Berlin a notamment cité un risque plus élevé de violations de la sécurité, la possibilité que les données soient transférées vers des pays sans protection adéquate, le manque de contrôle par rapport aux données personnelles ou encore une information insuffisante sur les modalités du traitement des données par un service « cloud ».

Afin de minimiser ces risques, le groupe de travail a fait des recommandations pour une utilisation responsable du cloud computing. Selon le groupe, le cloud computing ne devrait pas conduire à une baisse des standards de la protection des données. Les responsables du traitement devraient effectuer des études d'impact sur la protection de la vie privée avant de se lancer dans de tels projets. Les fournisseurs de services « cloud » devraient se montrer plus transparents envers leurs clients en la matière. De plus, davantage d'efforts devraient être faits dans le domaine de la recherche. Il faudrait également prendre en compte la protection de la vie privée dès la conception (« Privacy by design »).

2.6.4 Le séminaire d'échange d'expériences « Case Handling Workshop »

L'autorité de protection des données hongroise a organisé le séminaire européen « Case Handling Workshop » les 3 et 4 septembre 2012 à Budapest.

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

En 2012, le séminaire a abordé les thèmes suivants :

- les amendes - présentation d'exemples européens ;
- les méthodes d'investigation ;
- les contrôles judiciaires des décisions des autorités de protection des données ;
- la vidéosurveillance dans les transports publics ;
- le traitement de données personnelles dans le cadre d'activités d'associations religieuses ;
- le traitement de données sensibles se rapportant à des patients SIDA/HIV.

3 Les temps forts de 2012

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 La réforme de la protection des données européenne

La protection des données fait actuellement l'objet d'un important débat au niveau européen. Le processus législatif, visant à remplacer la directive 95/46/CE, a commencé le 25 janvier 2012 lorsque la Commission européenne a présenté ses propositions pour réformer le cadre légal règlementant la protection des données dans l'Union européenne. Le paquet de mesures contient deux volets : un règlement général sur la protection des données et une directive spécifique pour le domaine de la police et de la justice.

La réforme tient compte des progrès technologiques rapides et de la globalisation, phénomènes qui ont modifié en profondeur la manière de collecter, de consulter et d'utiliser les données de l'individu.

Les nouvelles technologies numériques de l'information et de la communication telles qu'Internet permettent d'échanger et de rendre disponibles, à l'échelle mondiale, des informations avec une aisance et une rapidité accrues.

Objectifs

Dans le contexte d'une meilleure harmonisation au niveau européen, les propositions visent à améliorer la protection des données en offrant aux citoyens la possibilité de mieux contrôler ce qui advient de leurs données, en responsabilisant davantage les détenteurs de données, en rendant plus efficace l'exécution des dispositions légales en la matière et en renforçant les pouvoirs des autorités de contrôle.

Le projet de règlement européen vise trois objectifs :

1) Renforcement des droits des citoyens

Il s'agit d'abord de permettre aux citoyens de renforcer leurs droits déjà existants conformément aux textes précédents, et surtout de mieux les exercer. Les propositions de la Commission européenne sont conçues pour garantir la protection des informations personnelles des citoyens - quel que soit le lieu où elles sont envoyées ou conservées

- même en dehors de l'Union européenne, comme cela peut souvent être le cas sur Internet. Cela vaut donc également pour des sociétés comme Google ou Facebook, basées aux Etats-Unis. Parmi les nouveautés, on trouve le droit à l'oubli numérique ou la protection renforcée des mineurs, ainsi que la possibilité d'interdire le profilage des données. Les citoyens pourront notamment obtenir la suppression de données les concernant si aucun motif légitime ne justifie leur conservation, que ce soit sur un moteur de recherche ou un réseau social. La transparence pour mieux accéder à ses propres données et le principe de finalité sont mieux encadrés.

2) Renforcement de la responsabilité et de l'obligation de rendre compte des acteurs qui gèrent la collecte de données

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

Avec le nouveau règlement, les citoyens et les entreprises

n'auront plus qu'une seule autorité nationale comme interlocuteur (« guichet unique »). Les citoyens pourront ainsi s'adresser à leur autorité nationale, même quand leurs données à caractère personnel sont traitées en dehors de leur pays d'origine. Les entreprises n'auront à traiter qu'avec l'autorité de contrôle du pays de l'Union où se trouve leur siège principal.

3) Renforcement des compétences des autorités nationales responsables de la protection des données

Le troisième objectif consiste à renforcer les compétences des autorités nationales responsables de la protection des données, afin qu'elles puissent mieux faire appliquer les règles de l'Union européenne dans leur pays. Au Luxembourg, cette initiative européenne aura une influence importante sur le fonctionnement de la Commission nationale et sur les citoyens. La Commission nationale pourra ainsi infliger des amendes, mais elle devra aussi être en mesure de collaborer efficacement avec les entreprises qui traitent des données à caractère personnel. Etant donné que les autorités de chaque pays seront chargées de centraliser les plaintes de leurs ressortissants, même si elles visent une entreprise qui ne se trouve pas sur leur territoire, le règlement exigera une collaboration plus étroite entre les différentes autorités nationales. Celles-ci seront chapeautées par une autorité européenne, l' « European Data Protection Board ». Les attentes des citoyens à l'égard de la Commission nationale en vue de l'application de la loi vont être beaucoup plus importantes.

Calendrier

Le projet de règlement doit encore passer plusieurs étapes législatives avant d'être validé. Le texte définitif devrait être adopté début 2014 et entrer en vigueur deux ans plus tard.

Les propositions de la Commission européenne ont été transmises au Parlement européen et aux Etats membres de l'UE (qui se réunissent au sein du Conseil des ministres) pour y être examinées et débattues.

Le Groupe de l'Article 29 a déjà rendu deux avis[13] sur ces textes. Ils proposent notamment des améliorations concernant la définition des données personnelles, la notion de consentement, les actes délégués et d'application, les dérogations aux transferts internationaux de données, la notification des failles de sécurité et le droit à l'oubli. La deuxième prise de position tient également compte des discussions qui ont eu lieu dans la commission LIBE du Parlement européen. Les 9 et 10 octobre,

[13] Voir partie 2.6.1.2

cette commission a organisé une réunion interparlementaire avec des membres des parlements nationaux, afin de débattre des instruments législatifs proposés dans le cadre de la réforme. En juin 2012, les rapporteurs (Jan Philipp Albrecht et Dimitrios Droutsas) ont présenté un document de travail soulignant les principaux éléments de la réforme, préconisant une approche globale et mettant en évidence plusieurs thèmes nécessitant de plus amples débats et clarifications. Des discussions ont également eu lieu au niveau du groupe de travail du Conseil via le Groupe de travail chargé des questions concernant les échanges d'informations et la protection des données (DAPIX).

Consultation publique ministérielle au Luxembourg

Le ministre des Communications et des Médias a lancé, le 28 mars, une vaste consultation nationale de toutes les personnes, entreprises, associations et autres organisations intéressées à commenter la proposition de règlement de la Commission européenne.

Dans le cadre de cette consultation, la Commission nationale a présenté au service du ministre des Communications et des Médias ses observations et recommandations lors d'échanges de vues réguliers. L'ABBL (Association des Banques et Banquiers Luxembourg) et la FEDIL (Business Federation Luxembourg) se sont également prononcées sur le projet de règlement européen.

L'ABBL a noté dans son avis que l'activité bancaire implique de la part des professionnels du monde de la finance la gestion d'un nombre important de données personnelles. Parallèlement aux informations relatives à leurs clients, les banques gèrent, par nécessité, des données relatives à des tiers (comme par exemple dans la lutte contre le blanchiment d'argent). Ces informations sont indispensables à leur bon fonctionnement. De ce fait, l'ABBL est d'avis que l'existence même de l'ensemble de ces fichiers ne doit pas être mise en péril par les règles relatives à la protection des données et a proposé que le législateur européen établisse l'ordre de primauté des règles issues des règlements et directives européennes.

L'ABBL a ensuite suggéré de prévoir des exceptions aux règles relatives au consentement et à l'information des personnes concernées, notamment dans le domaine de la prévention des fraudes. Il serait en effet incompatible avec la logique de prévention des fraudes qu'il soit imposé aux banques de recueillir le consentement des fraudeurs pour que les données les concernant soient répertoriées.

Dans sa prise de position, l'ABBL a encore critiqué que de nombreuses dispositions de la proposition de règlement utilisent des termes flous aux alentours incertains, que seuls des actes délégués viendront compléter ultérieurement. Selon elle, la possibilité prévue pour la Commission d'adopter des actes délégués devrait être remplacée par des clarifications introduites dans le dispositif du règlement.

Dans son avis sur la proposition de règlement, la FEDIL a également critiqué le pouvoir important revenant à la Commission européenne grâce aux actes délégués. D'après la FEDIL, cet instrument qui pourra être appliqué dans plusieurs domaines importants introduirait une trop grande insécurité juridique.

Si la FEDIL accueille favorablement les grandes lignes de la réforme, elle juge néanmoins qu'il est nécessaire, pour trouver un juste équilibre, d'adopter une approche plus pragmatique et orientée vers les résultats. Au lieu de suivre une approche axée sur des principes comme la responsabilisation des acteurs, le contexte dans lequel les données sont traitées et les risques réels pour les individus,

3 Les temps forts de 2012

la Commission européenne a opté pour un projet de règlement prescriptif. La FEDIL craint qu'une telle approche puisse augmenter les charges inutiles pour les entreprises, être sans aucun bénéfice pour l'individu et, plus important encore, freiner l'innovation et la croissance économique en Europe.

3.2 Conférence annuelle des autorités européennes à la protection des données à Luxembourg

Du 2 au 4 mai 2012, le Luxembourg a accueilli la conférence de printemps (« *Spring Conference* ») des commissaires européens à la protection des données dans l'amphithéâtre de la Cour des comptes européenne. La conférence a réuni 130 délégués des autorités de 38 pays ainsi que les représentants de la Commission européenne, du Conseil de l'Europe et de l'OCDE. A cette occasion, la Vice-présidente de la Commission européenne a adressé un message remarqué aux membres des autorités de protection des données participantes. La composition et les sujets de différentes sessions font ressortir l'intérêt et l'intensité des discussions de cette conférence qui a recueilli un succès remarquable.

La réforme de la protection des données européenne confrontée aux attentes !

Le paquet législatif sur la protection des données, présenté par la Commission européenne le 25 janvier 2012, a été au centre des discussions, comme en témoigne le thème de la conférence : « *La réforme de la protection des données européenne confrontée aux attentes !* ».

A côté des interventions du ministre des Communications et des Médias, François Biltgen, et de Viviane Reding, Commissaire européenne à la Justice et aux Droits fondamentaux, les discussions entre les délégués se

« Spring Conference »

sont tenues autour de six séances réparties sur deux journées.

Le nouveau cadre européen dans un monde globalisé

Lors d'une première table ronde présidée par le Superviseur européen Peter Hunstinx, le commissaire fédéral allemand Peter Schaar et son collègue britannique Christopher Graham sont notamment intervenus au sujet des défis et enjeux majeurs de la récente proposition législative de la Commission européenne.

Si les travaux de la conférence ont principalement porté sur la protection des données en Europe et en particulier dans l'Union européenne, la réflexion des commissaires a également été menée en tenant compte du contexte de l'évolution en matière de « privacy » dans d'autres parties du monde. La participation de David Vladeck, directeur de la Federal Trade Commission aux Etats-Unis (FTC), a particulièrement retenu l'attention, puisqu'il a exprimé un point de vue transatlantique sur les nouvelles dispositions proposées par la Commission européenne. L'approche américaine est généralement considérée comme plus incitative, davantage basée sur l'autorégulation et moins prescriptive.

Cette approche a eu le soutien de Christopher Graham, qui a demandé plus de flexibilité et un projet de règlement moins détaillé, donc une meilleure protection des données dans la pratique et pas dans les textes réglementaires difficilement applicables. Françoise Le Bail, directrice générale de la DG Justice de la Commission européenne, a défendu l'idée de la règle unique qui éviterait la fragmentation des différentes législations nationales. Peter Schaar a expliqué qu'une règle unique sera seulement acceptée, si elle reprend les normes de protection les plus élevées pour ne pas régresser par rapport aux lois nationales.

Les droits de la protection des données dans un monde connecté

La deuxième séance, présidée par la présidente de l'autorité française CNIL, Isabelle Falque-Pierrotin, a porté sur le renforcement des droits des utilisateurs de services sur Internet, notamment dans le contexte du cloud computing et des réseaux sociaux.

3 Les temps forts de 2012

Les questions du droit à l'oubli sur Internet et de la protection des mineurs ont également été abordées dans ce contexte.

Si ce principe est difficilement applicable en pratique, « *il reste cependant important que le droit à l'oubli reste dans le règlement, car les circonstances et les moyens technologiques peuvent changer et rendre le principe, juste en soi, plus aisément applicable* »[14].

A l'aide d'un exemple local, Janni Christoffersen, directrice de l'autorité du Danemark, a illustré les défis du cloud computing, en particulier lorsque les données sont traitées et conservées dans des pays tiers. Finalement, le commissaire irlandais Billy Hawkes s'est penché sur le rapport d'investigation de son autorité de contrôle sur le réseau social Facebook.

La réduction des contraintes administratives

Une troisième table ronde a porté sur la simplification des obligations administratives des acteurs, en faveur d'une plus grande responsabilisation.
A côté de l'allègement des contraintes administratives, les commissaires ont discuté des nouveaux outils pour améliorer la protection, notamment les PIA (« Privacy Impact Assessments »), du développement du rôle du chargé de la protection des données et des principes de « Privacy by Design » et « Privacy by Default ».

Le panel s'est achevé par une présentation sur les BCR et les clauses contractuelles. Ceux-ci

[14] Europaforum.lu: « L'avenir de la protection des données dans l'UE discuté à Luxembourg par les chefs des autorités nationales compétentes ».

assurent une protection appropriée pour les flux de données internationaux. Les commissaires ont notamment discuté des modifications induites par le projet de règlement européen.

Le rôle renforcé des autorités de contrôle

La quatrième séance était dédiée à l'évolution du rôle des autorités nationales de protection des données dans le cadre du système du « guichet unique », qui fait que les citoyens et les entreprises n'auront plus qu'une seule autorité nationale comme interlocuteur.

Le président du Groupe « Article 29 » Jacob Kohnstamm, qui a présidé cette séance, a insisté sur le fait que le règlement européen demandera une collaboration plus étroite entre les différentes autorités nationales. Il a estimé que le système du « one-stop-shop » ne devra pas être compris dans le sens qu'une seule autorité sera exclusivement compétente pour une entreprise donnée, mais qu'elle coordonnera plutôt la prise de décision.

Résolution sur la réforme de la protection des données européenne

Lors de la deuxième journée de conférence, des tables rondes spécifiques ont porté sur la protection des données dans le domaine de la police et de la justice, ainsi que sur la modernisation des autres instruments juridiques internationaux (Convention 108 du Conseil de l'Europe et lignes directrices de l'OCDE).

A la fin de la conférence, les commissaires ont adopté une résolution dans laquelle ils ont noté que la proposition actuelle nécessitait encore des améliorations, en particulier en ce qui concerne la directive sur la police et la justice. Celle-ci devra être adaptée pour correspondre davantage aux principes fondamentaux du règlement général sur la protection des données. En l'occurrence, des règles sur le transfert de données entre entités privées et organes répressifs manquent toujours.

Pour la suite du processus législatif, les commissaires sont préparés à contribuer de manière active à la modernisation du cadre légal relatif à la protection des données en Europe.

Message de Viviane Reding aux commissaires

La Vice-présidente de la Commission européenne, Viviane Reding, a défendu les grandes lignes de la réforme dans son message adressé aux participants : *« La réforme de la protection des données, présentée par la Commission européenne, établit un seul et même*

Les temps forts de 2012

ensemble de règles de protection des données fortes qui assurent davantage de contrôle sur leurs données à nos citoyens tout en rendant plus aisé aux entreprises d'être en conformité pour tirer profit du Marché Unique. Mais une législation uniforme, ce n'est pas suffisant. Nous avons aussi besoin que quelqu'un veille à ce que ces règles soient appliquées partout à travers l'UE, et partout de la même façon. C'est pour cela que notre réforme renforce considérablement le rôle des autorités de contrôle national et harmonise leurs missions et pouvoirs de façon à ce qu'elles puissent faire de ces règles une réalité effective pour les 500 millions de citoyens européens et les entreprises ».

Ensuite elle a répondu à un certain nombre de critiques, notamment en ce qui concerne les actes délégués par lesquels le règlement peut être amendé. Elle a noté que le recours à l'acte délégué se fera seulement si des adaptations s'avèrent nécessaires suite à certains changements technologiques, et qu'il ne s'agit pas d'un instrument pour empiéter sur les pouvoirs des autorités nationales de protection des données.
La commissaire européenne a également abordé la question du « one-stop-shop », qui implique que l'autorité de protection des données de l'Etat où une entreprise a son siège principal sera le point de contact de cette entreprise, et elle a noté que ce principe implique qu'il faut donner des moyens adéquats aux autorités nationales.

Madame Reding a par ailleurs souligné qu'elle est consciente que les autorités nationales ne sont pas satisfaites du projet de directive dans le domaine de la police et de la justice. A son avis, ce texte constitue néanmoins un progrès et le choix de la directive a été fait pour donner aux Etats membres des marges d'appréciation lors de la transposition.

Discours de Monsieur le Ministre François Biltgen

Le ministre François Biltgen, en sa double qualité de ministre de la Justice et ministre des Communications et des Médias, a appuyé l'approche pragmatique et moderne de la Commission européenne dans son discours : « *Au niveau européen, cette approche se traduit par la nécessité de disposer des mêmes règles dans tous les Etats membres. Ces règles se doivent d'être des plus claires si nous voulons renforcer la protection des données personnelles de tous les citoyens européens tout en établissant un marché intérieur complet en matière d'économie numérique, il faut que chacun sache à quoi s'en tenir – les citoyens aussi bien que les entreprises. Evitons donc des règles trop complexes, divergentes et obscures. La même réflexion vaut pour les citoyens et pour les entreprises.*

Voilà pourquoi nous pensons que l'adoption de règles claires et pragmatiques à travers le marché intérieur, associées au « one-stop-shop » tant pour les entreprises que pour les citoyens, n'apportera que des avantages pour tous les concernés. Il s'agit d'une véritable situation win-win. C'est la protection des données personnelles de nos citoyens qui en sortira gagnante avec un même niveau de protection élevé et avec les mêmes droits sur l'ensemble du territoire de l'Union. D'où encore une fois, et je le répète, notre appui à la solution du règlement pour justement établir l'équilibre entre protection des données et libre circulation ».

François Biltgen espère qu'on pourra faire émerger une véritable culture de la protection des données : « *Dans cette nouvelle culture, les autorités nationales doivent jouer un rôle-clé comme le prévoit le projet de la Commission. La protection des données est devenue un réel sujet de débat dans la société civile, les enjeux quotidiens et la prise de conscience des citoyens augmentée, je m'en félicite.*

En conséquence nous devons oeuvrer pour doter les autorités de moyens juridiques, financiers et humains adéquats pour leur accorder les instruments juridiques appropriés qui leur permettront d'accomplir les missions complexes avec efficacité et circonspection ».

4 Perspectives

Les affaires qui ont défrayé la chronique dans les médias internationaux au cours des dernières années - de SWIFT à Google Street View, de l'espionnage des salariés de Lidl au trafic des fichiers de données/consommateurs et de leur emploi abusif par des call center allemands, numéros de téléphone et de comptes bancaires compris, du traçage de géolocalisation des utilisateurs par leurs « smartphones » aux modifications subreptices des conditions générales d'utilisation de Facebook et Google, mais aussi de la dissémination en ligne des données des abonnés de la SNCB au Médicoleak luxembourgeois - sont toutes révélatrices d'une nouvelle sensibilité de l'opinion publique à l'égard des enjeux de la protection de la vie privée. Cette constatation est en contradiction avec celle d'un comportement trop souvent négligent de bon nombre d'utilisateurs d'internet en général et des réseaux sociaux en particulier, hâtivement interprété comme expression d'une nouvelle transparence décomplexée de la jeunesse qui aurait accepté une fois pour toutes que la recherche de « privacy » serait une valeur d'un autre âge, démodée et ringarde, car devenue irréaliste et inutile dans l'ère numérique et à laquelle il conviendrait donc de ne plus s'attacher.

Au Grand-Duché aussi des sujets de protection des données ont fait l'objet de débats publics, que ce soit sur la sécurisation améliorée des fichiers publics, l'introduction d'un fichier central des élèves de l'Education Nationale, les restrictions d'accès, la richesse des données y inscrites, leur anonymisation en cas d'utilisation à des fins de statistique et de recherche, etc., la conservation injustifiée des renseignements de fichage individuel établis il y a des décades par le Service de renseignement de l'Etat et les standards futurs auxquels ce service devrait être astreint à l'avenir.

C'est une attention toute particulière qu'a acquise dans notre société connectée d'aujourd'hui, la question du juste équilibre entre les formidables possibilités techniques du traitement de l'information en constante évolution et les restrictions et garanties qui doivent encadrer leur mise en oeuvre pour la préservation des libertés et droits fondamentaux de l'individu.

La responsabilité du législateur, mais aussi celle de l'autorité qu'il a chargée de contrôler la bonne application de la loi s'en retrouve accentuée. Le Luxembourg peinait un peu à voir s'établir une véritable culture

de la protection des données à caractère personnel dans les entreprises, administrations et organismes publics constations-nous dans le contexte de la révision de la loi de 2002 en 2007, et nous comptions alors sur la simplification des contraintes administratives au profit d'une responsabilisation accrue des acteurs pour faciliter le respect des dispositions légales en la matière et voir développer des modèles de bonnes pratiques dans le cadre du traitement des informations relatives aux administrés, aux clients ou patients, utilisateurs, salariés, visiteurs, etc.

Des progrès sont indéniables, encore qu'apparaisse également la nécessité de voir flanquer les moyens de sensibilisation, d'information et de constatation de la CNPD de véritables moyens d'intervention efficaces autres que par l'intermédiaire de la justice.

C'est une démarche similaire que le législateur européen s'apprête à faire entrer dans le futur cadre juridique communautaire, qui devrait non seulement donner aux principes essentiels développés depuis la Convention 108 du 28 janvier 1981 une application mieux harmonisée dans les Etats membres et un rayonnement transversal accru dépassant le contexte du premier pilier de l'époque précédent le traité de Lisbonne - le paquet législatif présenté le 25 janvier 2012 par la Commission Européenne comprend en effet un projet de règlement européen ainsi qu'un projet de directive applicable dans les domaines judiciaire et policier - mais aussi contribuer de façon décisive à faire entrer des textes doctrinaux dans la réalité pratique de tous les jours.

C'est ce que la Vice-présidente Viviane Reding, Commissaire à la Justice et aux Droits des citoyens s'efforce d'obtenir à travers une réforme équilibrée qui comporte son lot d'améliorations et de simplifications en faveur des entreprises, organisations et organismes publics collectant et traitant des données, mais qui s'attache en tout premier lieu à accorder au citoyen et consommateur un meilleur contrôle de ses données.

La « Durchsetzbarkeit » (« force exécutoire, enforceability ») des droits individuels inscrits dans les futurs textes devrait sortir considérablement renforcée de la réforme en raison de ses trois accents nouveaux :
« accountability (obligation de rendre compte) » des acteurs ; transparence, actions et recours à disposition de la personne concernée ; pouvoirs accrus et coopération des autorités de protection des données. Il nous semble que les trois années qui s'écouleront probablement avant l'entrée en vigueur des textes actuellement en débat au Parlement européen et au Conseil, devraient être mises à profit pour se préparer, chacun à son niveau, au nouvel environnement.

Aussi faisons-nous appel aux entreprises et aux acteurs publics de se préparer à être tenus comptables pour la protection des données individuelles traitées, notamment à mettre en place l'organisation nécessaire, compte tenu de l'envergure et de la sensibilité des fichiers, de l'attribution de responsabilité interne et de la formalisation des procédures. Pour les entités d'une certaine taille - et celles dont la nature de l'activité le commande - cela signifie qu'il faudra désigner et former un chargé de la protection interne, parfaire le recensement et l'analyse des processus et traitements touchant à des informations à caractère personnel, revoir la sécurisation des systèmes informatiques, les pratiques suivies en terme d'audit et de gestion des plaintes, etc. Les dispositions proposées permettent d'ailleurs de désigner des chargés qui se verront confier leur mission à côté de leur fonction actuelle au sein

4 Perspectives

de l'organisation ou l'assureront comme consultants externes, pour une ou collectivement pour plusieurs entreprises ou entités publiques, et qui auront donc la flexibilité nécessaire pour ne pas poser des problèmes insurmontables ou représenter un coût inacceptable de la mise en conformité.

Les activités des administrations et organismes publics devront être suivies systématiquement par des chargés de la protection des données, ce qui promet de contribuer à une culture de la protection des données plus homogène au sein des pouvoirs publics. Aujourd'hui il paraît nécessaire que l'Etat ainsi que les services et établissements publics se préparent à assumer leur responsabilité en la matière de façon plus « proactive », suivant la nouvelle démarche de l' « accountability ». L'actualité nationale récente nous conduit à penser qu'un renforcement de la culture de la protection des données et des libertés individuelles serait souhaitable également au niveau des autorités, relevant de l'article 17 de la loi. Dans cette perspective, notre Commission nationale appelle le gouvernement et le législateur à prendre en considération les questions de protection de la vie privée et des données personnelles dans la réforme du Service de Renseignement de l'Etat, et de mettre en chantier une transposition en bonne et due forme de la décision cadre du 27 novembre 2008 sur la protection des données dans le cadre de la coopération policière et judiciaire en matière pénale (2008/977/JAI), les dispositions existantes présentant des lacunes et la fragmentation textuelle ne faisant pas bénéficier les règles applicables à ces activités de la lisibilité et visibilité nécessaires dans le domaine des libertés et droits fondamentaux.

5 Ressources, structures et fonctionnement de la Commission nationale

5.1 Rapport de gestion relatif aux comptes de l'exercice 2012

Dépenses

Le total des frais de fonctionnement de l'établissement public au cours de l'exercice 2012 s'élève à 1.636.933,57 €. Ce chiffre représente une augmentation de 4.95% par rapport à l'exercice précédent et reste en dessous des prévisions budgétaires.

A ces frais de fonctionnement s'ajoutent les dépenses extraordinaires d'un montant de 81.010,52 € pour l'organisation de la Conférence de printemps des autorités européennes de la protection des données, qui a eu lieu à Luxembourg du 2 au 4 mai 2012.

Les charges relatives au personnel permanent sont en retrait de façon significative par rapport aux prévisions budgétaires (-101.440,50 €), étant donné que trois postes sont restés inoccupés pendant une grande partie de l'année.

Toutefois ces fonctions ont été pourvues autrement et ont donné lieu à une augmentation des dépenses d'honoraires et frais d'experts et de prestataires externes de +59.191,59 €. Parmi ces dépenses figurent également les honoraires d'avocats et factures de la fiduciaire qui tient la comptabilité et établit le bilan de l'établissement public.

Les loyers et charges locatives relatifs aux locaux provisoires de la CNPD (pris en location dans l'attente de son implantation dans le 1er bâtiment administratif en construction par l'Etat à Belval) s'élevant à 103.083,34 € ont dépassé les estimations budgétaires, vu que le déménagement à Esch-Belval prévu pour septembre 2012 n'a eu lieu qu'en décembre 2012.

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 25.730,66 €. Ils sont relatifs à la participation des membres effectifs et des collaborateurs de la Commission nationale aux différentes réunions, séances de travail et conférences organisées sur le plan européen dans le domaine de la protection des données, où le Luxembourg se doit d'être représenté.

Les dépenses d'information du public et de communication

de 14.853,80 € sont restées quelque peu en dessous de nos prévisions, alors que le coût des annonces de presse publiées dans le cadre de la campagne menée à l'occasion de la journée européenne du 28 janvier 2012 est venu s'ajouter à des dépenses ponctuelles non récurrentes.

A défaut de disposer des ressources spécialisées nécessaires en interne au début de l'exercice budgétaire pour la gestion et maintenance des systèmes et réseaux informatiques, les frais relatifs d'un montant de 12.259,00 € ont dépassé nos prévisions budgétaires.

Les amortissements comptabilisés en 2012 atteignent un montant total de 12.124,65 €. Ils concernaient pour l'essentiel le mobilier et les équipements informatiques, ainsi que les investissements relatifs au développement et à la mise en service de l'application informatique spécifique dédiée à l'établissement du registre public des traitements prévu à l'article 15 de la loi ainsi qu'à l'optimisation des procédures administratives.

Recettes

Le montant des redevances perçues en application des articles 37 paragraphe (4) et 13 paragraphe (4) de la loi s'élevant à 84.100 € a dépassé nos prévisions (60.000 €). En outre des produits financiers (intérêts créditeurs) ont été enregistrés à hauteur de 3.313,66 €.

Résultat d'exploitation

Compte tenu de la dotation annuelle de 1.645.200 € dont la Commission nationale a bénéficié en 2012 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 14.669,57 € au 31 décembre 2012. Il sera reporté sur l'exercice suivant.

5 Ressources, structures et fonctionnement de la Commission nationale

5.2 Personnel et services

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

Membres suppléants
Josiane PAULY
Marc HEMMERLING
Tom WIRION

Service juridique
Georges WEILAND,
attaché de direction 1er en rang
Michel SINNER,
attaché de direction 1er en rang
Christian WELTER,
attaché de direction 1er en rang
Laurent MAGNUS,
juriste
Arnaud HABRAN,
juriste
Franziska BOEHM,
enseignante/chercheuse à
l'Université de Luxembourg

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
Carla DE BASTOS SOARES,
employée administrative

Service communication et documentation
Tom KAYSER,
attaché de direction

5.3 Organigramme de la Commission nationale

Secrétariat
Tessy PATER, secrétaire de direction
Serge FERBER, employé de l'Etat
Carla DE BASTOS SOARES, employée administrative

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

Administration générale, personnel, budget et finances

Service communication et documentation
Tom KAYSER

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

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

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

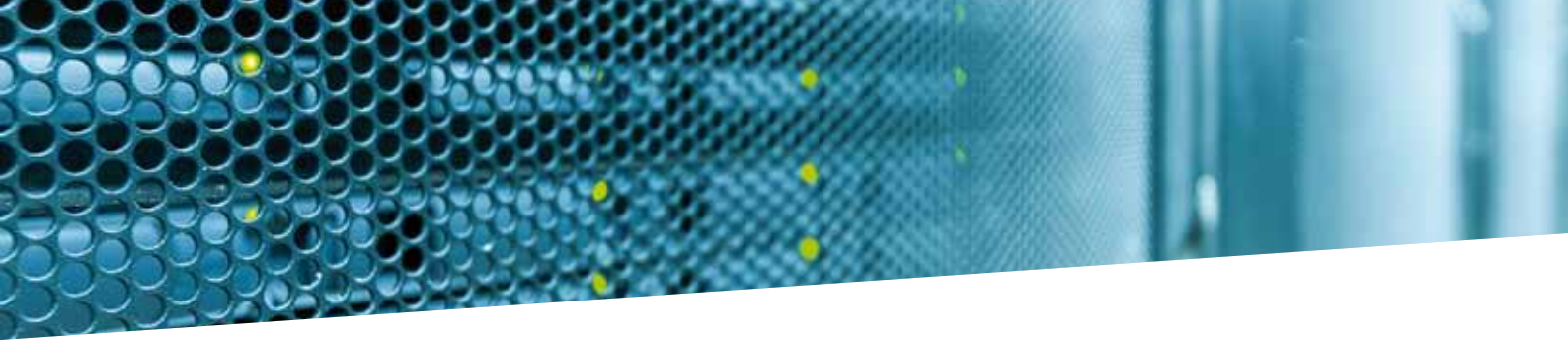
	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	
a) Notifications											TOTAL
Notifications ordinaires	2.646	850	500	250	760	385	345	295	355	437	6.823
Notifications simplifiées	750	900	720	890	537	-	-	-	-	-	3.797
Engagements de conformité	-	-	-	-	-	942	227	15	46	149	1.379
(Total a)	3.396	1.750	1.220	1.140	1.297	1.327	572	310	401	586	11.999
b) Autorisations préalables											TOTAL
Demandes d'autorisation	765	406	317	295	392	606	542	607	604	706	5.240
Engagements de conformité	718	14	17	19	151	220	70	92	49	70	1.420
(Total b)	1.483	420	334	314	543	826	612	699	653	776	6.660
(Total général a + b)	4.879	2.170	1.554	1.454	1.840	2.153	1.184	1.009	1.054	1.362	18.659
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	

Demandes de renseignements

	2004	2005	2006	2007	2008	2009	2010	2011	2012
a) Demandes de renseignements par écrit									
(Total a)	156	117	150	148	138	138	213	173	273
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
(Total général a + b)	1.936	1.667	2.080	2.018	1.724	1.545	1.618	1.807	1.697

Plaintes et investigations

	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
	15	38	40	30	34	63	133	145	115	133



Séances de délibération

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

Participations aux groupes de travail sur le plan européen

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

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

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

Séances d'information, conférences, exposés

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

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

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

7 Annexes

Avis relatif au projet de loi n°6330 relative à l'identification des personnes physiques, à la carte d'identité, aux registres communaux des personnes physiques et portant modification de 1) l'article 104 du Code civil ; 2) la loi modifiée du 22 décembre 1886 concernant les recensements de population à faire en exécution de la loi électorale ; 3) la loi modifiée du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales ; 4) la loi communale modifiée du 13 décembre 1988 ; 5) la loi électorale modifiée du 18 février 2003

Délibération n°1/2012
du 16 février 2012

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

Faisant suite à la demande lui adressée par Madame la Ministre déléguée à la Fonction publique et à la Réforme administrative en date du 11 août 2011, la Commission nationale expose ci-après ses réflexions et commentaires au sujet du projet de loi n°6330 (ci-après : le projet de loi).

Avant-propos

Le texte sous examen constitue la fusion, avec des modifications, des projets de lois n°5949[1] et n°5950[2].

La Commission nationale avait rendu son avis 48/2009 sur le projet de loi n°5949 en date du 10 mars 2009 puis son avis 11/2011 sur le projet de loi n°5950 en date du 14 février 2011.

Le projet de loi sous examen a modifié, parfois en profondeur, certaines dispositions sur lesquelles la Commission nationale s'était prononcée. Tout en regrettant que toutes ses observations n'aient pas été prises en compte par les auteurs du projet de loi sous examen, elle constate toutefois certaines améliorations apportées au texte fusionné.

La Commission nationale limitera son analyse aux points traités dans ses avis précités et qui ont fait l'objet de modifications dans le projet de loi sous examen.

[1] Projet de loi relatif aux registres communaux des personnes physiques.
[2] Projet de loi relatif à l'identification des personnes physiques, au registre national des personnes physiques et à la carte d'identité.

Quant au numéro d'identification nationale

Le projet de loi sous examen modifie le régime du numéro d'identification national par rapport au régime actuellement en vigueur ainsi que par rapport au projet de loi n°5949. La Commission nationale a insisté, dans le cadre des consultations préalables à la révision de la loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales[3] et des différents avis qu'elle a été amenés à rendre[4], sur la nécessité que l'usage de l'identifiant unique s'accompagne de solutions technologiques novatrices pour renforcer les garanties destinées à éviter des risques d'abus. Elle ne peut que regretter que le projet de loi ne fasse pas référence à de telles solutions technologiques.

Un modèle conciliant la protection des données avec l'efficacité administrative

Si la Commission nationale n'a jamais eu l'intention de remettre en cause le principe d'un numéro d'identification uniforme et non équivoque en faveur d'un système reposant sur des numéros d'identification sectoriels, elle a néanmoins toujours œuvré pour que le système envisagé soit accompagné des garanties appropriées les plus robustes qui permettent de protéger au mieux la vie privée des administrés.

Il est vrai que l'utilisation d'un système reposant sur un numéro d'identification unique pour l'ensemble ou pour une partie des démarches administratives peut présenter des avantages. Chaque citoyen qui se voit attribuer un numéro d'identification peut ainsi le mémoriser car la structure de ce numéro d'identification est préalablement connue (la date de naissance, le sexe,…). De plus, il n'a pas à se souvenir de plusieurs numéros d'identification, un numéro unique facilitant ses démarches auprès de différentes administrations.

Ces avantages présentent néanmoins des contreparties. Ainsi, toute personne est susceptible de composer le numéro d'identification d'une autre personne : en connaissant sa date de naissance, elle n'a qu'à se souvenir des derniers chiffres. Le risque majeur réside essentiellement dans les interconnexions de fichiers, c'est-à-dire sur la possibilité de regrouper des données contenues dans divers fichiers et de retracer tous les actes de la vie courante d'un administré qui deviendrait comme transparent (« Gläserner Bürger »).

Il est utile de rappeler que le numéro d'identification national a été institué pour identifier sans équivoque le citoyen dans ses relations avec les administrations et les établissements de sécurité sociale. Pour encadrer l'utilisation d'un identifiant unique et contrer les risques de dérives liées à son utilisation, la Recommandation (86)1 relative à la protection des données à caractère personnel utilisées à des fins de sécurité sociale adoptée par le Comité des Ministres du Conseil de l'Europe le 23 janvier 1986 précise que « *l'introduction ou l'utilisation d'un numéro de sécurité sociale uniforme et unique ou de tout autre moyen analogue d'identification devrait s'accompagner de garanties adéquates prévues par le droit interne* ». Dans cet ordre d'idées, l'article 8 point 7. de la Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et à la libre circulation de ces données[5] précise que « *les Etats membres déterminent les conditions dans lesquelles un numéro nationale d'identification ou tout autre identifiant de portée générale peut faire l'objet d'un traitement* ». Cette directive fait référence, sous une autre expression, aux garanties appropriées exposées par le Conseil de l'Europe dans sa recommandation précitée. Le Comité d'experts sur la protection des données précise également dans son étude remise en 1991 au Conseil de l'Europe que les conditions ou garanties accompagnant la mise en place et l'utilisation des

[3] Ci-après : la loi du 30 mars 1979.
[4] Notamment l'avis 2/2004 au sujet de l'avant-projet de règlement grand-ducal concernant l'accès au répertoire général des personnes physiques et morales par les officiers publics et autres créateurs ou exécuteurs d'actes translatifs de propriété immobilière ou de constitution d'hypothèque (ci-après : avis 2/2004).
[5] Ci-après : la directive 95/46/CE du 24 octobre 1995.

numéros d'identification peuvent avoir des aspects juridiques et techniques (l'utilisation du numéro autorisée par la loi, journalisation des saisies). Il est à rappeler que les garanties techniques qui sont devenues obsolètes ou dépassées ne protègent plus.

La loi du 31 mars 1979 avait prévu des garanties adéquates juridiques à l'identification numérique des personnes. Ainsi, ce numéro était réservé à un usage administratif interne ou aux relations avec le titulaire du numéro et des règlements grand-ducaux déterminaient les actes, documents et fichiers sur lesquels ce numéro pouvait figurer. Or, force est de constater que ces garanties sont devenues insuffisantes. En effet, les services fournis par les administrations se sont développés. Par ailleurs, et conformément à ce que d'aucuns ont pu critiquer, le numéro d'identification est souvent demandé et utilisé en dehors des démarches administratives, par des personnes non autorisées et/ou pour des finalités autres que celles pour lesquelles la loi du 31 mars 1979 les a autorisées. De plus, le numéro d'identification permet de faire le lien entre différents fichiers : dès lors qu'une personne connaît le numéro d'identification d'un administré, il est possible de regrouper des informations confidentielles le concernant, informations qui figurent dans des fichiers distincts.

Déjà dans son avis 2/2004 du 9 janvier 2004, la Commission nationale mettait en garde sur les faiblesses des garanties légales relatives à l'identification numérique des personnes et adoptées il y a plus de trente ans et qui sont dépassées dans notre société actuelle; elle insistait pour que de nouvelles garanties techniques et juridiques répondent aux évolutions de la société contemporaine.

Des pays européens qui utilisaient un numéro d'identification parlant ont modifié récemment leur législation pour l'adapter aux évolutions de la société tout en s'employant à recourir à des garanties appropriées performantes.

Ainsi, l'Autriche a opéré le changement par une loi du 27 février 2004. Le système qu'elle a adopté est, de l'avis de la Commission nationale et d'autres autorités nationales en matière de protection des données[6], le modèle qui concilie au mieux la protection des données avec l'efficacité administrative. L'Autriche a en effet fait le choix d'un système de communication électronique sécurisé qui intègre les enjeux de la protection des données. Les autorités publiques emploient différents identifiants personnels dérivés de la source-PIN de la personne physique et à usage sectoriel. Une « *plaque tournante informatique* » permet

[6] Et notamment du Préposé Fédéral suisse dans son article « Vers une société sous surveillance ? » d'août 2006.

les passerelles entre fichiers des différentes administrations ; elle trace et contrôle tous les flux d'informations. Ce système respecte les droits des personnes en matière de protection des données, tout en permettant les échanges informatiques d'informations entre administrations utilisant des numéros ss-PIN distincts pour une seule et même personne.

Ce système a un coût significatif mais il présente des idées tout à fait exploitables. D'ailleurs, la Suisse a souhaité importer ce modèle mais le projet n'a pas été adopté à une voix près. La Suisse a alors fait le choix de l'adoption d'une nouvelle structure de treize chiffres totalement aléatoire qui ne fournit aucune information parlante sur son titulaire. La modification est intervenue par une loi fédérale du 23 juin 2006 mise en vigueur par la Conseil fédéral le 1er décembre 2006.

Le projet de loi sous examen ne contient pas toutes les garanties appropriées recommandées par la Commission nationale.

<u>L'identification des personnes selon l'article 1er du projet de loi sous examen</u>

Tout d'abord, le projet de loi précise comment le numéro d'identification personnel des personnes physiques sera composé, à savoir à partir de la date de naissance, d'une plage séquentielle unique par date de naissance et de deux numéros de contrôle. La Commission nationale est satisfaite que, conformément à sa recommandation formulée dans son avis précité du 10 mars 2009, le projet de loi détaille la composition du numéro d'identification national. Elle comprend également que la structure ne soit pas arrêtée dans le projet de loi car un règlement grand-ducal permet plus facilement de l'adapter dans le futur.

Elle regrette néanmoins que le projet de loi sous examen n'envisage plus la possibilité d'adopter un numéro d'identification unique non parlant, comme le prévoyait le projet de loi n°5950[7]. Dans les commentaires des articles dudit projet de loi, il avait été reconnu qu'un numéro entièrement aléatoire était plus respectueux en matière de protection des données à caractère personnel qu'un numéro qui dévoilent des informations sur son titulaire. La Commission nationale n'est pas convaincue que la plus-value relative au fait que les individus peuvent facilement se souvenir de leur numéro d'identification national soit suffisamment importante par rapport aux dangers qu'elle peut présenter. La visibilité du numéro d'identification est, en fait, plus un risque car toute personne, autre que son titulaire, pourrait retenir un numéro d'identification dès lors qu'il connaît la date de naissance d'une personne car il ne lui reste qu'à se souvenir des derniers chiffres du numéro d'identification. Elle n'ignore pas pour autant que la migration de la structure parlante vers une structure aléatoire du numéro d'identification aurait demandé des moyens financiers et techniques; toutefois, elle fait valoir que la Suisse a opéré cette mutation pendant une période de transition de moins de deux ans[8].

Ensuite, le projet de loi prévoit l'élargissement des personnes et organismes pouvant utiliser le numéro d'identification national par rapport à ce qui était prévu dans la loi du 31 mars 1979. L'énumération de ces bénéficiaires semble justifiée dans le projet de loi à condition que l'utilisation du numéro d'identification reste cantonnée aux finalités pour lesquelles le projet de loi les a autorisées.

Toutefois, elle estime que les actes, documents et fichiers établis dans le cadre de l'initiative citoyenne ne devraient pas contenir le numéro d'identification, contrairement à ce qui est prévu à l'article 2 paragraphe (5) du texte sous examen. Dans son avis 378/2011 du 11 novembre 211 concernant le projet de

---

[7] *« … est prévu dans un premier temps de rajouter deux positions aux onze positions actuelles du numéro de matricule. A terme, l'objectif sera d'introduire un numéro d'identification à caractère aléatoire, c'est-à-dire qui ne comporte aucune indication quant à la date de naissance ou au sexe du titulaire du numéro, ceci dans un souci de protection des données personnelles »* (document parlementaire n°5950/0, page 11, avant-dernier paragraphe).

[8] Le nouveau numéro d'identification national est utilisé en Suisse depuis le 1er juillet 2008, soit après une période de transition d'une année et demie.

Annexes

loi n°6325 relatif à la mise en application du règlement (UE) n°211/2011 du Parlement et du Conseil du 16 février 2011 relatif à l'initiative citoyenne, elle recommandait en effet de ne pas recourir au numéro d'identification dans le cadre de l'initiative citoyenne. En effet, les formulaires contenant les numéros de matricules vont circuler entre les signataires et avec les organisateurs de l'initiative citoyenne et ces numéros de matricules sont susceptibles de circuler de manière totalement incontrôlée et il n'est pas exclu que les personnes qui prendront connaissance de ces numéros ne les copient pas dans un fichier.

La Commission nationaleregrette que les auteurs du projet de loi n'aient pas saisi l'occasion qui leur était donné d'apporter les garanties technologiques les plus novatrices et protectrices en termes de protection de données au système de l'identifiant unique.
Une telle occasion ne se présentera plus d'aussitôt, plus de trente ans s'étant écoulés entre la loi qui régit actuellement l'identification des personnes et la législation appelée à s'y substituer. Malgré les changements technologiques apparus durant cette période de plus de trente ans, les auteurs du projet de loi n'ont pas voulu profiter des avancées technologiques en la matière.

La Commission nationale conclut que l'identification des personnes physiques telle qu'elle est envisagée dans le projet de loi sous examen, ne présente pas les garanties appropriées exigées par l'article 8 paragraphe 7 de la directive 95/46/CE. Elle regrette que le projet de loi sous examen ne réponde pas aux ambitions de vouloir modifier et d'améliorer le système complètement dépassé mis en place en 1979, ni aux critiques et préoccupations relatives à l'utilisation du numéro d'identification et à l'application de la loi du 30 mars 1979. Dans son précédent avis 48/2009, elle rappelait que des questions parlementaires portaient sur des craintes d'un usage trop large du numéro d'identification. L'utilisation du numéro d'identification est élargie sans que des garanties appropriées soient prévues en contrepartie pour parer aux risques d'intrusion dans la vie des personnes, respectivement aux risques de dérives sur l'utilisation du numéro d'identification.

Quant à la Commission du registre national des personnes physiques

La Commission nationale constate que l'article 4 du projet de loi sous examen énumère les finalités pour lesquelles le registre national des personnes physiques est organisé et elle estime que ces attributions sont légitimes.

Elle remarque avec satisfaction que conformément à ce qu'elle avait recommandé dans son avis précité du 10 mars 2009 relatif au projet de loi n°5950, le projet de loi sous examen décrit la composition de cette commission au sein de laquelle la Commission nationale sera représentée.

Elle suggère encore que l'article 7 du projet de loi n°5950 maintienne l'exigence que la Commission du registre national doive donner un avis conforme aux demandes d'accès au registre national. Elle estime en effet que ce pouvoir lui attribuerait un rôle plus formel.

La carte d'identité

Le projet de loi apporte un certain nombre de modifications aux dispositions ayant trait à la carte d'identité. Ces modifications n'apportent pas d'observations particulières, sauf à relever que le texte précise de manière satisfaisante que les données biométriques ne figureront pas dans un fichier centralisé.

Il est intéressant de relever qu'en France, dans le cadre de l'examen actuel de la proposition de loi relative à la protection de l'identité telle que modifiée par l'Assemblée nationale lors de son séance du 13 décembre 2011, d'aucuns ont dénoncé la création d'un fichier centralisé des nouvelles cartes d'identité contenant les données biométriques des personnes[9]. Lors de sa séance plénière du 25 octobre 2011, la Commission nationale avait également considéré que « *les finalités invoquées* [la proposition de loi relative à la protection de l'identité] *ne justifiaient pas la conservation, au plan national, de données biométriques telles que les empreintes digitales et que les traitements ainsi mis en œuvre seraient de nature à porter une atteinte excessive à la liberté individuelle* »[10].

Quant aux registres communaux des personnes physiques

L'article 19 du projet de loi sous examen dispose que le bourgmestre est chargé de la tenue du registre communal et qu'il peut déléguer, sous sa surveillance et sa responsabilité la tenue dudit registre à un ou plusieurs fonctionnaires communaux. Cette précision s'inscrit parfaitement dans l'article 21 de la loi du 2 août 2002 qui précise que « *toute personne qui agit sous l'autorité du responsable du traitement ou sous celle du sous-traitant, ainsi que le sous-traitant lui-même, et qui accède à des données ne peut les traiter que sur instruction du responsable du traitement, sauf en vertu d'obligations légales* ».

L'ajout de cette précision dans le projet de loi permet de mettre en avant le rôle et l'importance du bourgmestre dans la tenue du registre communal, ce qui donne une meilleure visibilité de ses prérogatives vis-à-vis des administrés.

Quant aux demandes d'informations de tiers sur les données figurant dans les registres communaux

La Commission nationale avait fait part dans son précédent avis portant sur le projet de loi n°5949, du nombre important de demandes émanant de communes qui souhaitaient savoir les suites qu'elles devaient donner à des demandes de communications d'adresses portant sur une personne en particulier formulées par des tiers.

La Commission nationale a toujours revendiqué la nécessité d'un texte légal qui encadre la communication de données issues des registres communaux à des tiers. Elle a régulièrement dénoncé le vide juridique de la situation actuelle et elle a demandé à ce que le législateur règle cette situation en proposant un cadre légal qui présenterait les critères à réunir pour délivrer ces informations.

A défaut de base légale à ce sujet, elle faisait valoir en effet que la remise de l'adresse

[9] Par exemple, la Ligue des Droits de l'Homme, le Syndicat de la Magistrature et le Syndicat des Avocats de France ont diffusé un communiqué le 16 décembre 2011.
[10] Note d'observations de la Commission nationale de l'informatique et des libertés concernant la proposition de loi relative à la protection de l'identité, examinée en séance plénière le 25 octobre 2011, page 11.

d'une personne à des tiers ne rentrait pas forcément dans la finalité pour laquelle les fichiers communaux ont été créés, de sorte qu'il ne devrait pas être permis de leur transmettre cette information. Faisant sienne la position de la Commission consultative instituée par la loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques dans son avis du 9 novembre 1984, elle considérait, de manière pragmatique, que des demandes ponctuelles de communication d'adresses étaient permises à condition de justifier d'un intérêt légitime. Les auxiliaires de justice, agissant dans le cadre de l'exercice de leurs fonctions et de leurs missions respectives, pouvaient se prévaloir de cet intérêt légitime ; pour tout autre demande, la commune devait faire une appréciation au cas par cas pour apprécier l'existence réelle de l'intérêt légitime du demandeur.

Pour la première fois, le projet de loi n°5949 avait prévu une procédure d'autorisation préalable près de la Justice de Paix : tout en saluant la mise en place d'une telle procédure judiciaire, la Commission avait estimé que la procédure pouvait paraître excessive et avait demandé que certaines professions - dont les auxiliaires de justice - soient exemptées de cette procédure du fait de leurs missions professionnelles.

Le projet de loi sous examen ne mentionne plus du tout la mise en place d'une quelconque procédure pour la remise d'information ponctuelle. Il ne règle plus le vide juridique existant pour les demandes ponctuelles d'informations introduites par des tiers. En d'autres mots, le projet de loi sous examen ne propose pas de cadre légal pouvant répondre aux attentes des administrations saisies de demandes ponctuelles de renseignements d'adresse. Par conséquent, et en faisant application des règles générales en matière de protection des données, la Commission nationale considère que la communication à des tiers de données à caractère personnelles issues des fichiers communaux serait interdite dès lors que ces fichiers communaux sont créées pour répondre à des finalités précises mais différentes aux raisons pour lesquelles les informations sont demandées.

A titre d'illustration, la Commission nationale est actuellement saisie de demandes d'administrations ou d'organismes étrangers portant sur des demandes de recherche d'adresses aux fins de recouvrements de créances, des recherches d'héritiers ou des accès aux origines personnelles

après un accouchement sous X. Si pour les demandes de recouvrement de créance, la Commission nationale peut renvoyer aux dispositions du Nouveau Code de procédure civile relatives aux saisies, elle constate que les informations ne pouvaient pas être délivrées à des tiers parce que les finalités des différentes demandes étaient incompatibles avec les finalités pour lesquelles les fichiers administratifs ont été créés. Pourtant certaines demandes de recherche d'adresses sont introduites pour apporter un bénéfice à la personne recherchée (la remise d'un héritage par exemple).

La Commission estime par conséquent que le projet de loi devrait être complété pour remédier à l'insécurité juridique en la matière. Il serait en effet judicieux que le projet de loi sous examen précise les conditions et critères selon lesquels les administrations sont en droit de délivrer des informations ponctuelles à des tiers. La détermination de critères légaux conduirait également à éviter que les réponses soient différentes d'une administration à une autre et permettrait aux citoyens de savoir dans quelles conditions des tiers peuvent obtenir des renseignements les concernant. D'autres pays ont adopté des dispositions légales pour réglementer les hypothèses dans lesquelles un tiers peut obtenir communication de l'adresse d'un citoyen à partir de fichiers communaux ou d'autres fichiers nationaux.

En ce qui concerne la possibilité de communiquer des listes contenant des informations sur les administrés, le projet de loi sous examen a modifié de manière satisfaisante la possibilité de communiquer les listes des personnes inscrites sur le registre nationale telle qu'elle était envisagée dans le projet de loi n°5949. La possibilité de remettre uniquement des données statistiques, ne contenant pas de donnée à caractère personnel s'inscrit parfaitement dans un souci de protection de la vie privée des personnes physiques.

Pour le surplus, la Commission nationale renvoie à ses observations formulées dans ses avis 48/2009 et 11/2011.

Ainsi décidé à Luxembourg en date du 16 janvier 2012.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

Avis complémentaire de la Commission nationale pour la protection des données relatif au projet de loi n°6021 portant modification : 1. de la loi modifiée du 8 décembre 2000 sur le surendettement, 2. de l'article 2016 du Code civil, 3. des articles 1er et 4 du Nouveau Code de procédure civile et 4. de l'article 536 du Code de commerce sur le surendettement et modifiant certaines dispositions légales

Délibération n°143/2012 du 18 mai 2012

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 5 avril 2012, Monsieur le Ministre de la Justice a invité la Commission nationale à se prononcer au sujet de la

Annexes

version amendée du projet de loi n°6021 portant modification : 1. de la loi modifiée du 8 décembre 2000 sur le surendettement, 2. de l'article 2016 du Code civil, 3. des articles 1er et 4 du Nouveau Code de procédure civile et 4. de l'article 536 du Code de commerce sur le surendettement et modifiant certaines dispositions légales.

La Commission s'est déjà prononcée dans un avis du 17 juin 2011 sur le projet de loi précité. Depuis lors, des amendements gouvernementaux ont été déposés et le projet de loi est modifié de manière substantielle.

Mis à part l'amendement relatif au répertoire des personnes surendettées, le projet de loi sous examen ne contient pas d'autres dispositions pouvant concerner la matière de la protection des données, de sorte que la Commission nationale se limitera à examiner, dans le présent avis, les modifications qu'apporte cette disposition au projet de loi amendé dans sa version du 4 novembre 2011.

Elle voudrait soulever d'emblée qu'elle observe avec satisfaction d'ores et déjà que certaines remarques exposées par la Commission nationale ont été intégrées dans les amendements soumis à son appréciation.

Si l'économie générale du régime relatif au répertoire des personnes surendettées n'a pas été fondamentalement modifiée par rapport au texte sur lequel la Commission nationale s'était prononcée dans son précédent avis, des précisions et éclaircissements ont été apportés.

A ce titre, il est à relever que l'article 23 paragraphe (2) indique que l'inscription des informations sera réalisé dans un fichier informatique. Dans la version antérieure, le projet de loi évoquait un fichier informatique ou « *mécanique* », expression difficile à appréhender. La nouvelle rédaction de cet article élimine ainsi les interrogations sur le sens d'un fichier « *mécanique* ».

La Commission nationale suit la position du Conseil d'Etat qui estime dans son avis complémentaire du 30 mars 2012 relatif au projet de loi amendé qu'il y a lieu de prévoir une disposition pénale sanctionnant la diffusion des informations reçues par la consultation du répertoire à des fins étrangères à la finalité de la loi, à savoir l'information des créanciers, cautions et coobligés du débiteur surendetté sur l'état d'avancement de la procédure de règlement collectif des dettes. Cette disposition permettrait de sanctionner les abus relatifs à l'utilisation du répertoire dont la consultation est désormais

permise à toute personne qui justifie de son identité. Il est en effet à craindre que des personnes mal intentionnées consultent le répertoire « *par simple curiosité malsaine* », comme l'avait déjà relevé également la Commission nationale dans son avis précédent. Dans le même ordre d'idées pour ce qui est de la consultation du répertoire par de simples particuliers, elle partage aussi la proposition du Conseil d'Etat de « *limiter l'information de toute personne justifiant de son identité à la seule confirmation ou infirmation de l'inscription au répertoire* ».

L'article 23 indique encore que le répertoire centralisera « *les avis et informations établis en matière de procédure de règlement collectif des dettes* » et qu'il assurera la « *publicité des extraits de décision et des avis* ».

Dans son précédant avis, la Commission nationale avait énuméré une liste des avis et informations que ce répertoire pouvait contenir, en se référant à différentes dispositions éparses du projet de loi et elle avait indiqué qu'il aurait été préférable que le projet de loi indique au moins les grandes catégories de données. Or, elle constate que le projet de loi amendé n'énumère pas non plus les différents avis, informations et décisions qui seront intégrés dans le répertoire.

Les commentaires des articles y relatifs n'apportent pas non plus de précision sur ce point. Il est vrai que, comme dans le projet de loi initial, des dispositions éparses précisent la publication dans le répertoire : ainsi, par exemple, l'article 16 paragraphe (4) prévoit que l'avis du jugement d'ouverture de la procédure de redressement personnel est publié au répertoire mais l'article 19 ne précise pas si l'avis du jugement de clôture de cette procédure de rétablissement personnel sera publié. Il n'est dès lors pas possible d'apprécier l'exhaustivité du contenu du répertoire. Il aurait été préférable que le texte sous examen énumère dans cet article 23 les différentes décisions, avis et informations qui doivent obligatoirement être publiés dans le répertoire.

Le projet de loi amendé allonge la durée de conservation des données dans le répertoire à dix années au maximum.

En effet, dans la première version du projet de loi, la durée de conservation dans le répertoire était de sept années pour les plans de règlement conventionnel, les plans de redressement judiciaire, les plans établis à des fins probatoires et les recommandations de la Commission. La durée de conservation de l'information relative aux débiteurs surendettés ayant bénéficié de la procédure de rétablissement personnel était de cinq ans à partir de la date du jugement de clôture de la procédure.

Cet allongement des délais de conservation n'est pas motivé. Une explication apparente ne découle pas non plus des durées respectives des procédures de règlement conventionnel et de redressement judiciaire, alors que celle-ci restent inchangées. La Commission nationale relève que la conservation de données pendant sept années pour les plans et recommandations décrits à l'article 23 paragraphe (4) était justifiée dans la version initiale car elle correspondait à la durée maximale de la procédure de redressement. En ce qui concerne la procédure de rétablissement personnel, s'il est logique de prévoir un allongement de la durée de l'inscription parce que le plan judiciaire peut être établi pour une durée maximale de sept années, il n'est toutefois pas justifié pourquoi cette inscription peut être maintenue à l'issue de ce plan.

A défaut de précisions qui puissent justifier un allongement à dix années de la durée de conservation des données dans le répertoire et eu égard à l'article 4 paragraphe (1) lettre (d) de la loi modifiée du 2 août 2002, la Commission nationale recommande de maintenir la durée d'inscription à sept ans

Annexes

pour les plans de règlement conventionnel, les plans de redressement conventionnel, les plans à des fins probatoires et les recommandations de la Commission de médiation ayant fait l'objet d'une acceptation et ayant trait au moratoire. Elle propose également que l'inscription au répertoire des débiteurs surendettés ayant bénéficié de la procédure de rétablissement personnel soit possible pendant sept ans à compter de la date du jugement de clôture de la procédure ayant acquis autorité de chose jugée.

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

Ainsi décidé à Luxembourg en date du 18 mai 2012.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

Avis complémentaire de la Commission nationale pour la protection des données relatif au projet de loi n°6284 portant sur l'exploitation d'une base de données à caractère personnel relative aux élèves

Délibération n°156/2012
du 15 juin 2012

En considération de ses avis précédents du 26 juillet 2010, du 15 avril 2011 et de sa note du 22 mai 2012 relatifs au projet de loi n°6284 portant sur l'exploitation d'une base de données à caractère personnel relative aux élèves, et suite à l'adoption par la Commission de l'Education nationale, de la Formation professionnelle et des Sports de la Chambre des Députés d'amendements lors de sa réunion du 7 juin 2012, la Commission nationale tient à formuler encore quelques observations au sujet de certaines dispositions du projet de loi amendé.

D'emblée, elle s'empresse de saluer les nombreuses améliorations apportées au texte du projet de loi en termes de protection des données et de la vie privée.

Ainsi, pour n'en citer que quelques unes, le texte amendé prévoit désormais la désignation d'un chargé de la protection des données (tel que visé à l'article

40 de la loi modifiée du 2 août 2002) au sein du MENFP ; les dispositions relatives à la sécurité et la confidentialité des données ainsi que celles relatives à l'accès aux données ont été précisées et renforcées ; les données relatives aux revenus des représentants légaux des élèves ne seront pas collectées et traitées ; en outre, pour des considérations de transparence et de loyauté envers les personnes concernées, les représentants légaux et l'élève majeur recevront une information individuelle, écrite et exhaustive sur le traitement des données les concernant etc. .

La photographie de l'élève stockée dans la base de données centralisée

Pour les raisons plus amplement détaillées ci-après, la CNPD se doit toutefois d'émettre ses plus expresses réserves sur l'intention maintenue de faire figurer une photographie de chaque élève dans un fichier centralisé (article 3 paragraphe (2) du projet de loi amendé).

Dans son avis du 6 décembre 2011, le Conseil d'Etat a également exprimé ses doutes quant à la nécessité de stocker dans une base de données les photographies des élèves. A ce titre, les auteurs du projet de loi ont fourni des précisions au Conseil d'Etat en date du 21 mai 2012 (doc. parl. n°6284-6). Il résulte des explications fournies que la finalité du traitement de la photographie est la personnalisation de la carte d'élève « myCard » qui est une pièce d'identification officielle prouvant pour les élèves leur statut d'élève inscrit à un lycée. La carte sert comme moyen d'identification, d'authentification et de paiement électronique et peut encore être utilisée pour accéder à toute une série de services offerts dans le lycée. Il n'est cependant pas précisé pourquoi il serait nécessaire de stocker les photographies dans le fichier au-delà du temps nécessaire pour confectionner les cartes « myCard » ?

La Commission nationale voudrait faire remarquer qu'à l'heure actuelle, il n'existe aucun autre fichier informatique, exploité par une administration ou un service de l'Etat, qui contiendrait de façon permanente des photographies des administrés ou de seulement une partie ou catégorie de citoyens. Le projet de loi n°6330 relative à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité (électronique) et aux registres communaux des personnes physiques en fait abstraction à dessein parmi les données figurant au registre national des personnes physiques ou aux registres communaux.

Elle rappelle qu'une photographie numérique présente la particularité qu'elle est une donnée biométrique. Une donnée biométriques n'est pas une donnée à caractère personnel « comme une autre », mais particulièrement sensible, alors qu'elle permet à tout moment l'identification de la personne concernée sur la base de caractéristiques biologiques qui lui sont propres, permanentes et dont elle ne peut se défaire. Elle appartient donc à la personne qui l'a générée et tout détournement ou mauvais usage de cette donnée fait alors peser un risque majeur sur l'identité de celle-ci. Cette spécificité des données biométriques a d'ailleurs conduit le législateur à leur conférer une protection et un encadrement particulier dans la loi modifiée du 2 août 2002.

La CNPD s'est exprimée à plusieurs reprises sur des projets mis en œuvre dans le cadre de la délivrance de titre d'identité ou de voyage et en particulier dans le cadre de l'introduction du passeport biométrique, du projet de loi n°6330 relative à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité et aux registres communaux des personnes physiques ainsi que de la délivrance d'un titre de séjour pour les ressortissants de pays tiers[11].

[11] Règlement grand-ducal modifiée du 26 septembre 2008 portant création des traitements de données à caractère personnel nécessaires à l'exécution de la loi du 29 août 2008 sur la libre circulation des personnes et l'immigration et déterminant les données à caractère personnel auxquelles le ministre ayant l'immigration dans ses attribution peut accéder aux fins d'effectuer les contrôle prévues par la loi.

7 Annexes

Dans ce contexte, elle a toujours estimé que l'introduction dans un titre d'identité et de voyage (ou tout autre carte électronique destinée à identifier ou authentifier une personne afin d'accéder à un service) d'un composant électronique contenant des données biométrique telles la photographie ou l'empreinte digitale était légitime et proportionnée dans la mesure où les données biométriques sont conservées dans le support individuel exclusivement détenu par la personne concernée.

Par contre, à l'instar de ses homologues européens et du groupe « Article 29 », elle s'est toujours prononcée contre l'insertion d'une donnée biométrique dans une base de données centralisée (et en particulier au plan national) compte tenu des usages possibles de ces traitements et des risques d'atteintes graves à la vie privée et aux libertés individuelles. Citons, à titre d'exemple, la CNIL française qui elle aussi a toujours considéré que « *la création d'une base centralisée de données biométriques de grande ampleur comporte des risques importants et implique des sécurités techniques complexes et supplémentaires. En effet, un fichier est d'autant plus vulnérable, « convoité » et susceptible d'utilisations multiples qu'il est de grande dimension, qu'il est relié à des milliers de points d'accès et de consultation, et qu'il contient des informations très sensibles comme des données biométriques* »[12].

Au Luxembourg, le Gouvernement tout comme la Chambre des Députés dans leur rôle de législateur ont aussi toujours adopté cette position. En effet, lors de l'introduction du passeport biométrique (ayant fait l'objet d'une autorisation de la part de la CNPD), le gouvernement a décidé de ne pas stocker, ni les photographies, ni les empreintes digitales dans le fichier central exploité par le Bureau des passeports, mais de ne les conserver que pendant le temps nécessaire à la confection des passeports. Le même principe se retrouve dans le règlement grand-ducal modifiée du 26 septembre 2008 précité qui prévoit en son article 1er paragraphe (2) que « *Les données biométriques destinées à émettre un titre de séjour recueillies conformément au Règlement CE n°380/2008 du Conseil du 18 avril 2008 modifiant le Règlement CE n°1030/2002 établissant un modèle uniforme de titre de séjour pour les ressortissants de pays tiers, sont conservées dans un fichier temporaire. Une fois que le titre de séjour a été délivré au bénéficiaire, ou au plus tard six mois après la production du titre, le ministre efface ces données* ». Enfin, dans sa version actuelle, le projet de loi n°6330 relative

[12] Note d'observations de la Commission nationale informatique et libertés concernant la proposition de la loi relative à la protection de l'identité du 25 octobre 2011.

à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité et aux registres communaux des personnes physiques prévoit lui aussi en son article 16 paragraphe (3) que « *Les données biométriques ne sont conservées que pendant une durée de deux mois après la délivrance d'une carte d'identité et sont, à l'expiration de ce délai, automatiquement et irréversiblement supprimées* ».

En considération des développements qui précèdent, le projet de loi sous examen constituerait un précédent, alors qu'il prévoit l'enregistrement permanent de la photographie de quelques 95.000 élèves dans un fichier centralisé à l'échelle nationale. Notons par ailleurs que ce fichier contient en plus des données à caractère personnelle relatives à plus ou moins 180.000 parents d'élèves.

Si la finalité précise n'est pas expliquée, il semblerait que le ministère souhaite enregistrer les photos dans la base de données pour des pures raisons de simplification administrative dans le sens que cela faciliterait l'établissement ou le renouvellement (en cas de perte ou de vol) des cartes « MyCard », les élèves n'ayant plus besoin de fournir à nouveau une photo pour la production de la carte.

La Commission nationale estime en tout état de cause qu'en l'espèce les considérations administratives doivent céder devant les intérêts prévalant des élèves à voir protégé leurs données personnelles et leur vie privée.

Elle réitère dès lors sa position que l'enregistrement de la photographie dans la base de données centralisée des élèves n'est ni nécessaire, ni proportionné par rapport aux finalités poursuivies.

La sanction pénale prévue à l'article 4(7) (Amendement 3)

Comme déjà souligné plus haut, la CNPD salue les amendements proposés à l'endroit de l'article 4 paragraphe (7) du projet de loi dont le nouveau libellé assure désormais aux représentants légaux de l'élève ainsi qu'à l'élève majeur une information individuelle par écrit, claire et exhaustive.

Elle s'étonne toutefois que cette disposition prévoit maintenant au point 5. une amende pénale de vingt-cinq à deux cent cinquante euros en cas de refus de fournir les données mentionnées à l'article 3 (2). La Commission nationale est opposée à l'idée d'assortir la disposition en question de sanctions pénales et s'interroge sur la compatibilité de cette disposition avec le droit d'opposition que l'article 30 de la loi modifiée du 2 août 2002 confère à tout citoyen. Une telle disposition apparaît particulièrement mal à propos dans le texte de l'article ayant pour objet de consolider la confiance du public.

Elle se pose, par ailleurs, la question s'il n'est pas disproportionné de prévoir une amende pénale en cas de refus de fournir des données comme par exemple l'adresse électronique ou la photographie (au cas où celle-ci serait maintenue dans le projet de loi).

La catégorie de donnée « premier emploi » mentionné à l'article 4(4) (Amendement 3)

L'article 4 paragraphe (4) prévoit entre autres de collecter directement auprès de l'élève ou de ses représentants légaux les données relatives au « premier emploi ». Cette catégorie de données ne figure nulle part à l'article 3 qui énumère les différentes données traitées. La Commission nationale suppose dès lors que les termes « premier emploi » se réfèrent ou sont à mettre en relation avec la catégorie de donnée « *occupation(s) professionnelle(s)* » dont il est question à l'article 3 paragraphe (3) lettre d) point 5. Si tel était le cas, elle propose d'utiliser la même terminologie à l'endroit

7 Annexes

des deux dispositions concernées, afin d'éviter toute confusion ou malentendu.

Ainsi décidé à Luxembourg en date du 15 juin 2012.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

Avis concernant la mise en place d'un système de pétition électronique à la Chambre des Députés

Délibération n°200/2012
du 13 juillet 2012

Par courrier du 14 mars 2012, Monsieur le Président de la Chambre des Députés a invité la Commission nationale à se prononcer au sujet d'une note établie par l'Administration parlementaire portant sur la mise en place d'un système de pétition électronique à la Chambre des Députés.

Dans le cadre de la modernisation du droit de pétition, la Chambre des Députés envisage d'instaurer une nouvelle catégorie de pétition appelée « *pétition publique* ». Cette forme novatrice de pétition tient compte des grandes évolutions qui se sont produites dans le domaine de l'informatique et qui ont, notamment grâce à Internet, fondamentalement changé la manière, les techniques et les moyens des individus à communiquer entre eux. Contrairement à la pétition ordinaire, toutes les démarches relatives à la pétition publique se feront exclusivement de manière électronique. Après s'être inscrit au biais du formulaire sur le site Internet de la Chambre des Députés et une vérification de sa recevabilité, la pétition publique

sera publiée pour la collecte des signatures sur ledit site Internet pendant une période de six semaines. La signature d'une pétition publique sera réservée, sauf exception spécifique, qu'aux résidents du Grand-Duché de Luxembourg âgés d'au moins 15 ans. Lorsqu'une pétition publique aura recueilli 4.500 signatures, un débat public devra obligatoirement être organisé à la Chambre des Députés et la Commission des Pétitions décidera sur le suivi à accorder à cette pétition.

Dans sa version initiale du projet, la Chambre des Députés avait envisagé de demander l'indication du numéro d'identité[13] (matricule national), afin de vérifier l'identité des signataires, les conditions d'âge et de résidence. Dans sa missive du 11 juin 2012, la Chambre des Députés a communiqué à la Commission nationale pour la protection des données son intention de renoncer à collecter le matricule dans le contexte de la pétition publique. Depuis sa création, la Commission nationale a toujours suivi une politique limitant l'utilisation du numéro d'identité, notamment au vu des nombreux risques par rapport aux libertés et droits des citoyens. Dès lors, la Commission nationale accueille de manière très favorable la décision de l'administration parlementaire d'un contrôle sans recours au matricule dans le cadre du présent projet.

Dans la version actuelle du projet, pour lancer une pétition publique, son initiateur devra fournir, sur le formulaire à remplir en ligne, les catégories de données suivantes :

- le nom et prénom,
- l'adresse (rue, numéro, code postal et localité),
- l'adresse e-mail,
- la date et le lieu de naissance,
- l'intitulé de la pétition,
- le texte de la pétition,
- des explications concernant l'objet de la pétition.

Les personnes souhaitant soutenir la pétition en la signant devront fournir les indications suivantes :

- le nom et prénom,
- l'adresse (rue, numéro, code postal et localité),
- l'adresse e-mail,
- la date et le lieu de naissance.

Il est prévu que le système de pétition publique ne sera mis en œuvre qu'après la mise en place du nouveau registre national des personnes physiques[14]. Etant donné que la Chambre des Députés a abandonné l'intention de collecter le matricule, il ne sera plus nécessaire de créer une base légale expresse à cet effet. Cependant, pour le contrôle de l'exactitude des données fournies par les signataires, un accès au registre national des personnes physiques par l'administration parlementaire sera néanmoins nécessaire. Celui-ci pourra être demandé conformément aux dispositions de l'article 7 deuxième paragraphe du projet de loi n°6330, qui prévoit que *« le ministre accorde l'accès au registre national en conformité avec les dispositions légales et réglementaires relatives au registre national et celles relatives à la législation sur la protection des données, après avoir demandé l'avis de la commission prévue à l'article 11*[15]*»*.

La Commission nationale relève qu'il peut arriver que le thème d'une pétition tombe dans le champ d'application de l'article 6 de la loi modifiée du 2 août 2002, par exemple lorsqu'une pétition porte sur une question ou problématique philosophique ou politique. Suivant le principe de l'article 6 paragraphe (1) , *« les traitements qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les traitements de données relatives à la santé et à la vie sexuelle, y compris le traitement des données génétiques sont interdits »*. Ce principe d'interdiction connaît cependant neuf exceptions prévues aux lettres (a) à (i) du paragraphe (2) de l'article 6. Parmi ces exceptions figure le consentement exprès donné par la personne concernée au traitement. Au

[13] Tel que défini par la loi modifiée du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales. Le numéro d'identité est plus communément connu sous les termes de « matricule » ou d'« identifiant unique ».

[14] Projet de loi n°6330 relative à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité, aux registres communaux des personnes physiques …

[15] La « commission du registre national », projet de loi n°6330, Section 4, art 11.

regard de la procédure décrite dans la note de la Chambre des Députés, la Commission nationale estime que la signature du pétitionnaire remplit les conditions du consentement exprès au traitement des données.

En ce qui concerne la signature d'une pétition publique, la Commission nationale recommande à la Chambre des Députés de prévoir si ce n'est exclusivement, du moins de manière facultative, la possibilité pour les personnes disposant d'un certificat Luxtrust de pouvoir signer la pétition publique au moyen de leur signature électronique, notamment afin d'éviter au maximum les possibilités d'abus par l'usurpation d'identité. En effet, il n'est pas à exclure qu'une personne usurpe l'identité d'une autre personne pour lui causer préjudice, voire qu'elle usurpe plusieurs identités pour atteindre par exemple un certain seuil de signatures de la pétition.

Le projet sous analyse prévoit également la publication sur Internet du nom et du prénom ainsi que de la localité de résidence (code postal inclus) de chaque signataire d'une pétition publique. La CNPD considère que la publication de ces données à caractère personnel est susceptible de poser problème à plusieurs égards. Cette problématique est d'autant plus évidente si l'on compare la procédure de la pétition ordinaire avec celle de la pétition publique.

La collecte des données dans le cadre d'une pétition ordinaire se fait exclusivement au moyen de signatures manuscrites sur papier. Bien que les listes de pétitionnaires aient un certain caractère public, il n'y a cependant pas, en principe, de publicité ou de diffusion des données personnelles des signataires à grande échelle. En effet, l'accès à l'intégralité des données des signataires de la pétition reste limité principalement aux initiateurs ainsi qu'aux membres de la Commission des Pétitions qui la reçoivent.

Contrairement à la pétition ordinaire, la pétition publique prévoit une publication obligatoire des données d'identification, du code postal et de la localité des pétitionnaires sur Internet. La diffusion des données à caractère personnel par le site internet de la Chambre des Députés aura encore un effet multiplicateur en raison de l'indexation des données faite par les moteurs de recherche sur internet (par exemple Google, Bing, Yahoo, etc.).

Le signataire d'une pétition publique court ainsi le risque d'être catégorisé ou profilé philosophiquement ou politiquement par exemple. Il

suffira de taper le nom d'une personne dans un moteur de recherche pour la voir associée, le cas échéant, à une pétition. Il est évident que cela, surtout dans le cadre d'un sujet de pétition plus « sensible », pose un risque non négligeable pour la vie privée des signataires d'une pétition, en considérant que ces informations pourront être utilisées dans un tout autre contexte. Ce risque peut par ailleurs amener certaines personnes à ne pas signer une pétition publique, par peur de conséquences négatives par exemple dans leur entourage ou sur le lieu de travail. Ceci serait contre-indiqué et pourrait avoir pour conséquence de rendre inefficace le système de pétition publique qui se destine à être un outil moderne de démocratie directe.

Dès lors, la Commission nationale se demande s'il n'existent pas d'autres choix plus protecteurs de la vie privée des signataires. Différentes solutions ont été proposées dans nos pays voisins.

Ainsi, la Commission de la protection de la vie privée belge a estimé récemment[16] que même la publication des coordonnées du pétionnaire initial (nom, prénom, résidence et signature) ne se justifiait pas, après avoir procédé à une mise en balance des intérêts poursuivis et les risques présents dans le cadre de pétitions. Elle considère notamment qu'il « *serait tout à fait suffisant de ne reprendre que les initiales de la personne qui a déposé la pétition* ».

La CNIL française recommande[17] quant à elle de « *mentionner le nombre de signataires plutôt que de faire apparaître leur identité (et/ou leur adresse postale, électronique, numéro de téléphone…)* » et de « *ne pas permettre l'indexation de l'identité des personnes consultées par les moteurs de recherche* ».

Le modèle allemand, sur lequel se base le présent projet sous analyse, ne requiert que la publication du nom, du prénom ainsi que du Land dans lequel réside le signataire de la pétition concernée. Pour le reste, le système laisse le choix à la personne concernée de publier également son pseudonyme, son adresse e-mail, ainsi que ses éventuels commentaires[18].

Dans une étude de 2009[19], le « *Büro für Technikfolgen-Abschätzung beim deutschen Bundestag* » a dressé un inventaire des systèmes de pétition électronique existants. La Commission nationale voudrait relever le système adopté au Parlement Ecossais, qui permet au signataire de décider lui-même de publier son nom sur la liste ou non[20]. Le système retenu par l'état du Queensland en Australie va encore plus loin. En effet, celui-ci ne permet pas la publication des données des signataires d'une pétition, mais prévoit uniquement la publication du nombre total des signataires[21].

Au vu de ce qui précède, la CNPD estime que la publication des données des signataires d'une pétition publique devrait être d'avantage limitée que ne le prévoit le projet actuel. Elle recommande de laisser le libre choix aux signataires de voir publié ou non leur nom, prénom et leur localité de résidence. Cette solution présenterait l'avantage que les personnes soucieuses de leur vie privée pourraient garder confidentielles leurs données à caractère personnel, alors que les personnes souhaitant conférer un caractère public à leur soutien de la pétition auraient aussi le choix en ce sens. Alors même que les données de certains signataires ne seraient pas publiées, le système pourra toujours indiquer le nombre total de signataires pour une pétition donnée, en vue de renseigner le public sur le succès d'une pétition.

En tout état de cause – au cas où la Chambre des Députés opterait quand même pour rendre public en ligne l'identité des signataires – la Commission nationale considère qu'il serait préférable de ne pas inclure le code postal parmi les données indiquées

---

[16] CPVP, Avis n°01/2012 du 18 janvier 2012 portant sur la publicité des feuilletons de pétitions de la Chambre des Représentants (CO-A-2011-035).
[17] CNIL, Guide Communication Politique – Obligations légales et bonnes pratiques, p.25.
[18] Datenschutzerklärung Bundestag, E-petitionen, https://epetitionen.bundestag.de/index.php?action=data
[19] Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB), Bürgerbeteiligung durch E-Petitionen – Analysen von Kontinuität und Wandel im Petitionswesen, U. Riehm, C. Coenen, R. Lindner et C. Blümel, 2009, http://www.tab-beim-bundestag.de/de/pdf/publikationen/buecher/riehm-etal-2009-127.pdf
[20] TAB, op. cit., p. 141.
[21] TAB, op. cit., p. 175.

Annexes

ensemble avec les noms et la localité.

Enfin, toutes les mesures possibles devraient être prises, afin d'éviter une indexation de l'identité des signataires par les moteurs de recherche. Considérant que l'insertion de balises empêchant l'indexation des pages internet concernées se sont avérées insuffisantes jusqu'à ce jour, la Commission nationale recommande une insertion du nom et prénom au format image au lieu d'un format texte. L'ajout des balises prémentionnées peut bien évidemment être effectué en tant que mesure supplémentaire de protection contre d'éventuels abus.

La Commission nationale salue la faculté laissée au signataire de retirer en cours de route son soutien à la pétition en supprimant sa signature.

Ainsi décidé à Luxembourg en date du 13 juillet 2012.

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 déterminant les modalités et les conditions de fonctionnement du registre national du cancer et modifiant le règlement grand-ducal du 20 juin 1963 rendant obligatoire la déclaration des causes de décès

Délibération n°239/2012
du 24 septembre 2012

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

Faisant suite à la demande lui adressée par Monsieur le Ministre de la Santé en date du 6 août 2012, la Commission nationale expose ci-après ses réflexions et commentaires au sujet de l'avant-projet de règlement grand-ducal déterminant les modalités et les conditions de fonctionnement du registre national du cancer et modifiant le règlement grand-ducal du 20 juin 1963 rendant

obligatoire la déclaration des causes de décès

Dans l'ensemble, la CNPD accueille favorablement l'avant-projet de règlement grand-ducal dont les dispositions sont très respectueuses à l'égard de la protection des données et de la vie privée et félicite les auteurs d'avoir intégré dans le texte suffisamment de dispositions qui prévoient des garanties appropriées.

Elle voudrait cependant formuler ci-après quelques réflexions, observations et recommandations susceptibles d'améliorer le texte en projet.

- Légitimité de la collecte et de l'utilisation des données dans le registre national du cancer (ci-après « RNC »)

Pour être licite, tout traitement de données doit se baser sur un des critères de légitimation que prévoit la loi modifiée du 2 août 2002 sur la protection des données. Parmi ces critères figure aussi le consentement.

L'avant-projet indique que le traitement des données du RNC est légitimé sur le consentement implicite des patients. En effet, l'exposé des motifs relatif à l'avant-projet de règlement grand-ducal précise que la « *recherche de l'exhaustivité engendre la construction d'un RNC reposant sur un consentement implicite du patient. En effet, il a été démontré dans d'autres pays européens, que le fait de demander un consentement préalable écrit systématique pour la participation au RNC engendrait une diminution rapide de l'exhaustivité et rendait les résultats épidémiologiques contestables* ».

Or, lorsqu'un traitement de données de santé est basé sur le consentement, le consentement implicite ne suffit pas, alors que la loi modifiée du 2 août 2002 (tout comme la directive 95/46/CE) exige le consentement exprès préalable (art. 6 (2)(a)).

La CNPD comprend parfaitement que le RNC doit être aussi exhaustif que possible pour que les données du RNC soient utilisables à des fins cliniques, scientifiques et épidémiologiques et qu'il n'est dès lors pas envisageable de recueillir systématiquement le consentement exprès des patients.

Les recommandations pour la confidentialité de l'enregistrement des cancers au sein de la population de l'Union européenne, adoptées par le Réseau Européen de Registres de Cancers et qui tiennent aussi compte de la directive 95/46/CE, énumèrent d'ailleurs une série d'autres raisons pour arriver à la conclusion que l'exigence du consentement exprès « *rend pratiquement impossible l'utilisation des données issues des registres du cancer* » (point 1.3.2. des susdites Recommandations).

La directive 95/46/CE et la loi modifiée du 2 août 2002 prévoient d'autres critères de légitimation que le consentement exprès. Ainsi, le traitement de données de santé est notamment légitime lorsque celui-ci s'avère nécessaire pour un motif d'intérêt public (art. 6(2)(g) de la loi). Il va sans dire que la mise en place d'un RNC répond bien à un motif d'intérêt public et plus particulièrement en matière de santé publique.

La Commission nationale est dès lors d'avis que le traitement de données mise en œuvre dans le cadre du registre national du cancer doit être considéré comme légitime sur base du critère du « motif d'intérêt public » et non pas sur base du consentement.

- Le droit d'opposition, une garantie appropriée qui respecte l'autodétermination du patient

Lorsque les auteurs de l'avant-projet parlent de consentement implicite, ils se réfèrent en réalité au droit d'opposition. Par rapport au critère de légitimation du motif d'intérêt public qui sert

comme base juridique au RNC, le droit d'opposition (ou le consentement implicite) doit être considéré comme une garantie ou sauvegarde supplémentaire en termes de protection de la vie privée.

Le « consentement » du patient en tant que garantie appropriée ne doit pas être confondu avec le « consentement » qui sert de base juridique à un traitement de données de santé. En effet, comme expliqué plus haut, ce dernier doit toujours être exprès, alors que le consentement en tant que garantie de l'autodétermination peut être exprimé sous forme implicite ou être conféré sous forme d'un droit d'opposition.

La CNPD salue dès lors que les patients puissent s'opposer préalablement ou postérieurement à ce que leurs données figurent au registre national du cancer. D'aucuns diront que le droit d'opposition n'est pas compatible avec le principe de l'exhaustivité des données du registre. Or, les expériences faites à l'étranger montrent que le taux des patients, atteints d'un cancer, qui s'opposent à ce qu'ils figurent dans un registre est extrêmement faible et ne porte pas à conséquence.

Dans d'autres pays européens comme p.ex. en France, le droit d'opposition est également accordé au patient.
Etant donné que le consentement ne sert pas comme critère de légitimité au RNC et en considération des développements formulés plus haut, la CNPD propose de ne pas utiliser à l'endroit de l'article 4 de l'avant-projet de règlement grand-ducal les termes de « consentement initial » et de « consentement exprès », alors que cette terminologie prête à confusion quant à la base juridique qui légitime le traitement de données de santé dans le cadre du RNC.

Pour ce qui est de l'exercice du droit d'opposition avant le début du traitement des données, l'article 4 paragraphe (3) du texte en projet prévoit que les données du patient ne sont pas communiquées au RNC, mais que le gestionnaire du RNC reçoit toutefois l'information qu'il s'est opposé.

La Commission nationale se demande pourquoi le gestionnaire doit recevoir cette information. Si dans ces cas le registre ne contiendra pas de données sur les patients opposants, le gestionnaire connaîtra cependant leur identité et disposera en quelque sorte d'une « liste noire ». Nous estimons que pour des raisons statistiques, il suffit que le gestionnaire dispose uniquement

du nombre des patients qui se sont opposés. Lorsque par après un patient décide de participer au RNC, la source communiquera ses données au RNC et il sera sans importance pour le gestionnaire de savoir que ce patient n'a pas voulu initialement figurer dans le RNC au moment du diagnostic. Nous suggérons dès lors de supprimer la deuxième phrase du paragraphe (3) de l'article 4 et d'adapter aussi en ce sens la brochure d'information contenue à l'annexe 1 du règlement grand-ducal.

- Le contenu du registre

L'annexe 2 du règlement grand-ducal sous examen énumère les données qui doivent être fournies par les sources et figurer dans le RNC.

L'article 4 de la loi modifiée du 2 août 2002 prévoit que seules les données adéquates et strictement nécessaires à la réalisation des finalités du traitement doivent être collectées et utilisées par le responsable du traitement.

A ce titre, la CNPD ne comprend pas pourquoi il serait nécessaire de collecter la date de naissance exacte (j/m/a) et le code postal en plus de la localité. Elle estime que pour effectuer des analyses de survie, il suffit de disposer du mois et de l'année de naissance et qu'il n'est pas indispensable de connaître le jour de naissance. Elle suggère dès lors de n'enregistrer dans le RNC que les seuls mois et année de naissance.

La CNPD ne voit pas non plus la nécessité de vouloir collecter le code postal en plus de la localité. Il est clair que pour pouvoir analyser les liens entre environnement et cancer il faut disposer d'une donnée géographique ; or, nous pensons que le code postal est une donnée trop détaillée qui n'est pas indispensable pour faire ce genre de recherche. Il n'est pas nécessaire de savoir si un patient vit ou a vécu dans une rue X ou dans une rue parallèle Y distante de quelques mètres. Il est vrai aussi que la commune de résidence comme seule donnée géographique peut s'avérer trop imprécise surtout lorsqu'il s'agit d'une commune ayant une superficie plus importante. C'est pourquoi nous proposons de travailler avec un géocode qui serait moins précis que le code postal, mais en même temps plus précis que la situation géographique d'une commune. Ceci correspond aux Recommandations du ENCR précitées et à ce qui est également prévu dans la législation belge sur les registres de cancer.

Le texte en projet a le mérite d'imposer une procédure de pseudonymisation des données contenues dans le RNC. Or, un patient pourra facilement être identifié p.ex. lorsqu'il habite dans une petite commune et que l'on combine les données « date de naissance exacte – sexe – date de diagnostic – code postal ».

- Les mesures pour garantir la sécurité et la confidentialité des données

Alors que le fichier dont question est susceptible, du fait de sa nature, des catégories de personnes concernées, des données recueillies et de la durée de conservation, de présenter des risques substantielles pour la vie privé des patients et de leur proches, la Commission nationale considère qu'il est impératif d'encadrer son accès et son fonctionnement de mesures et procédures strictes assurant la confidentialité et la sécurité des données à caractère personnel.

Pour les finalités poursuivies plus amplement décrites ci-avant, il n'est pas nécessaire que les personnes autorisées à consulter le fichier obtienne connaissance de l'identité des patients dont les données d'évolution clinique et de traitement y sont renseignées, à l'exception du médecin traitant qui fournit les données et les revoit ou les complète en fonction de son dossier du patient personnel. Il apparaît indispensable d'éviter toute

Annexes

suspicion que les indications du registre du cancer puissent conduire, ne serait-ce que par des indiscrétions individuelles, à ce que la maladie et son évolution soient connues par des personnes non autorisées et que le risque de traitement discriminatoire, y compris par les compagnies d'assurances, employeurs ou autres tiers de la personne concernée, mais également ultérieurement de ses proches, puisse être explicitement exclu.

C'est pour cette raison que le recours à la procédure de dépersonnalisation des enregistrements consultables nous paraît particulièrement précieux et indispensable.

La Commission nationale salue dans ce contexte les différentes dispositions du texte sous avis prévoyant les mesures qui doivent garantir la confidentialité et la sécurité des données.

En ce qui concerne la charte de sécurité qui devra être adoptée avec le règlement interne, la CNPD souhaiterait bien évidemment être consultée préalablement.

Ainsi décidé à Luxembourg en date du 24 septembre 2012.

La Commission nationale pour la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

Avis de la Commission nationale pour la protection des données à l'égard du projet de loi n°6418 relatif à l'organisation du casier judiciaire et aux échanges d'informations extraites du casier judiciaire entre les Etats membres de l'Union européenne et modifiant le Code d'instruction criminelle

Délibération n°304/2012
du 25 octobre 2012

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 Président de la commission juridique de la Chambre des Députés et Monsieur le Ministre de Justice, la Commission nationale formule par la présente les observations qu'elle a eu l'occasion d'exposer oralement lors de la séance de la commission parlementaire le 10 octobre 2012.

Elle entend limiter ses réflexions aux dispositions relatives à la délivrance du bulletin n°2 du casier judiciaire et au traitement des données résultant des extraits du casier judiciaire par les administrations, autorités et organismes publics ainsi que par les employeurs du secteur privé. Les autres dispositions du texte sous revue, en particulier celles relatives aux échanges d'informations entre Etats membres de l'Union européenne et portant transposition de la décision-cadre afférente, n'appellent pas d'observations de la part de notre Commission nationale.

I) Prise en compte de la règle édictée par l'article 8 de la loi sur la protection des personnes à l'égard du traitement des données à caractère personnel

En son paragraphe (2), l'article 8 de la loi cadre modifiée du 2 août 2002 sur la protection des données dispose que le traitement de données relatives aux infractions, condamnations pénales et aux mesures de sûreté *« ne peut être mis en œuvre qu'en exécution d'une disposition légale ».*

La même loi englobe sous la définition de traitement *« toute opération ou ensemble d'opérations (…) appliquées à des données, telles que la collecte, l'enregistrement, l'organisation, la conservation, (…), la consultation, l'utilisation, la communication par transmission, ou toute autre forme de mise à disposition, le rapprochement (…) »* de données concernant une personne identifiée ou identifiable.

Sauf l'exception prévue au profit des activités journalistiques et de création artistique et littéraire aux termes de l'article 9 de la même loi (pour réconcilier les deux droits fondamentaux, à savoir la liberté d'expression avec le droit à la vie privée) les seuls textes légaux autorisant expressément le traitement de données par l'employeur dans le contexte du recrutement ou de la gestion des candidatures sont les lois spéciales prévoyant le recueil des données du casier judiciaire par les établissements financiers concernant les personnes auxquelles des fonctions dirigeantes sont confiées (loi du 5 avril 1993 relative au secteur financier) et la loi du 12 novembre 2002 relative aux activités privées de gardiennage et de surveillance pour ce qui est de l'embauche des convoyeurs de fonds et agents de sécurité ainsi que la législation relative aux agents et courtiers d'assurance.

Par ailleurs le projet de loi examiné reprend en son article 8 la possibilité d'obtenir communication du bulletin n°2

pour 1) les administrations de l'Etat saisies de demandes d'emplois publics, 2) les autorités militaires pour les candidats qui demandent à contracter un engagement et 3) aux administrations et personnes morales luxembourgeoises de droit public énumérées par règlement grand-ducal (qui remplacera l'arrêté ministériel modifié du 22 novembre 1977 qui règle actuellement la délivrance des bulletins n°2 aux administrations et organismes publics).

Hormis ces hypothèses prévues par la loi, le recueil de données résultant du casier judiciaire par l'employeur ou le futur employeur serait illicite.

Dans la réalité des choses l'usage généralisé depuis des décennies de demander aux candidats la production d'un extrait récent (bulletin n°3 que les personnes concernées se font délivrer à leur demande par le Parquet général) lorsqu'ils postulent pour un emploi n'a nullement disparu depuis l'entrée en vigueur de la loi du 2 août 2002. La CNPD, à l'instar de son homologue la Commission de protection de la vie privée en Belgique, a donc dû se résoudre à conseiller aux employeurs ne bénéficiant pas d'une autorisation légale de se borner à prendre connaissance du contenu des bulletins produits par les candidats sans pour autant pouvoir en faire mention dans des dossiers structurés ou fichiers informatiques. Bien que non prévue par une disposition légale, une telle communication/consultation de données relatives aux condamnations n'entre pas en conflit avec l'interdiction posée par la loi modifiée du 2 août 2002 sur la protection des données pour la bonne et simple raison que le champ d'application de celle-ci se limite aux traitements automatisés (informatiques) et aux seuls traitements manuels pour lesquels les données sont appelées à figurer dans un fichier structuré.

La Commission nationale n'étant pas favorable à de telles jongleries avec les limites formelles des textes et préférant que les dispositions légales soient en harmonie avec les pratiques généralisées qui ne heurtent pas la sensibilité des citoyens et qui sont couramment suivies dans la réalité des choses, nous suggérons au législateur d'introduire dans le corps du projet de loi une disposition (une proposition de rédaction figure en annexe au présent avis) servant de base légale légitimant le traitement de cette catégorie particulière de données (relatives aux condamnations, infractions pénales et mesures de sûreté) pour les finalités usuelles d'évaluation des candidatures dans le cadre d'une procédure de recrutement et pour une

conservation dans le dossier du collaborateur pendant une durée limitée de deux ans maximum.

Une telle mesure œuvrerait par ailleurs dans le sens d'un rapprochement (encore que des différences subsisteraient) de la situation des employeurs du secteur privé avec ceux du secteur public, ce qui se justifie dans de nombreux cas où la fonction à pouvoir au sein de l'autorité, de l'administration ou de l'organisme public en question ne participe pas réellement de l'exercice de la puissance publique.

II) Condamnations mentionnées sur le bulletin délivré à l'intéressé

Deux observations peuvent être faites à cet égard, à savoir

1) L'intéressé ne se verra remettre à sa demande que le bulletin n°2 (qui est incomplet et tout comme actuellement le bulletin n°3) ne renseigne pas toutes les condamnations. *Le droit d'accès* visé à l'article 12 de la directive 95/46/CE et repris *à l'article 28 de la loi modifiée du 2 août 2002 sur la protection des personnes à l'égard du traitement des données à caractère personnel n'en est-il pas indûment et excessivement restreint par la disposition des articles 7 et 8 du projet de loi ?*

Il résulte des explications de la représentante du Parquet général à la Commission juridique de la Chambre des Députés que l'intéressé peut parfaitement obtenir accès et consulter sur place l'intégralité des inscriptions le concernant en se présentant au guichet du casier judiciaire alors même qu'il ne peut obtenir délivrance d'un extrait que sous la forme du bulletin n°3 (et à l'avenir du bulletin n°2 après la suppression du bulletin n°3) tel que prévu à l'article 10 du règlement grand-ducal (modifié) du 14 décembre 1976 portant réorganisation du casier judiciaire.

Son avocat y a également accès dans le cadre de toute procédure judiciaire pénale.

Il est vrai que ni le texte du règlement grand-ducal du 14 décembre 1976 ni celui du projet de loi sous revue n'indiquent un tel accès. La Commission nationale estime qu'il serait souhaitable que cette faculté soit expressément prévue et qu'elle soit en outre portée à la connaissance du public dans les guichets (y compris sur la page web du guichet électronique) du casier judiciaire.

La Commission nationale partage cependant le choix des auteurs du texte sous examen de ne pas prévoir la délivrance d'un extrait complet des inscriptions du casier judiciaire à l'intéressé par peur qu'une telle pratique n'évolue dans ce sens que de plus en plus d'employeurs n'en exigent copie dans le cadre des procédures de recrutement.

Le bulletin dont la délivrance à la personne concernée y est prévue au point 4) de l'article 8 sert en effet à celle-ci pour être joint en annexe à une demande d'emploi ou pour en faire état à l'occasion d'un entretien d'embauche. Il est donc en quelque sorte dans l'intérêt des intéressés que les mentions de l'extrait qui leur est délivré ne mentionne pas les éventuelles condamnations pour faits mineurs ou à des peines assorties de sursis.

2) Les condamnations mentionnées au bulletin n°2 visé à l'article 8 du projet de loi comprennent désormais celles pour contraventions de police (de 1ère et 2ème classe) et pour infractions à la législation relative à la circulation routière (à l'exception des contraventions en matière de stationnement) alors que le bulletin n°3 délivré actuellement ne renseigne que les condamnations à des peines privatives de liberté pour crime et délit, sauf condamnations conditionnelles avec ou sans mise à l'épreuve.

L'adoption du projet de loi aura donc pour conséquence une visibilité substantiellement

élargie de l'employeur sur les condamnations du candidat ou de son nouveau salarié. Certes, il ne s'agira que d'un alignement sur ce point sur la situation des fonctionnaires et employés publics, mais il n'en reste pas moins que la Commission nationale n'est pas convaincue qu'il est indispensable d'englober ces condamnations pour les infractions à la législation sur la circulation routière ni celles pour les peines de police.

Ce n'est en effet qu'une fraction infime des candidats à l'emploi ou du personnel employé qui exercent une fonction de chauffeur pour lesquelles une disposition spéciale pourrait être nécessaire.

La Commission nationale est consciente que la réduction du nombre de bulletins distincts dont le nouveau texte prévoit la délivrance comme extraits du casier judiciaire emporte forcément certains changements par rapport à la situation existante. Elle peut concevoir que des condamnations à des peines privatives de liberté supérieures à six mois figurent dorénavant sur l'extrait y compris celles assorties de sursis pour crimes et délits.

L'inclusion dans le bulletin remis à l'employeur de condamnations à des peines de police ne procède en revanche pas d'une nécessité évidente.

Pour le recrutement du personnel appelé à exercer leur fonction au volant de véhicules automoteurs, il serait concevable de recourir à un texte spécifique ultérieur exigeant la production d'une pièce du Ministère des transports sur la situation du permis de conduire de l'intéressé, le permis à points étant aussi pertinent que le relevé des condamnations pénales en matière d'infractions à la législation sur la circulation routière.

III) Finalités justifiant la délivrance du bulletin n°2 aux autorités publiques et personnes morales de droit public et administrations énumérées au projet de règlement grand-ducal

La Commission nationale se rallie à la demande formelle du Conseil d'Etat, formulée dans son avis du 13 juillet 2011, de voir préciser dans la loi les finalités pour lesquelles les organismes publics peuvent se faire délivrer un extrait des inscriptions au casier judiciaire de leurs agents ou des personnes y sollicitant un emploi (ne serait-ce que pour participer à une soumission de marché public) ou dans le contexte d'examen des critères d'honorabilité. Ceci découle du principe de légalité posé à l'article 8 § 2 de la Convention européenne des Droits de l'Homme et des Libertés fondamentales pour toute ingérence d'une autorité publique dans la sphère privée des citoyens.

Les principes de base du droit fondamental des citoyens à bénéficier de la protection de leurs données à caractère personnel ont acquis depuis leur inscription à l'article 8 de la Charte des droits fondamentaux de l'Union européenne, un rang constitutionnel que nombre d'Etats membres ont formellement inscrits dans leur Constitution nationale. L'intention d'en faire de même à l'article 30 nouveau de la Constitution luxembourgeoise reflète donc le vœu d'inscrire un droit reconnu à chaque individu par les travaux du Conseil de l'Europe (développement spécifique du droit au respect de la vie privée et familiale inscrit à l'article 8 de la Convention européenne des droits de l'homme). Ce droit est même devenu un droit fondamental autonome dans l'ordre juridique de l'Union européenne (comme le documente l'inscription de deux articles spécifiques afférents dans la Charte, à savoir l'article 7 (vie privée) et l'article 8 (données à caractère personnel)).

L'inscription du droit à la protection des données à caractère personnel à l'article 30 nouveau viendra donc compléter, de façon cohérente avec les textes de l'Union européenne, la référence à la protection de la vie privée inscrite au paragraphe (3) de l'article 11 de la Constitution depuis sa révision du 29 mars 2007.

Parmi les démembrements essentiels du droit à la protection des données il y a lieu de prendre en considération – en tenant compte de l'exigence d'une finalité déterminée explicite et légitime à la base de la collecte et du traitement des données (et de l'interdiction de leur utilisation à des fins incompatibles); - les principes suivants :

a) consentement ou autre critère de légitimation du traitement prévu par la loi

Il s'agit en l'occurrence des missions d'intérêt public qui relèvent de l'exercice de l'autorité publique, acteurs énumérés au projet de règlement grand-ducal.

b) le principe de nécessité et de proportionnalité

Il s'applique à l'étendue des catégories de données traitées et des opérations de traitements y appliquées (et donc aussi à la transmission à des tiers sous réserve du respect de la finalité (cf. ci-dessus), à la transmission et à la durée la conservation des données (du moins celle précédant éventuellement leur anonymisation complète et irréversible).

c) le principe de transparence à l'égard des personnes concernées se traduisant par l'obligation de les informer préalablement des traitements et par leur droit d'accès, de rectification ou de mise à jour si nécessaire et d'effacement si les données, leur utilisation ou durée de conservation s'avère excessive.

C'est par référence à l'exigence de transparence que nous avons donné à considérer au point III ci-dessus qu'il y aurait lieu de prévoir la possibilité de consultation par les personnes concernées de l'intégralité des inscriptions au casier judicaire et leur information des demande de délivrance d'extraits par les autorités, administrations et organismes publics visés aux points 1 à 3 du premier paragraphe de l'article 8 du projet de loi.

IV) Transparence et information des personnes concernées en cas de délivrance d'un extrait (bulletin n°2)

Si le projet de loi débouchera sur un certain rapprochement de la situation des employeurs du secteur privé avec l'Etat, les communes, les établissements et autres organismes publics énumérés à l'article 1er du projet de règlement grand-ducal, pour autant que le législateur suivra notre recommandation d'insérer un paragraphe supplémentaire à l'article 8 du projet de loi autorisant les employeurs du secteur privé à se faire remettre

Annexes

par les intéressés une copie du bulletin n°2 délivré à ces derniers et de pouvoir le conserver pendant une durée limitée (nous suggérons 2 ans dans le cadre de la gestion des candidatures à l'embauche et du suivi afférent) la procédure d'obtention des renseignements restera radicalement différente.

S'il peut se justifier que les autorités, administrations et organismes publics puissent se faire délivrer directement de tels extraits du casier judiciaire, il s'avère nécessaire de mettre en place un minimum de mesures de sauvegarde destinées à prévenir et détecter des abus.

Bien sûr, il reviendra au responsable hiérarchique des autorités, administrations et organismes publics de veiller à ce que sous leur autorité (responsables du traitement) ne soient demandés des extraits du casier judiciaire que dans les seuls cas prévus par la loi (et le règlement grand-ducal) et seulement en cas de nécessité dûment justifiée.

Par ailleurs, il nous paraît impératif de prévoir dans le texte même de la loi, l'information systématique et obligatoire des personnes concernées de toute demande et délivrance d'un extrait les concernant avec mention de l'organisme demandeur.

Annexe : Proposition de rédaction d'un amendement pour compléter l'article 8 du projet de loi sous revue.

Article 8 :

Nouveau § 2

Dans les cas visés aux points 1 à 3 la personne concernée est informée préalablement et pourra s'opposer à la délivrance conformément à l'article 30 de la loi modifiée du 2 août 2002 sur la protection des personnes à l'égard du traitement des données à caractère personnel.

Nouveau § 3

Les employeurs peuvent demander dans le cadre de la gestion des candidatures et du recrutement de personnel la production par les postulants d'un extrait du casier judiciaire et traiter les données afférentes pour les besoins de la gestion des ressources humaines sous réserve des limitations prévues au paragraphe 4).

Nouveau § 4

Les extraits du casier judiciaire délivrés aux administrations et organismes publics et aux écoles européennes saisis de demandes d'emploi et ceux remis par les personnes concernées aux employeurs du secteur privé portant des indications autres que

la mention « Néant » ne peuvent être conservés, même sous forme de photocopies, au-delà d'un délai de 24 mois après la date d'établissement du bulletin. Tout traitement des données afférentes doit cesser après l'écoulement de ce délai.

Ainsi décidé à Luxembourg
en date du 25 octobre 2012.

La Commission nationale pour
la protection des données

Gérard Lommel
Président

Pierre Weimerskirch
Membre effectif

Thierry Lallemang
Membre effectif

Resolution on the European data protection reform Spring Conference 2012 of the European Data Protection Commissioners (Luxembourg, 3-4 May 2012)

The Spring Conference of the European Data Protection Commissioners, (130 delegates from 38 countries) meeting in Luxembourg on 3-4 May 2012, discussed recent developments for the modernization of the data protection frameworks of the EU, the Council of Europe and the OECD.

The Conference recognized the current efforts seeking to guarantee to citizens and consumers enhanced rights and effective ways for exercising them, while taking into account technological changes and globalization. The Data Protection Commissioners welcome in particular the following key aims:

- the strengthening and clarification of the rights of individuals;
- the emphasis put on accountability of data controllers and processors;
- the reduction of some administrative burdens and the search for consistency;
- the key role devoted to independent data protection authorities;
- the move to develop a more comprehensive framework ensuring the application of the fundamental data protection principles across all areas;
- the initiative of the Council of Europe to revise Convention 108, which has been leading the way since 1981, including the objective to assure consistency and compatibility with the legal framework of the EU and supporting firmly the intention to follow more closely the implementation of the Convention by States Parties;
- the ongoing reflection process at the level of OECD on the evolving international privacy landscape.

The Conference also analysed the proposed improvement of the European legal texts against the background of the international developments in the field of data processing and privacy, including in the transatlantic relations, in particular in light of the white paper of the U.S. Administration released on 23 February 2012 and the FTC Report published in March 2012.

Taking into account the previously adopted resolutions[22], the Conference studied in more detail the recent legislative package of the European Commission aimed at modernizing EU data protection rules. The Conference welcomes that the proposals address the new challenges resulting from the pervasive collection and use of personal

[22] Resolution on the need for a comprehensive data protection framework adopted by the European Data Protection Commissioners Conference in Brussels, 5 April 2011 and resolution on future development of data protection and privacy adopted by the European Privacy and Data Protection Commissioners Conference in Prague, 30 April 2010.

data in a connected and globalised world. The Data Protection Commissioners are especially pleased with:

- the rules providing for more transparency and greater control over the data processing;
- the codification of the principle of data minimization;
- greater redress possibilities for data subjects;
- the strengthening of rules concerning the rights to access and to object;
- the inclusion of rights in order to address the challenges arising out of the online environment (a specific protection of children, the "right to be forgotten" and the new right to data portability);
- the attempt to introduce simplified and consistent rules for data controllers;
- the introduction of the principle of accountability;
- the introduction of mechanisms and tools serving as incentives to demonstrate accountability such as data protection by design and by default, privacy impact assessments, the appointment of DPOs and data breach notification duties;
- the introduction of a one-stop shop solution both for controllers by creating the concept of a lead authority cooperating with other concerned DPAs and also for individuals (subject to the latter being improved further);
- the requirement of an active cooperation between DPAs and the strengthening of their independence and powers, including the introduction of administrative fines.

The Data protection Commissioners are convinced that the expertise and practical experience of DPAs can play an important role in the practical application of data protection rights also in the future, in particular through:

1. the mandatory consultation of DPAs on legislative measures at EU as well as at national level;
2. the development of guidelines and recommendations for the practical implementation, considering national and sectoral specificities;
3. the possibility to carry out ex officio investigations and audits.

They also highlighted that a good performance of these and other tasks, including in international cooperation in the EU and beyond, depends on the continued availability of adequate financial, technical and human resources.

With regard to the consistency of the EU package, the conference warns against the risk that too many exemptions and derogations hinder the effective application of core data

protection principles. Exemptions provided for public authorities, law enforcement activities or the use of data for governmental purposes, including fiscal purposes, must comply with the core aspects of data protection law. Essential data protection rules should be applied in a consistent way and independent of the respective sector.

The conference therefore notes that further improvements to the current proposals are needed, especially to bring the proposed Directive regarding the area of police and justice more in line with the core principles of the General Data Protection Regulation. Rules on the transfer of data between private parties and law enforcement bodies are, for instance, still missing. Having this in mind, the Data Protection Commissioners are prepared to contribute actively to the success of a modernised and effective data protection framework for Europe.

The strengthening and simplification of data protection is more important than ever. The Conference therefore encourages both the Council of Europe to accomplish the ambitious revision of Convention 108 and the European Parliament and the Council to maintain the current progress in the legislative process.

Participations aux travaux internationaux

Documents adoptés par le groupe de travail européen « Article 29 » en 2012

Document	Date d'adoption	Référence
Avis 08/2012 apportant des contributions supplémentaires au débat sur la réforme de la protection des données	05.10.2012	WP 199
Avis 07/2012 sur le niveau de protection des données à caractère personnel dans la Principauté de Monaco	19.07.2012	WP 198
Avis 05/2012 sur l'informatique en nuage	01.07.2012	WP 196
Document de travail 02/2012 établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes pour les sous-traitants	06.07.2012	WP 195
Avis 04/2012 sur l'exemption de l'obligation de consentement pour certains cookies	07.06.2012	WP 194
Avis 3/2012 sur l'évolution des technologies biométriques	27.04.2012	WP 193
Avis 02/2012 sur la reconnaissance faciale dans le cadre des services en ligne et mobiles	22.03.2012	WP 192
Avis 01/2012 sur les propositions de réforme de la protection des données	23.03.2012	WP 191
Programme de travail 2012-2013	01.02.2012	WP 190
Document de travail 01/2012 sur epSOS	25.01.2012	WP 189

7 Annexes

Groupe de travail européen « Article 29 » - Programme de travail 2012-2013

Adopté le 1er février 2012

Mission

Le groupe de travail a été institué par l'article 29 de la directive 95/46/CE et a pour mission (article 30, paragraphe 1) :

a) d'examiner toute question portant sur la mise en oeuvre des dispositions nationales prises en application de ladite directive, en vue de contribuer à leur mise en oeuvre homogène ;
b) de donner à la Commission un avis sur le niveau de protection dans la Communauté et dans les pays tiers ;
c) de conseiller la Commission sur tout projet de modification de la présente directive, sur tout projet de mesures additionnelles ou spécifiques à prendre pour sauvegarder les droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel, ainsi que sur tout autre projet de mesures communautaires ayant une incidence sur ces droits et libertés ; et
d) de donner un avis sur les codes de conduite élaborés au niveau communautaire.

Ces tâches doivent également être accomplies dans le secteur des communications électroniques (article 15, paragraphe 3, de la directive 2002/58/CE).

Activités en 2012-2013

Pour la période 2012-2013, le groupe de travail s'est fixé pour objectif non seulement d'assurer une mise en oeuvre cohérente et correcte du cadre juridique actuel, mais également de continuer à préparer le futur cadre juridique proposé par la Commission européenne le 25 janvier 2012.

Le cadre juridique révisé aura des répercussions à la fois sur la réglementation relative à la protection des données et sur le fonctionnement du groupe de travail proprement dit. De plus, l'innovation et le développement technologique constants, en particulier dans l'environnement en ligne, représentent un défi à relever. Le groupe de travail entend préciser et renforcer le rôle de tous les acteurs dans le domaine de la protection des données: personnes concernées, responsables du traitement des données et autorités chargées de la protection des données. Le groupe de travail examinera aussi sa propre efficacité et poursuivra l'amélioration de ses méthodes de travail, en étroite collaboration avec son secrétariat. Le groupe de travail va en outre développer ses échanges avec les autorités internationales chargées de la

protection des données ainsi que d'autres institutions et organisations, tant à l'intérieur qu'à l'extérieur de l'Union européenne, y compris le Conseil de l'Europe et la Commission fédérale du commerce des États-Unis.

Compte tenu des défis exposés ci-dessus, le groupe de travail entend se concentrer sur six thèmes stratégiques principaux et quelques thèmes d'actualité qu'il juge les plus pertinentes aux fins de la protection des données:

I) mettre en oeuvre la directive existante en matière de protection des données et préparer un cadre juridique futur ;
II) accroître l'efficacité du groupe de travail « article 29 » et des autorités chargées de la protection des données ;
III) répondre aux défis technologiques ;
IV) assurer une approche cohérente et efficace en matière de protection des données, dans le domaine de la liberté, de la sécurité et de la justice ;
V) faire face à la mondialisation et aux transferts internationaux ;
VI) thèmes d'actualité.

Par ailleurs, le groupe de travail reste disponible pour traiter les demandes d'avis de la Commission, du Conseil et du Parlement européen, ainsi que toutes autres questions imprévues. Les questions en matière de protection des données peuvent être étroitement liées à plusieurs niveaux, et le groupe de travail choisira donc le meilleur moyen de les traiter. Il examinera la mise en oeuvre de ce programme de travail à intervalles réguliers et se réserve le droit, le cas échéant, de le préciser davantage ou de le mettre à jour.

I - Assurer la mise en oeuvre correcte du cadre juridique actuel et préparer l'avenir

- Interprétation des principales dispositions
  - restriction de la finalité (de la « description de la finalité » à l'« usage compatible », et exceptions éventuelles)
  - autres motifs de traitement, s'appuyant sur des « intérêts légitimes »
- Examen et conseil relatifs aux principales notions figurant dans la proposition portant sur un nouveau cadre juridique
- Suivi de la mise en oeuvre de la directive « Vie privée et communications électroniques »
  - notification des violations (article 4, paragraphe 5) (par ex. consultation et évaluation de la gravité)
- Assurer la cohérence par rapport à d'autres cadres (internationaux) en matière de protection des données (OCDE, Conseil de l'Europe)

II - Accroître l'efficacité des autorités chargées de la protection des données et du groupe de travail « article 29 »

- Garantir l'existence d'un groupe de travail « article 29 » indépendant et efficace
- Renforcer l'application des règles (inventaire des prérogatives permettant d'approfondir la coopération entre les autorités chargées de la protection des données, développement et amélioration des méthodes d'enquête, harmonisation des pouvoirs des autorités chargées de la protection des données et promotion de la coopération internationale entre les autorités chargées de la protection de la vie privée)

III - Défis technologiques

- Informatique dématérialisée
- Reconnaissance faciale
- Utilisation de techniques d'anonymisation
- Système de suivi par capture d'empreintes numériques (device fingerprinting)/ identification de dispositif (device ID)
- Lignes directrices sur les applications smartphone

IV - Assurer une approche cohérente et efficace en matière de protection des données dans le domaine de la liberté, de la sécurité et de la justice

7 Annexes

- Evaluation de la mise en oeuvre de la décision-cadre 2008/977/JAI
- Avenir de la surveillance relevant de l'ancien troisième pilier
- Négociations d'un accord général entre l'Union européenne et les États-Unis en matière de protection des données à propos des données liées à l'application de la législation
- Système européen de surveillance du financement du terrorisme
- Echange de données PNR avec les pays tiers
- Propositions relatives à un système européen de données PNR
- Notion de « frontières intelligentes »
  - système d'entrée/sortie
  - programme d'enregistrement des voyageurs
- Système européen de surveillance des frontières (EUROSUR)
- Propositions (législatives) sur l'utilisation de scanners corporels
- Modèle européen d'échange d'informations – EIXM
- Questions liées à la coopération dans le domaine de la justice

V - Faire face à la mondialisation et aux transferts internationaux

- Efforts de normalisation (ISO, CEN)
- Transferts internationaux
  - caractère adéquat du niveau de protection assuré dans les pays tiers
  - règles d'entreprise contraignantes (BCR)
- rationaliser les procédures en vigueur (y compris la reconnaissance mutuelle)
- mise au point de règles d'entreprise contraignantes (BCR) pour les sous-traitants
  - sphère de sécurité
  - obtention de preuves préalablement au procès

VI - Thèmes d'actualité

- Administration en ligne
- IMI
- Aspects financiers
- Biométrie
- Agence mondiale antidopage (AMA)
- Données en matière de santé

Groupe de travail européen « Article 29 » - Avis 01/2012 sur les propositions de réforme de la protection des données

Adopté le 23 mars 2012

Table des matières

Introduction

Le groupe de travail « article 29 » sur la protection des données (ci-après le « groupe de travail » ou le "groupe de travail « article 29 »") salue les propositions adoptées par la Commission européenne dans le but de renforcer la position des personnes concernées, d'accroître la responsabilité des responsables du traitement et de consolider la position des autorités de contrôle, sur le plan tant national qu'international. Sous réserve d'améliorations à apporter, les règles proposées peuvent réduire de manière significative la fragmentation actuelle et renforcer la protection des données dans toute l'Europe.

Le groupe de travail salue en particulier l'introduction de dispositions qui encouragent les responsables du traitement à se mobiliser, dès le début, pour une protection correcte des données (au moyen, notamment, d'analyses d'impact relatives à la protection des données, d'une protection des données dès la conception et d'une protection des données par défaut). Les propositions attribuent clairement aux entités chargées du traitement des données à caractère personnel une responsabilité et une obligation de rendre compte, tout au long du cycle de vie de ces informations.

Le groupe de travail souligne l'importance des dispositions visant à clarifier et renforcer les droits des personnes concernées, notamment par la clarification de la notion de consentement, l'introduction d'un principe général de transparence et de mécanismes de recours améliorés. De même, le groupe

de travail salue vivement l'instauration d'une obligation de notification des violations de données, qui assure une cohérence dans tous les secteurs.

Le groupe de travail se félicite également du fait que les propositions harmonisent les pouvoirs et compétences des autorités de contrôle afin qu'elles garantissent de manière plus efficace le respect des dispositions, et au besoin imposent ce respect, tant sur un plan individuel qu'en coopération les unes avec les autres, par exemple en ayant la capacité d'infliger des amendes importantes.

En dépit de sa position globalement positive à l'égard de la proposition de règlement, le groupe de travail estime que certaines de ses parties ont besoin d'être clarifiées et améliorées. En ce qui concerne la directive relative à la protection des données dans le domaine de la police et de la justice, le groupe de travail est déçu par le degré d'ambition de la Commission et souligne le besoin de dispositions plus fortes.

Le groupe de travail a examiné avec soin les deux propositions et livre, avec le présent avis, sa première réaction générale à leur égard. L'avis attire l'attention sur des domaines de préoccupation et, selon le cas, propose des améliorations. Au besoin, le groupe de travail pourra formuler à l'avenir d'autres avis sur des dispositions ou des aspects particuliers des propositions.

Le groupe de travail prie le Conseil et les membres du Parlement européen de saisir la possibilité qui leur est offerte d'améliorer les deux propositions pour renforcer la protection des données à caractère personnel dans l'Union européenne.

Remarques générales

Le règlement répond à l'ambition de produire un texte rendant compte de l'importance accrue de la protection des données au sein de l'ordre juridique de l'UE (article 16 du traité, article 8 de la charte). Il conserve et renforce les principes fondamentaux de la protection des données, impose des obligations claires et uniformes aux responsables du traitement et aux soustraitants, favorise la libre circulation des données à caractère personnel et offre un cadre juridique renforcé pour que la législation soit appliquée de manière uniforme par les autorités chargées de la protection des données, dont les pouvoirs ont été consolidés.

Le groupe de travail regrette que les opinions qu'il a exprimées quant au caractère global n'aient pas donné lieu à un seul instrument juridique. Il relève

que la Commission a choisi de présenter une proposition distincte de directive applicable dans le domaine de la police et de la justice pénale, en raison de contraintes politiques. Il est donc d'autant plus nécessaire de disposer d'un niveau élevé de normes cohérentes en matière de protection des données, également applicables à ce domaine. En tout état de cause, il convient de préciser que la nouvelle directive ne doit pas amener les États membres à abaisser les normes de protection des données qu'ils appliquent actuellement au secteur de la police et de la justice pénale. De même, le nouveau cadre juridique doit être conforme aux autres accords internationaux, y compris la convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et son protocole additionnel. Le groupe de travail propose de mentionner clairement la convention 108 et son protocole additionnel dans le préambule du règlement et celui de la directive.

Dans de précédents avis, le groupe de travail a souligné la nécessité de parvenir à conférer un caractère global au cadre juridique. De ce point de vue, la directive est décevante en ce qu'elle manque d'ambition par rapport au règlement.

Le fait que deux instruments juridiques aient été présentés ne signifie pas nécessairement qu'un cadre juridique global n'est plus possible, dès lors que le but est le même (atteindre un niveau élevé et global de protection des données pour le citoyen européen) et que les instruments ont une approche commune à l'égard, entre autres, des principes de la protection des données, des droits des personnes concernées et des obligations qui incombent aux responsables du traitement et aux sous-traitants.

Des efforts considérables doivent être déployés par le législateur européen pendant la procédure législative pour rapprocher les dispositions de fond de la directive de celles du règlement et garantir la cohérence des deux textes.

En outre, les institutions de l'UE devraient être tenues par les mêmes règles que celles qui s'appliquent au niveau des États membres. Dès lors, pour que la réforme soit véritablement globale, lors de l'entrée en vigueur du règlement, le cadre pour la protection des données propre aux institutions de l'Union européenne, tel qu'il est actuellement prévu par le règlement n°45/2001, devra être aligné sur ce nouveau règlement.

Il en va de même pour les règles spécifiques applicables au traitement des données dans le cadre de l'ancien troisième pilier de l'UE, par exemple relativement aux agences européennes comme Europol et Eurojust. Le groupe de travail prend note des difficultés pratiques susceptibles de faire obstacle à toute proposition de remaniement général de l'acquis actuel, mais estime dans le même temps que le même niveau de protection des données devrait en aux organes de l'UE.

Ceci dit, le groupe de travail prend note du fait que la Commission s'est engagée à réexaminer dans un délai de trois ans d'autres instruments juridiques afin de déterminer si leur adaptation est nécessaire. Le groupe de travail recommande au législateur de fixer un délai beaucoup plus strict et demande à la Commission d'effectivement présenter ces propositions. Dans le même temps, le groupe de travail reconnaît que les régimes actuels de protection des données applicables à certains instruments et organes existants sont plus ambitieux que la directive proposée. Comme mentionné pour les États membres se trouvant dans une situation semblable, l'alignement des régimes actuels sur la directive ne devrait en aucun cas signifier un abaissement de la norme actuelle en matière de protection des données.

Annexes

Dans un autre registre, le groupe de travail regrette que ni le règlement ni la directive n'abordent la question de la collecte et du transfert par des entités privées ou des autorités publiques non répressives de données en fait destinées à des fins répressives, ainsi que l'utilisation ultérieure de ces données par les autorités répressives. Plusieurs exemples survenus au cours des dix dernières années (données des dossiers passagers (PNR), rétention des données de télécommunications) ont fait clairement ressortir que des conditions strictes sont nécessaires, en particulier lorsque le traitement se fait sur une base structurelle. Il en va de même dans l'autre sens: des règles sont également nécessaires pour garantir la protection des données lorsque des informations sont transférées par les autorités répressives ou d'autres autorités «compétentes» au secteur privé ou à d'autres autorités publiques.

Enfin, en ce qui concerne les deux instruments proposés, le groupe de travail constate avec préoccupation l'étendue du pouvoir conféré à la Commission pour adopter des actes délégués et des actes d'exécution. Tout en reconnaissant qu'il est nécessaire de veiller à ce que certaines questions puissent, à un stade ultérieur, être traitées de manière plus précise, le groupe de travail estime que cela ne vaut pas, par exemple, pour les règles relatives à la notification des violations de données. Afin de garantir la sécurité juridique, il convient d'insérer les éléments essentiels dans le règlement lui-même, comme le prévoit l'article 290 du TFUE.

<u>En ce qui concerne le règlement</u>

<u>Aspects positifs</u>

- D'une manière générale, le règlement apporte davantage de clarté par des définitions plus précises et des dispositions destinées à garantir une application plus harmonisée de la législation, facilitant ainsi la libre circulation des données.
- En ce qui concerne les personnes, le règlement renforce leurs droits, y compris par une transparence accrue, un plus grand contrôle du traitement, la minimisation des données, des dispositions particulières pour le traitement des données à caractère personnel concernant des enfants, un droit d'accès aux données renforcé, un droit d'opposition renforcé, le droit à la portabilité des données, un droit à la suppression des données renforcé («droit à l'oubli numérique») et un droit renforcé de recours devant les autorités chargées de la protection des données et devant les cours et tribunaux.

- En ce qui concerne les responsables du traitement, le règlement apporte une simplification et une plus grande cohérence, un recentrage sur leur responsabilité à l'égard des données traitées et la nécessité de prouver cette responsabilisation par une protection des données dès la conception, une protection des données par défaut, des analyses d'impact sur le respect de la vie privée, la désignation d'un délégué à la protection des données, des obligations liées à la notification des violations de données et l'adoption de mesures de précaution à l'égard des transferts internationaux. En outre, les règles d'entreprise contraignantes sont expressément reconnues comme un outil permettant d'encadrer les transferts internationaux.
- En ce qui concerne les sous-traitants, les obligations en matière de sécurité des données sont juridiquement fondées, et une obligation a été introduite pour que le sous-traitant endosse la responsabilité du responsable du traitement à l'égard d'une opération spécifique de traitement de données au cas où il outrepasserait les instructions du responsable du traitement à propos de ladite opération de traitement (cela présente de l'intérêt pour les prestataires « cloud »).
- En ce qui concerne les autorités chargées de la protection des données, le règlement prévoit une indépendance et des pouvoirs renforcés, y compris des amendes administratives et l'obligation de consulter ces autorités à propos des mesures législatives, et il comprend des dispositions visant à garantir une application harmonisée de la législation et, au besoin, son application forcée, en particulier au moyen du « mécanisme de contrôle de la cohérence ».

Rôle de la Commission

Le groupe de travail émet de sérieuses réserves à l'égard de l'étendue du pouvoir conféré à la Commission pour adopter des actes délégués et des actes d'exécution, ce qui est tout particulièrement pertinent au vu du fait qu'il est question d'un droit fondamental. Naturellement, il peut être nécessaire de laisser certaines questions à des actes délégués et/ou d'exécution. Toutefois, toutes les questions mentionnées à l'article 86 et à l'article 87 ne constituent pas des points de détail. Certaines dispositions du règlement (par exemple, sur la notification des violations de données, l'assistance mutuelle, la cohérence et la dérogation au droit d'information et d'accès dans le cadre d'un traitement à des fins historiques, statistiques et scientifiques) ne peuvent être appliquées sans que l'acte délégué ou d'exécution soit en vigueur. De plus, d'autres actes délégués concernent le champ d'application matériel du règlement, par exemple l'article 6, paragraphe 1, point f), lu conjointement avec l'article 6, paragraphe 5, qui permet à la Commission de définir les « intérêts légitimes » du responsable du traitement dans des situations particulières de traitement et des secteurs donnés. Afin de garantir la sécurité juridique, il faut insérer les éléments essentiels dans le règlement luimême, comme le prévoit l'article 290 du TFUE.

Dans la pratique, l'adoption d'actes délégués ou d'actes d'exécution pour un grand nombre d'articles peut prendre plusieurs années et pourrait représenter une insécurité juridique pour les responsables du traitement et les sous-traitants qui espèrent une mise en oeuvre rapide et obtenir des lignes directrices concrètes à bref délai. Le groupe de travail prie la Commission d'indiquer à tout le moins quels sont les actes délégués et d'exécution qu'elle compte adopter à court, moyen et long terme.

En dépit du rôle de gardienne des traités dévolu à la

Commission, le groupe de travail émet également de sérieuses réserves quant au rôle attribué à la Commission dans les cas particuliers examinés dans le cadre du mécanisme de contrôle de la cohérence, puisqu'il empiète sur l'indépendance des autorités chargées de la protection des données. Lorsqu'une question est examinée ou a été examinée par le comité européen de la protection des données dans le cadre du mécanisme de contrôle de la cohérence, la Commission devrait être en mesure de donner son appréciation juridique tout en s'abstenant en principe d'intervenir. Une procédure pourrait être envisagée pour permettre à la Commission et au comité européen de la protection des données de demander à la Cour de justice de l'Union européenne d'émettre un avis sur l'interprétation du règlement.

Rôle des autorités européennes chargées de la protection des données dans l'élaboration des politiques

Le groupe de travail estime que les propositions devraient refléter le rôle important qu'il a lui-même joué jusqu'à présent et celui que le comité européen de la protection des données est susceptible de jouer dans le futur en termes d'élaboration des politiques (par exemple, en formulant des lignes directrices ou des recommandations).

A l'article 66, il est prévu que le comité européen de la protection des données, de sa propre initiative ou à la demande de la Commission, a pour mission de conseiller sur toute question relative à la protection des données à caractère personnel et d'examiner toute question portant sur l'application du règlement. Le groupe de travail entend cette disposition comme incluant également d'autres instruments législatifs et suggère dès lors d'ajouter à l'article 66, paragraphe 1, point a), « […] ainsi que sur toute mesure additionnelle ou particulière visant à garantir les droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel et sur toute autre proposition de mesure de l'Union affectant lesdits droits et libertés ».

De plus, le groupe de travail suggère d'introduire la possibilité pour la Commission européenne mais aussi pour le Parlement européen de solliciter l'avis du comité européen de la protection des données en ajoutant les termes « et du Parlement européen » à l'article 66, paragraphe 1, point b).

En outre, le groupe de travail suggère vivement d'inclure l'obligation pour la Commission

de toujours consulter le comité européen de la protection des données au sujet des décisions relatives au caractère adéquat du niveau de protection (article 41) et des clauses types de protection des données (article 42), et de consulter et obtenir l'approbation dudit comité au sujet des codes de conduite au niveau européen (article 38). En tout état de cause, il convient d'insérer une obligation faite à la Commission de consulter le comité européen de la protection des données au sujet de tous les actes délégués et d'exécution (articles 86 et 87).

Les autorités nationales devraient continuer à pouvoir formuler des lignes directrices et des recommandations devant être soumises au mécanisme de contrôle de la cohérence si celles-ci risquent d'avoir une incidence importante sur d'autres États membres. Elles devraient également pouvoir contrôler l'élaboration des marques et labels de certification destinés à protéger les personnes.

Seuils pour les PME

Le groupe de travail relève que tout au long de la proposition de règlement, des exceptions et seuils sont introduits dans le but de limiter les charges administratives des micro, petites et moyennes entreprises et d'atténuer les conséquences pour celles-ci. Des seuils sont introduits dans les dispositions concernant l'obligation de désigner un représentant dans l'UE (article 25), la documentation (article 28, paragraphe 4), la désignation d'un délégué à la protection des données (article 35, paragraphe 1) et les amendes administratives (articles 79, paragraphe 3). De surcroît, la proposition prévoit des actes délégués et d'exécution autorisant la Commission à prendre d'autres mesures pour les micro, petites et moyennes entreprises à l'article 12, paragraphe 6, sur les procédures et mécanismes prévus pour l'exercice des droits de la personne concernée, à l'article 14, paragraphe 7, sur l'obligation d'informer la personne concernée, à l'article 22, paragraphe 4, sur les obligations de rendre compte et à l'article 33, paragraphe 6, sur les analyses d'impact relatives à la protection des données.

Le groupe de travail est d'avis que les personnes concernées devraient bénéficier du même niveau de protection, que leurs données soient traitées par une micro, petite, moyenne entreprise ou une grande entreprise. Toutefois, il reconnaît que certaines des obligations envisagées pourraient être pesantes pour les micro, moyennes et petites entreprises. Dès lors, si le groupe de travail comprend le principe qui justifie d'introduire ces seuils, il craint que ces exceptions n'aboutissent, dans la pratique comme en ce qui concerne la protection des données à caractère personnel, à des effets incohérents et des résultats non souhaitables. Le groupe de travail estime qu'un seuil tenant compte de la nature et de l'étendue du traitement des données serait plus approprié.

Incidences sur le budget et les ressources

Le groupe de travail se réjouit de ce que les propositions reconnaissent le rôle important susceptible d'être joué par les autorités chargées de la protection des données pour assurer le respect de l'instrument, en attribuant des fonctions renforcées à la fois à ces autorités et au comité européen de la protection des données. Le groupe de travail doute toutefois sérieusement que l'incidence budgétaire considérable de ces fonctions renforcées soit suffisamment reconnue. Pour permettre aux autorités chargées de la protection des données et au comité européen de la protection des données de s'acquitter efficacement de leurs fonctions, y compris en termes d'assistance mutuelle et de coopération au sein du mécanisme de contrôle de la cohérence, les Etats membres doivent s'engager à fournir les ressources financières, humaines et techniques nécessaires.

A cet égard, le groupe de travail suggère vivement qu'une évaluation approfondie indépendante soit réalisée concernant les coûts supplémentaires que cela représente pour les autorités chargées de la protection des données et le contrôleur européen de la protection des données (en tant que secrétariat du comité européen de la protection des données), sur la base des propositions actuelles. Eu égard aux résultats de cette évaluation, il conviendrait de préciser ce que constituent pour les autorités chargées de la protection des données les « ressources humaines, techniques et financières appropriées, ainsi que [les] locaux et [...] l'infrastructure » mentionnés à l'article 47, paragraphe 5.

Le groupe de travail compte adresser un courrier séparé à la Commission au sujet de la finalité et des paramètres d'une analyse d'impact de ce type.

Dispositions générales

Champ d'application

Conformément à l'article 3, paragraphe 2, le règlement s'applique également au traitement des données à caractère personnel relatives à des personnes concernées ayant leur résidence sur le territoire de l'Union, par un responsable du traitement qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes concernées dans l'Union ou à l'observation de leur comportement.

En dépit des tentatives de définition des expressions « offre de biens et de services » et « observation de leur comportement » dans les considérants, le groupe de travail estime qu'il serait utile de clarifier davantage ces notions.

Il devrait être précisé que l'« offre de biens et de services » comprend également les services gratuits (dans le cadre desquels les personnes paient en fait le service en fournissant leurs données à caractère personnel). Le groupe de travail propose dès lors d'ajouter une formule du genre « y compris des services fournis sans qu'aucune contrepartie financière ne soit exigée de la personne ».

En outre, le considérant 21 laisse entendre que l'« observation [du] comportement » est liée à un suivi sur l'internet et à la création de profils. Le groupe de travail recommande de modifier le libellé afin de garantir que même si le responsable du traitement ne crée pas de profils en tant que tels, les activités de traitement puissent parfois être considérées comme une « observation du

comportement » si elles donnent lieu à des décisions à propos d'une personne concernée ou impliquent d'analyser ou de prévoir ses préférences personnelles, ses comportements et ses attitudes.

Personne concernée et données à caractère personnel

Le groupe de travail salue la définition de la « personne concernée » donnée à l'article 4, point 1, de la proposition de règlement, qui dispose: « "personne concernée": une personne physique identifiée ou une personne physique qui peut être identifiée […] ».
On peut considérer qu'une personne physique est identifiable lorsque, au sein d'un groupe de personnes, elle peut être distinguée des autres membres du groupe et, par conséquent, être traitée différemment. C'est ce qui a été exposé dans l'avis sur le concept de données à caractère personnel précédemment adopté par le groupe de travail (WP 136). Il convient donc de modifier le considérant 23 afin de préciser que la notion de caractère identifiable comprend également le fait d'être distinguable de cette manière.

Le considérant 24 relatif à la définition des données à caractère personnel prévoit que les numéros d'identification, données de localisation, identifiants en ligne ou autres éléments spécifiques ne doivent pas nécessairement être considérés comme des données à caractère personnel dans tous les cas de figure. Telle qu'elle est rédigée actuellement, la dernière phrase pourrait donner lieu à une interprétation indûment restrictive de la notion de données à caractère personnel en ce qui concerne, par exemple, les adresses IP ou les témoins de connexion (« cookies »).
Le groupe de travail rappelle que les données à caractère personnel sont des données concernant une personne identifiable. « Les données concernent une personne si elles ont trait à l'identité, aux caractéristiques ou au comportement d'une personne ou si cette information est utilisée pour déterminer ou influencer la façon dont cette personne est traitée ou évaluée »[23]. Le groupe de travail a déjà présenté, dans l'avis WP 136, différents scénarios qui justifieraient de considérer que les adresses IP se rapportent à des personnes identifiables, « notamment […] lorsque le traitement d'adresses IP [a] été effectué pour identifier les utilisateurs de l'ordinateur (par exemple, par des titulaires de droits d'auteur afin de poursuivre ces utilisateurs d'ordinateurs pour violation de droits de la propriété intellectuelle) […] ». Dans ce cas, de même que dans celui des cookies, le responsable du traitement part du principe que des «moyens susceptibles d'être raisonnablement mis en oeuvre» seront disponibles pour identifier les personnes et les traiter d'une manière particulière[24]. Dès lors, le groupe de travail suggère de modifier en conséquence le considérant 24.

Données biométriques

Le groupe de travail salue l'introduction d'une définition des données biométriques à l'article 4, point 11, du règlement. Néanmoins, il émet des réserves quant au libellé actuel, qui s'attache au fait de permettre l'identification unique d'une personne. Les données biométriques ne sont pas uniquement utilisées à des fins d'identification, mais également dans un but d'authentification (pour vérifier l'identité d'une personne sans en fait identifier la personne elle-même). Il conviendrait de modifier la définition pour l'axer sur les types de données qui doivent être considérées comme des données biométriques plutôt que sur ce que ces données permettent de faire. Le groupe de travail suggère dès lors de modifier le libellé de l'article 4, point 11, en remplaçant « […] permettent son identification unique […] » par « […] sont uniques pour chaque personne en particulier […] ».

[23] WP 136, p. 10.
[24] WP 136, p. 16.

7 Annexes

Etablissement principal

Il faut davantage clarifier la manière dont il est décidé du lieu où une entreprise multinationale (que ses propriétaires soient établis ou non dans l'UE) a son établissement principal, tel que ce terme est défini à l'article 4, point 13, et au considérant 27, y compris lorsqu'elle comprend des entités juridiques distinctes actives dans différents secteurs. A titre d'exemple, il pourrait être tenu compte de l'« influence dominante » exercée par un établissement sur les opérations de traitement en ce qui concerne l'application des règles relatives à la protection des données à caractère personnel.

Le groupe de travail relève que la proposition de règlement comporte, à l'article 4, différentes définitions d'entités économiques, qui ne sont pas clairement distinctes les unes des autres. Les notions de « responsable du traitement » et d'« établissement principal », d'une part, renvoient au lieu où sont prises les décisions importantes concernant le traitement des données, tandis que les définitions d'« entreprise » et de « groupe d'entreprises », d'autre part, parlent de l'activité économique et de la structure de l'entreprise.

Un terme supplémentaire est introduit en ce qui concerne les sous-traitants dont l'établissement principal est censé être le lieu de leur « administration centrale ». En outre, le chapitre VIII sur les recours, la responsabilité et les sanctions mentionne un établissement, quel qu'il soit, lorsqu'il s'agit de déterminer la juridiction compétente pour intenter une action contre un responsable du traitement ou un sous-traitant, indépendamment du fait que ledit établissement ait un lien quelconque avec le traitement en question (il pourrait en effet être, d'un point de vue juridique, complètement indépendant des autres établissements du responsable du traitement/sous-traitant établis dans l'UE).

De l'avis du groupe de travail, ces définitions se chevauchent et devraient dès lors faire l'objet d'une clarification. En tout état de cause, il conviendrait de préciser quel est le lien entre l'établissement principal et les responsabilités du responsable du traitement.

La définition de l'établissement principal semble essentiellement destinée à déterminer quelle est l'autorité nationale chargée de la protection des données qui doit être l'autorité chef de file dans un cas particulier ou pour une entreprise donnée. Il est essentiel que le terme « établissement principal » soit clairement compris, puisqu'il est décisif pour déterminer l'autorité

chef de file au sens de l'article 51, paragraphe 2, lorsque le traitement des données à caractère personnel a lieu dans le cadre des activités d'un responsable du traitement ou d'un sous-traitant établis dans l'Union, et lorsque le responsable du traitement ou le sous-traitant sont établis dans plusieurs États membres (voir page 30 pour de plus amples détails).

Pseudonymisation

Le groupe de travail estime que la notion de pseudonymisation devrait être introduite de manière plus explicite dans l'instrument (par exemple, en intégrant une définition des données pseudonymisées, cohérente avec la définition des données à caractère personnel), car elle peut permettre d'accéder à une meilleure protection des données, comme dans le cadre de la protection des données dès la conception et de la protection des données par défaut. Le groupe de travail suggère dès lors d'instaurer une obligation générale d'anonymisation ou de pseudonymisation des données à caractère personnel dans la mesure de ce qui est possible et proportionné par rapport à la finalité du traitement. Ce principe pourrait être introduit à l'article 5 et, dans le cadre de la protection des données dès la conception et par défaut, à l'article 23.

Protection des données dès la conception et protection des données par défaut

Le groupe de travail salue l'introduction à l'article 23 de la protection des données dès la conception et de la protection des données par défaut, mais recommande de clarifier le sens de ces notions dans un considérant, par exemple, en indiquant que les fonctions respectueuses de la vie privée devraient être automatiquement activées sur les biens et services et que des procédures adéquates devraient être mises en oeuvre pendant la conception du traitement des données ou du produit. Naturellement, il appartient au responsable du traitement de prouver que ses activités de traitement tiennent compte des notions de protection des données dès la conception et de protection des données par défaut, qui constituent des mesures appropriées au sens de l'article 22, paragraphe 1.

Le groupe de travail note que la Commission est habilitée à définir des normes techniques en la matière. Le groupe de travail est convaincu que la Commission devrait associer le comité européen de la protection des données et des organismes de normalisation internationaux à l'élaboration de ces normes techniques, et le cas échéant les consulter.

Le principe du droit d'accès du public aux informations

Le considérant 18 prévoit que le règlement permet de prendre en compte, dans la mise en oeuvre de ses dispositions, le principe du droit d'accès du public aux documents administratifs. Ce principe constituant de longue date un droit fondamental important, il devrait être mentionné dans un considérant, mais également exprimé dans un article du règlement.

Utilisation ultérieure incompatible

L'article 6, paragraphe 4, introduit la possibilité d'un traitement ultérieur des données à des fins non compatibles lorsque ledit traitement peut trouver une autre base juridique (à l'exception de l'intérêt légitime du responsable du traitement). Si le groupe de travail ne conteste pas la nécessité de laisser ouverte la possibilité d'un traitement ultérieur des données à d'autres fins, la disposition telle qu'elle est actuellement proposée crée les conditions d'une utilisation ultérieure des données à des fins non compatibles qui pourraient, dans le secteur tant public que privé, en particulier si elles se fondent sur les points b) (exécution d'un contrat) et e) (intérêt général), donner lieu à des résultats extrêmement peu souhaitables. De l'avis du groupe de travail, cette disposition va à

Annexes

l'encontre du principe général de limitation de la finalité, l'une des notions clés de la protection des données en Europe, et suggère donc vivement soit de supprimer l'article 6, paragraphe 4, soit de le reformuler, d'une manière plus précise avec un renvoi à l'article 21. Dans ce contexte, le groupe de travail souhaite également attirer l'attention sur le fait qu'il abordera la question de l'utilisation compatible de manière plus substantielle dans un avis distinct dans le courant de 2012, comme indiqué dans son programme de travail pour 2012-2013.

Exceptions introduites pour les autorités publiques

L'une des raisons qui motivent la révision du cadre régissant la protection des données est de garantir son caractère global. En offrant un ensemble unique de règles applicables tant par le secteur public que privé, le cadre juridique devrait améliorer la sécurité juridique à l'égard des garanties offertes en matière de protection des données dans les différents secteurs, en particulier pour les personnes physiques.

Le groupe de travail a déjà fait part de sa déception quant au manque d'ambition dans le domaine de la police et de la justice. Toutefois, dans le règlement lui-même, une position particulière est également accordée au secteur public. Le groupe de travail s'inquiète du fait qu'en plusieurs endroits du règlement, de larges exceptions en faveur des autorités publiques soient introduites pour des motifs d'intérêt général. Le groupe de travail estime que des exceptions larges et indéterminées, qui ne présentent pas non plus les garanties adéquates pour la protection des personnes, ne sont pas justifiées. Dès lors, il suggère de définir autant que possible dans le règlement les intérêts généraux spécifiques. Cela contribuerait également à une harmonisation au sein de l'UE.

Comme mentionné ci-dessus, l'article 6, paragraphe 4, introduit pour les autorités publiques également la très large possibilité de remplacer la finalité initiale du traitement par des finalités non compatibles. En outre, l'article 9, paragraphe 2, point g), permet le traitement de données sensibles pour des missions effectuées « dans l'intérêt général ». Il en va de même pour les exceptions formulées à l'article 17, paragraphe 5, en particulier en ce qui concerne l'intérêt général et les intérêts de tiers. Le groupe de travail recommande de limiter cette exception selon les termes suivants: « […] pour des motifs d'intérêt général important ».

En outre, l'article 21 prévoit la possibilité de limiter les principes

de protection des données et les droits des personnes concernées, élargissant ainsi les possibilités de limitation par rapport à la situation actuelle, sans prévoir les garanties adéquates à respecter lorsque l'article est invoqué. De plus, l'article 21, paragraphe 1, point c), peut être invoqué pour sauvegarder une catégorie ouverte d'« autres intérêts généraux ». Le groupe de travail juge ces possibilités trop vastes et suggère donc vivement de supprimer les termes « sauvegarder d'autres intérêts généraux de l'Union ou d'un État membre [...] » de l'article 21, paragraphe 1, point c), et de commencer par « [...] un intérêt économique ou financier important [...] ».

L'article 33, paragraphe 5, introduit pour les autorités publiques une dérogation à l'obligation d'effectuer des analyses d'impact relatives à la protection des données lorsque le traitement est effectué en exécution d'une obligation légale. Le groupe de travail est d'avis que la seule dérogation qui pourrait être justifiée dans ce contexte serait le cas dans lequel une analyse d'impact relative à la protection des données aurait déjà été effectuée dans le cadre de la procédure législative.

Le groupe de travail est convaincu que des exceptions générales pour le secteur public ne sont pas justifiées et qu'elles portent préjudice au caractère global du cadre juridique; il recommande vivement que, dans la mesure du possible, les secteurs public et privé soient traités de la même manière et tenus de respecter le même ensemble de règles de base. Toutefois, il faut également empêcher que le nouveau cadre juridique puisse entraîner un affaiblissement du niveau de protection des données déjà atteint dans différents domaines dans les Etats membres. Dans le secteur public en particulier, le niveau de protection des données varie du fait des pratiques et évolutions constitutionnelles et juridiques. Le nouveau cadre juridique devrait dès lors prévoir un niveau élevé et harmonisé de normes dans ce domaine, tout en offrant aux Etats membres la possibilité d'apporter d'autres précisions (comme le prévoit déjà le chapitre IX), mais sans préjudice du règlement. Cela signifie également qu'elles pourraient compléter le règlement.

Mineurs

Le groupe de travail reconnaît l'importance du principe de l'« intérêt supérieur de l'enfant » et de la notion de protection progressive en fonction du degré de maturité[25]. Bien que le règlement n'affecte pas les dispositions régissant la validité, la formation ou les effets d'un contrat à l'égard d'un enfant figurant dans la législation générale des Etats membres en matière contractuelle, le groupe de travail salue le fait que l'article 8, paragraphe 1, prévoie que, s'agissant de l'offre directe de services de la société de l'information aux enfants, le traitement des données à caractère personnel relatives à un enfant de moins de 13 ans n'est licite que si et dans la mesure où le consentement est donné ou autorisé par un parent de l'enfant ou par une personne qui en a la garde.

Le groupe de travail est attentif aux contraintes relatives à l'harmonisation des limites d'âge dans un tel instrument et comprend que dans des situations purement nationales, le droit des États membres devrait s'appliquer. Toutefois, le groupe de travail suggère d'élargir à des domaines autres que l'offre de services de la société de l'information la portée de la norme minimale introduite dans le règlement en ce qui concerne la manière dont sont traités les mineurs, puisqu'il existe davantage de situations dans lesquelles des règles spécifiques pourraient être envisagées.

D'une manière générale, le règlement manque de dispositions relatives à la manière dont des droits peuvent

[25] Voir l'avis 2/2009 sur la protection des données à caractère personnel de l'enfant (WP 160) et le document de travail 1/2008 sur la protection des données à caractère personnel de l'enfant (WP 147).

être exercés par le biais d'une représentation par des avocats, non seulement dans le cas des mineurs mais également des personnes incapables.

Droit à l'oubli numérique

Le groupe de travail salue l'inclusion spécifique dans le règlement du droit à l'oubli numérique et à l'effacement en tant que moyen permettant de renforcer le contrôle exercé par les personnes sur leurs propres données à caractère personnel. Toutefois, la façon dont ces droits sont configurés par le règlement et la manière dont l'internet fonctionne dans la réalité pourraient considérablement limiter leur efficacité.
Le responsable du traitement est chargé, non seulement, d'effacer les données mais également d'informer de la demande de la personne concernée les tiers qui traitent ces données par le biais de liens vers celles-ci, de copies ou de reproductions de celles-ci. Le fait de faire porter cette obligation au seul responsable du traitement comporte des limites, puisqu'il peut y avoir des situations dans lesquelles le responsable du traitement a pris toutes les mesures raisonnables pour informer les tiers, mais n'a pas connaissance de toutes les copies ou reproductions existantes ou des nouvelles copies ou reproductions qui apparaissent après qu'il a informé tous les tiers connus. Mais surtout, aucune disposition du règlement ne semble obliger les tiers à respecter la demande formulée par la personne concernée, à moins que ces tiers ne soient également considérés comme responsables du traitement.

Le règlement n'indique aucunement comment les personnes concernées peuvent exercer leurs droits si le responsable du traitement n'existe plus, a disparu ou ne peut être identifié ou contacté. Dès lors, la position des tiers qui traitent des données devrait être clarifiée afin de définir dans quelles conditions et à quel titre ils doivent exécuter la demande de la personne concernée, et quelles sont les conséquences s'ils ne le font pas.

De la même façon, on pourrait envisager d'élargir le droit des personnes concernées pour leur permettre d'adresser leur demande d'effacement directement aux tiers dans le cas où cela ne peut être fait par le biais du responsable du traitement.

Pour finir, aucun mécanisme ne prévoit la suppression des copies ou reproductions des données ou des liens vers les données qui ne sont pas effacées conformément à l'article 17, paragraphe 3, mais qui, en soi, ne relèvent pas des motifs exposés dans l'article. Or ces liens, copies ou

reproductions peuvent faciliter l'accès au contenu d'origine, alors que cela ne se justifie pas forcément en vertu dudit article. Naturellement, le groupe de travail reconnaît la nécessité de trouver le juste équilibre entre les droits relatifs au respect de la vie privée et le droit à la liberté d'expression. Il conviendrait que le règlement clarifie la relation entre l'article 17, paragraphe 3, et l'obligation formulée à l'article 17, paragraphe 2.

Marketing direct

Nonobstant l'article 19, paragraphe 2, du règlement qui prévoit un droit d'opposition au traitement des données en vue d'un marketing direct, le groupe de travail souligne que les dispositions de la directive 2002/58/CE demeurent pleinement applicables, comme le prévoit également l'article 89 du règlement. Cela s'applique tout spécialement dans le contexte de la publicité comportementale en ligne et du marketing par courrier électronique, pour lesquels un consentement est prévu.

Profilage

Le groupe de travail soutient la disposition du règlement qui traite du profilage. Toutefois, il a des doutes quant au fait que l'approche adoptée puisse être suffisante pour tenir compte des questions de création et d'utilisation de profils, en particulier dans l'environnement en ligne.

De plus, le groupe de travail relève que les termes « l'affectant de manière significative » employés à l'article 20, paragraphe 1, sont imprécis. Il conviendrait de préciser qu'il couvre également l'utilisation, par exemple, d'outils d'analyse web, le suivi pour évaluer le comportement de l'utilisateur, la création de profils de déplacement par les applications mobiles, ou la création de profils personnels par les réseaux sociaux.

En outre, la disposition ne devrait pas être limitée au traitement exclusivement automatisé mais également couvrir les méthodes de traitement partiellement automatisé. De l'avis du groupe de travail, il faudrait aborder la question en définissant clairement les fins auxquelles des profils sont susceptibles d'être créés et utilisés, y compris l'obligation spécifique incombant aux responsables du traitement d'informer la personne concernée, en particulier de son droit d'opposition à la création et utilisation de profils.

Représentant

Le groupe de travail estime que le rôle et les obligations du représentant tel qu'ils sont définis à l'article 25 devraient être davantage clarifiés. Il conviendrait de préciser quel est le rôle du représentant à l'égard des personnes concernées, des juridictions et des autorités chargées de la protection des données, en particulier au vu du fait que l'article 79, paragraphe 6, point f), prévoit l'amende la plus élevée possible en cas de non-désignation d'un représentant. Le mandat du représentant devrait être spécifié afin de définir clairement l'étendue de sa mission, son rôle et sa responsabilité.

L'article 78, paragraphe 2, prévoit que lorsque le responsable du traitement a désigné un représentant, les sanctions sont appliquées au représentant. Il conviendrait d'apporter la même clarté dans le cas des sanctions administratives prévues à l'article 79. Les termes « devrait pouvoir être contacté par toute autorité de contrôle » et « peut être contactée à sa place par les autorités de contrôle » utilisés au considérant 63 et à l'article 4, paragraphe 14, ne sont pas suffisamment précis quant au fait qu'un représentant peut également être le destinataire d'une sanction administrative au sens de l'article 79.

Il devrait également être bien clair que l'établissement d'un

représentant dans l'UE, tel que visé à l'article 25, paragraphe 3 (« est établi dans l'un des États membres ») ne déclenche pas le mécanisme relatif à l'établissement principal défini à l'article 4, paragraphe 13, au sens où il ne joue pas un rôle décisif dans la détermination d'une autorité chef de file chargée de la protection des données conformément à l'article 51, paragraphe 2.

En ce qui concerne les dérogations à l'obligation de désignation d'un représentant, le groupe de travail ne voit aucune raison importante d'exclure un responsable du traitement établi dans un pays tiers qui offre un niveau de protection adéquat. Le fait qu'un pays tiers présente un niveau de protection adéquat ne modifie en rien la nécessité d'avoir un point de contact dans l'Union européenne, et le groupe de travail suggère dès lors de supprimer l'article 25, paragraphe 2, point a).

S'il y a lieu de prévoir des dérogations à l'obligation de désignation d'un représentant, celles-ci devraient se baser sur la nature et l'étendue du traitement des données à caractère personnel, ainsi que sur le nombre (potentiel) de personnes concernées affectées dans l'UE. Le seuil actuel concernant le nombre de personnes employées par le responsable du traitement risque d'exclure des entités de petite taille dont les activités de traitement représentent un risque pour les particuliers. De même, en dépit de l'explication donnée au considérant 64, la formulation « n'offrant qu'occasionnellement des biens ou des services à des personnes concernées » est trop vague et pourrait, dans la pratique, trop souvent donner lieu à une interprétation erronée.

Responsabilité

Le groupe de travail accueille très favorablement l'introduction du principe de responsabilité dans le règlement, en particulier à l'article 22, et souscrit pleinement à l'objectif de mettre en place des procédures et mécanismes efficaces ciblant les traitements susceptibles de présenter des risques particuliers pour les droits et libertés des personnes concernées. Néanmoins, le groupe de travail émet quelques doutes quant aux articles qui visent à préciser le principe général.

Tout d'abord, il faut veiller à la modularité. Dans la mise en oeuvre du principe de responsabilité, il devrait être possible de tenir compte de la taille du responsable du traitement et de la nature des activités de traitement. En outre, les autorités de contrôle devraient pouvoir tenir compte des mécanismes de responsabilité mis en oeuvre

lorsqu'elles infligent des sanctions et amendes.

De plus, l'article 28 prévoit l'obligation pour le responsable du traitement de conserver une trace documentaire de tous les traitements effectués sous sa responsabilité. L'article 28, paragraphe 2, précise le type de documentation spécifique que cela implique. Cette obligation s'articule avec les obligations générales de responsabilité énoncées à l'article 22, en vertu duquel les responsables du traitement sont tenus d'être à même de démontrer quelles sont les règles internes adoptées et les mesures mises en oeuvre pour garantir le respect du règlement. En principe, chaque responsable du traitement, chaque sous-traitant et, le cas échéant, le représentant du responsable du traitement devraient être tenus de conserver la documentation principale relative à leurs activités de traitement de données.

Si le groupe de travail salue l'obligation d'effectuer une analyse d'impact relative à la protection des données, comme le prévoit l'article 33, il estime que cette analyse devrait naturellement être aussi réalisée lorsque l'on ne peut savoir avec certitude si le traitement est susceptible de présenter des risques particuliers pour les droits et libertés des personnes concernées. Dès lors, le groupe de travail suggère d'aligner l'article 33, paragraphe 1, sur le considérant 70 et propose d'ajouter « sont susceptibles de », de manière à ce que la première phrase de l'article soit libellée ainsi: « Lorsque les traitements sont susceptibles de présenter des risques particuliers [...] ».

Le groupe de travail estime que les dérogations prévues à l'article 28, paragraphe 4, point b), sur la documentation et l'article 35, paragraphe 1, point b), sur la désignation des délégués à la protection des données sont susceptibles d'avoir des conséquences non voulues, en particulier lorsqu'une entité de petite taille comptant moins de 250 salariés traite beaucoup de données à caractère personnel ou que le traitement est de nature risquée. De même, le libellé actuel a une incidence disproportionnée sur les entités de grande taille qui traitent un nombre limité de données à caractère personnel. Le groupe de travail estime qu'au lieu d'indiquer le nombre total de salariés d'une entreprise, il serait plus approprié de tenir compte de la nature et de l'étendue du traitement des données à caractère personnel, ainsi que du nombre de salariés directement associés au traitement des données à caractère personnel et/ou du nombre de personnes concernées.

Le groupe de travail estime que les traitements portant sur les catégories de données sensibles indiquées à l'article 9 du règlement devraient faire l'objet d'une analyse d'impact relative à la protection des données. Dès lors, tous les types de données sensibles devraient être repris à l'article 33, paragraphe 2, point b).

De plus, il conviendrait de supprimer la restriction introduite par l'expression « à grande échelle » en ce qui concerne les traitements mentionnés à l'article 33, paragraphe 2, points b), c) et d), car le groupe de travail estime qu'une analyse d'impact relative à la protection des données est requise pour les traitements de ce type, même à petite échelle.

Cela vaut tout particulièrement en ce qui concerne le traitement des données biométriques, qui, de l'avis du groupe de travail, devrait être considéré comme risqué dans certaines circonstances, et une analyse d'impact relative à la protection des données devrait dès lors être effectuée indépendamment d'un quelconque seuil prévu à l'article 33. De même, comme mentionné plus haut, la dérogation, à l'article 33, paragraphe 5, dispensant les autorités publiques d'effectuer une analyse d'impact n'est pas justifiée, à moins que ladite analyse n'ait déjà été

effectuée lors de la procédure législative.

Notification des violations de données

Le groupe de travail salue l'introduction de l'obligation de notification d'une violation de données à caractère personnel, qui assure une cohérence dans tous les secteurs. Néanmoins, le groupe de travail doute que l'obligation de notification puisse donner lieu à des résultats satisfaisants au vu de la manière dont elle est établie. La portée de l'obligation de notification à l'autorité de contrôle devrait notamment être davantage ciblée et limitée. Il faudrait éviter que les autorités de contrôle soient dérangées et surchargées par le traitement de notifications de violations mineures de données, risquant peu de porter atteinte aux droits des personnes concernées. En outre, il faut clarifier le rôle et les responsabilités des autorités chargées de la protection des données en cas de notification (et après celle-ci).

Le groupe de travail est attentif au fait que, dans certaines circonstances, il peut être impossible d'adresser une notification dans un délai de 24 heures. L'article 31, paragraphe 1, répond à cette question en offrant la possibilité d'adresser la notification plus de 24 heures après avoir eu connaissance de la violation. Il est néanmoins important de faire la notification en temps utile. Le groupe de travail propose donc d'adopter une approche en deux étapes, selon laquelle le responsable du traitement doit en principe adresser la notification de la violation dans un délai de 24 heures après en avoir eu connaissance. Si toutes les informations ne peuvent être fournies dans le délai de 24 heures, le responsable du traitement aura la possibilité de compléter la notification dans un second temps.

Il faut apporter de plus amples précisions en ce qui concerne le critère utilisé pour établir une violation de données à caractère personnel et les circonstances dans lesquelles une violation doit être notifiée à l'autorité chargée de la protection des données et aux personnes concernées visées par la violation (par exemple, s'il y a un risque de danger ou de préjudice concret pour les personnes concernées). Le groupe de travail estime que le comité européen de la protection des données devrait en tout état de cause être associé à la définition de ces critères et circonstances.

Pour prendre en compte les recommandations formulées par le groupe de travail et l'ENISA, le formulaire de notification devrait comporter une évaluation

de la gravité de la violation des données à caractère personnel, fondée sur des critères objectifs.

En ce qui concerne le rôle et le fonctionnement des autorités chargées de la protection des données

Indépendance

Le texte indique, dans sa version actuelle, que les membres des autorités chargées de la protection des données ne peuvent être nommés que par un parlement ou un gouvernement. Toutefois, le groupe de travail souhaite que les Etats membres puissent donner la possibilité à d'autres organes indépendants, comme le conseil de la magistrature, de nommer et/ou désigner eux aussi des membres des autorités chargées de la protection des données.

Pouvoirs

Outre la possibilité qui leur est offerte de mener des enquêtes, les autorités chargées de la protection des données devraient également avoir expressément la possibilité de réaliser des audits.

Budget

Pour que les autorités chargées de la protection des données exercent efficacement les fonctions et pouvoirs étendus qui leur incombent au titre du règlement, notamment ceux qu'elles doivent mettre en oeuvre dans le cadre de l'assistance mutuelle, de la coopération et de la participation au comité européen de la protection des données, le règlement prévoit que les Etats membres doivent veiller à ce que lesdites autorités disposent des ressources humaines, techniques et financières appropriées, ainsi que des locaux et de l'infrastructure nécessaires. Comme mentionné plus haut, le groupe de travail recommande vivement d'indiquer de manière plus concrète en quoi consiste un budget adéquat, par exemple après la réalisation d'une évaluation approfondie indépendante des coûts supplémentaires pour les autorités chargées de la protection des données, sur la base des propositions actuelles.

Un budget adéquat pourrait partir d'un montant fixe destiné à couvrir les fonctions de base que toutes les autorités doivent toutes assumer de la même manière, complété par un montant calculé à partir d'une formule tenant compte de la population d'un Etat membre et de son PIB. Il pourrait également y avoir un élément tenant compte du nombre de multinationales dont le siège est établi dans l'Etat membre concerné. L'un des considérants devrait expressément encourager les Etats membres à envisager diverses options de financement de l'autorité chargée de la protection des données, afin de garantir que soit remplie l'obligation d'allouer des ressources suffisantes à l'autorité.

Marge d'appréciation

Les autorités chargées de la protection des données devraient être autorisées à faire des choix pour être efficaces; elles devraient pouvoir définir leurs propres priorités et engager des actions de leur propre initiative, comme des enquêtes, en dépit de leurs obligations en matière de coopération, d'assistance mutuelle et de contrôle de la cohérence conformément au chapitre VII. Les autorités chargées de la protection des données devraient pouvoir allouer des ressources en fonction du caractère stratégique et de la complexité des enjeux, par exemple en tenant compte du préjudice réel ou potentiel pour la protection des données, du nombre de personnes visées et de la technologie utilisée. Le fait d'autoriser ces autorités à fixer leurs propres priorités faciliterait également la gestion des contraintes financières et budgétaires.

Les fonctions prévues à l'article 52, paragraphes 2 et 3, qui indique que les autorités chargées de la protection des données « sensibilise[nt] » et « sur demande, conseille[nt] toute

personne concernée », semblent réduire la marge d'appréciation dont ces autorités doivent nécessairement disposer pour être efficaces. En outre, afin que ces autorités bénéficient de cette marge, le groupe de travail suggère d'insérer le verbe « peut » à l'article 34, paragraphe 3, comme suit : « et peut formuler des propositions appropriées afin de remédier à cette non-conformité ».

Territorialité et compétence des autorités chargées de la protection des données (guichet unique)

L'article 51, paragraphe 1, prévoit qu'une autorité chargée de la protection des données est compétente sur le territoire de l'Etat membre dont elle relève. Cette règle générale est complétée par l'article 51, paragraphe 2, qui indique que l'autorité chargée de la protection des données d'un Etat membre où un responsable du traitement a son établissement principal est réputée être l'autorité compétente pour contrôler les activités de traitement dans tous les États membres.

Le groupe de travail est favorable à la création du concept d'autorité chef de file et à l'instauration d'une obligation claire, faite aux autorités chargées de la protection des données, de coopérer et de s'en remettre au mécanisme de contrôle de la cohérence dans les cas où des personnes concernées dans plusieurs autres Etats membres sont susceptibles d'être affectées par des activités de traitement, car cela permettra une interprétation et une application uniformes du cadre juridique de l'UE, ce qui contribuera à la sécurité juridique. Toutefois, comme mentionné ci-dessus, afin que le mécanisme puisse fonctionner, il convient de clarifier la définition de la notion d'établissement principal et les conséquences sur la compétence des autres autorités chargées de la protection des données. De même, la manière dont est envisagé le mécanisme de contrôle de la cohérence soulève des questions.

En tout état de cause, il doit être clair qu'une autorité chargée de la protection des données qui a été désignée chef de file ne dispose pas d'une compétence exclusive. La compétence de l'autorité chef de file est soumise aux obligations de coopérer, fournir et accepter l'assistance mutuelle et de recourir au mécanisme de contrôle de la cohérence, comme énoncé au chapitre VII sur la coopération et la cohérence, ainsi que d'agir en accord avec les autres autorités chargées de la protection des données concernées.

En outre, le groupe de travail souligne que le principe de guichet unique énoncé à l'article 51, paragraphe 2, ne s'applique que lorsque le responsable du traitement ou le sous-traitant possède plus d'un établissement au sein de l'UE ;
il ne s'applique pas lorsqu'il n'y a aucun établissement dans l'UE et lorsque les activités de traitement sont liées à l'offre de biens et de services à des personnes concernées dans l'Union ou à l'observation de leur comportement, conformément à l'article 3, paragraphe 2.
Par conséquent, dans ce cas, toute autorité chargée de la protection des données dont l'Etat membre est affecté par des activités de traitement est compétente conformément à l'article 51, paragraphe 1, mais le règlement manque de règles pour déterminer l'autorité « chef de file » dans ces situations. Le groupe de travail estime que la coopération et la cohérence sont tout particulièrement importantes dans ces situations.

Etant donné que les éléments actuellement énoncés pour définir l'établissement principal à l'article 4, paragraphe 13, ne sont pas satisfaisants, comme expliqué plus haut, et qu'il y a donc un manque de clarté quant à la détermination de l'autorité chef de file compétente dans les situations transfrontières, le groupe de travail propose d'envisager :

1. d'accepter que la compétence d'une autorité chef de file est non exclusive, mais subordonnée aux obligations de coopérer, de fournir et d'accepter l'assistance mutuelle et de recourir au mécanisme de contrôle de la cohérence, comme énoncé au chapitre VII sur la coopération et la cohérence ; et
2. lorsqu'il n'y a aucun établissement dans l'UE (ou que le lieu de l'établissement principal n'est pas clair), de définir des critères permettant de désigner l'autorité chef de file, qui pourraient être notamment :
   - l'Etat membre dans lequel les traitements en question ont lieu ;
   - l'Etat membre dans lequel des personnes font l'objet des traitements ;
   - l'Etat membre dans lequel des personnes ont expressément introduit une réclamation ou fait part de leurs préoccupations auprès de l'autorité chargée de la protection des données, conformément à l'article 73, paragraphe 1.

Il est évident qu'il peut y avoir plusieurs Etats membres pour chacun des critères susmentionnés. Toutefois, à partir de ces critères, les autorités concernées devraient convenir entre elles de celle qui endosse la responsabilité de chef de file. Dans les cas où cette désignation n'est pas évidente ou ne fait pas l'objet d'un accord, le comité européen de la protection des données devrait décider, en se fondant sur les mêmes critères, quelle est l'autorité chef de file.

Assistance mutuelle

Le groupe de travail suggère l'adoption d'un concept global concernant l'autorité chef de file et la coopération. Chaque fois que, au sens de l'article 56, « des personnes concernées dans plusieurs autres Etats membres sont susceptibles de faire l'objet de traitements », les autorités respectives chargées de la protection des données devraient avoir l'obligation générale de coopérer dans la mesure où leurs citoyens sont affectés. Cette coopération devrait comprendre une appréciation juridique ainsi que l'adoption de mesures de contrôle spécifiques.

Relativement à l'article 55, paragraphe 1, le groupe de travail estime que les autorités chargées de la protection des données devraient se communiquer d'autres informations utiles, également lorsqu'une mesure, au sens de l'article 58, paragraphe 1, n'a pas encore été adoptée (par exemple, en cas de violation de la sécurité). De plus, les autorités

chargées de la protection des données devraient se communiquer leurs décisions favorables en ce qui concerne les analyses d'impact relatives à la protection des données.

Le groupe de travail suggère de préciser, aux articles 55 et 56, que chaque fois qu'une décision doit être prise qui implique tant l'autorité chef de file, au sens de l'article 51, paragraphe 2, qu'une autre autorité chargée de la protection des données concernée en vertu de l'article 51, paragraphe 1, l'autorité chef de file et l'autorité nationale «sur place» devraient agir de concert en ce qui concerne l'évaluation de la situation et les mesures à adopter. Lorsque les autorités concernées ne parviennent pas à un consensus en ce qui concerne l'évaluation de la situation et/ou les mesures à adopter sur un plan bilatéral ou multilatéral, la situation devrait être soumise au mécanisme de contrôle de la cohérence prévu à l'article 57.

Le groupe de travail salue les mesures proposées pour garantir que les autorités chargées de la protection des données puissent travailler ensemble, et note que la compétence de l'autorité chef de file examinée ci-dessus n'est pas exclusive. Le groupe de travail souligne toutefois qu'il en faut davantage pour assurer l'assistance mutuelle, en termes de budget pour les autorités chargées de la protection des données, comme mentionné ci-dessus, mais également en ce qui concerne la prise en charge de certains détails importants de la mise en pratique de l'assistance mutuelle. La langue utilisée, les délais, la quantité et la nature des informations demandées ainsi que les moyens techniques, les formats et les procédures pour l'échange des informations constituent des questions qui, dans la pratique, sont vitales pour assurer une coopération efficace entre les autorités chargées de la protection des données et sont donc également au coeur du principe de « guichet unique ».

Cohérence

Le groupe de travail se félicite que sa proposition relative à un mécanisme de coopération et de coordination destiné à garantir une application cohérente des règles en matière de protection des données ait été introduite aux articles 57 et 58 de la proposition.

Le groupe de travail estime toutefois que ce mécanisme devrait assurer une cohérence uniquement dans les domaines où cela est nécessaire, qu'il ne devrait pas empiéter sur l'indépendance des autorités de contrôle nationales et les différents acteurs devraient conserver leurs responsabilités telles qu'elles sont réparties.

Au vu de la large portée de l'article 58, paragraphe 2, point a), qui couvre le traitement de données dans le cadre de tout type d'offre transfrontière de biens ou services au sein de l'UE, le groupe de travail suggère que ne soient soumis au comité européen de la protection des données, dans le cadre du mécanisme de contrôle de la cohérence, que les cas dans lesquels les autorités compétentes, conformément à l'article 51, ne parviennent pas à un consensus sur l'évaluation de la situation et/ou les mesures à adopter sur un plan bilatéral ou multilatéral. En tout état de cause, le comité européen de la protection des données devrait être informé des situations présentant un intérêt général pour la protection des données ou la libre circulation des données à caractère personnel au sein de l'UE.

Afin d'éviter qu'un grand nombre de dossiers ne soient ouverts en raison de la portée très large du mécanisme (du fait de l'article 58, paragraphe 3, qui indique que toute autorité peut demander que toute question soit traitée dans le cadre du mécanisme de contrôle de la cohérence), le groupe de travail suggère de soumettre à un vote au sein du comité européen de la protection des données les demandes présentées au titre de l'article 58, paragraphe 3.

En dépit du rôle de gardienne des traités de la Commission, le groupe de travail émet de sérieuses réserves quant au rôle envisagé pour la Commission en ce qui concerne les cas particuliers en cours d'examen dans le cadre du mécanisme de contrôle de la cohérence, puisqu'il empiète sur l'indépendance des autorités chargées de la protection des données et du comité européen de la protection des données. Lorsqu'une question est examinée ou a été examinée par le comité européen de la protection des données dans le cadre de ce mécanisme, la Commission devrait être en mesure de donner son appréciation juridique tout en s'abstenant en principe d'intervenir. Cela vaut particulièrement en cas de suspension d'une mesure, comme énoncé à l'article 60, paragraphe 1, et à l'article 62, paragraphe 1, point a), et paragraphe 2. De plus, l'existence de « doutes sérieux » n'est pas suffisante pour déclencher l'intervention de la Commission.

Le groupe de travail souligne qu'il appartient au comité européen de la protection des données de veiller à ce que ses avis soient respectés et appliqués de manière uniforme par toutes les autorités concernées chargées de la protection des données.

Afin d'accroître l'efficacité des avis du comité européen de la protection des données, un « mécanisme de confirmation » pourrait être introduit pour le cas où une ou plusieurs autorités chargées de la protection des données entendent déroger à un avis adopté par le comité dans le cadre du mécanisme de contrôle de la cohérence, conformément à l'article 58, paragraphe 7. Le comité devrait, dans ce cas, être en mesure de reconfirmer son avis par un vote à la majorité qualifiée, soulignant ainsi l'importance d'une approche commune pour les situations présentant un intérêt général pour la protection des données au sein de l'UE. Une autre solution consisterait à offrir aux autorités chargées de la protection des données la possibilité d'exprimer des positions minoritaires. Ces positions devraient être motivées et rendues publiques.

De plus, il conviendrait d'envisager une procédure pour permettre au comité européen de la protection des données et à la Commission de solliciter l'avis de la Cour de justice de l'Union européenne sur l'interprétation du règlement, au cas où une autorité chargée de la protection des données aurait l'intention de ne pas suivre un avis reconfirmé par le comité européen à l'issue d'un vote à la majorité qualifiée.

Annexes

Application de la législation nationale (chapitre IX)

Lorsque des règles particulières seront adoptées dans les Etats membres au titre des articles 80 à 83, ces règles s'articuleront avec les règles relatives à la compétence des autorités chargées de la protection des données et au mécanisme d'autorité chef de file.

Le texte ne résout pas, dans sa version actuelle, la question des cas découlant de la législation nationale connexe, par exemple dans le contexte du travail, par rapport au champ de compétence de l'autorité chargée de la protection des données dont relève l'établissement principal du responsable du traitement. La question est de savoir si, par exemple, l'autorité allemande chargée de la protection des données serait tenue d'interpréter et d'appliquer la législation du travail espagnole en cas de litige concernant un salarié d'une filiale espagnole d'une société dont l'établissement principal se situe en Allemagne. Il faudrait dès lors préciser que, par dérogation à l'article 51, paragraphe 2, pour les cas subordonnés à l'application de la législation nationale conformément au chapitre IX du règlement, l'autorité nationale chargée de la protection des données devrait toujours (en coopérant, bien entendu, avec l'autorité chef de file) être compétente pour appliquer la législation nationale connexe dans ce cas particulier (dans l'exemple donné ci-dessus, l'autorité espagnole chargée de la protection des données serait compétente pour appliquer, dans le contexte du travail, la législation espagnole en matière de protection des données).

D'une manière générale, le groupe de travail souligne la nécessité de clarifier le champ d'application des lois nationales adoptées au titre du chapitre IX.

Délais

Le groupe de travail convient qu'il est important que les avis du comité européen de la protection des données sollicités par le biais du mécanisme de contrôle de la cohérence soient émis en temps utile. Le délai imparti pour obtenir des résultats devrait toutefois permettre d'assurer la qualité des conseils. Afin de garantir une influence et un soutien effectifs sur le terrain et de garantir que l'avis puisse être confirmé dans le cadre d'une éventuelle procédure juridictionnelle, le délai strict qui est proposé devra en tout état de cause être étendu.

« Guichet unique » pour les personnes concernées

A l'instar des responsables du traitement, les personnes

concernées relevant de la compétence des autorités chargées de la protection des données dans les pays de l'UE devraient également disposer d'un « guichet unique ». Dans le règlement, plusieurs possibilités sont offertes aux personnes concernées pour exercer leurs droits et demander justice. Les personnes concernées peuvent introduire une réclamation auprès d'une autorité chargée de la protection des données dans tous les Etats membres (auprès de leur autorité nationale chargée de la protection des données, de l'autorité de l'Etat membre où le responsable du traitement a son établissement principal ou auprès de toute autre autorité de l'Union). Les personnes concernées peuvent également engager une action devant leur juridiction nationale et devant la juridiction du pays où le responsable du traitement a un établissement.

Si ces possibilités peuvent vraisemblablement accroître les droits des personnes concernées, elles peuvent également entraîner de la confusion et de l'incertitude quant à l'entité qui sera chargée, en définitive, de fournir une réponse à la personne concernée.

En dépit du droit d'introduire un recours juridictionnel, le groupe de travail suggère de préciser que les personnes concernées doivent, en principe, contacter l'autorité chargée de la protection des données du pays où elles résident ou celle du pays où le responsable du traitement ou le sous-traitant a un établissement. Afin de pouvoir répondre à la personne concernée, l'autorité sollicitée dans cet Etat membre serait tenue de coopérer avec l'autorité dont relève l'établissement principal du responsable du traitement (l'autorité chef de file) afin de convenir des mesures nécessaires pour procéder à l'examen du dossier et, dans certains cas, pour faire respecter le règlement. Toutefois, dans toutes les circonstances, c'est l'autorité initialement sollicitée qui restera chargée de répondre à la personne concernée.

Structure institutionnelle du comité européen de la protection des données

Le groupe de travail note qu'il sera remplacé par le comité européen de la protection des données, institué à l'article 64.

Le groupe de travail estime qu'il devrait pouvoir choisir de manière démocratique ses propres président et vice-présidents. Il estime qu'aucune raison convaincante n'a été avancée pour exiger que le contrôleur européen de la protection des données (CEPD) en soit un vice-président permanent.

En outre, il serait souhaitable de disposer d'un secrétariat entièrement indépendant. Or, le groupe de travail relève que le secrétariat du comité doit être assuré par le CEPD et non plus par la Commission. Il conviendrait de réfléchir plus avant à cette organisation en termes de dispositions pratiques et de rapports hiérarchiques, en particulier en ce qui concerne la nécessité de garantir l'indépendance des membres du secrétariat et les conséquences juridiques et institutionnelles liées au fait de confier le secrétariat du comité à l'un de ses membres.

Transferts internationaux

Le règlement souligne à juste titre la responsabilité qui incombe aux responsables du traitement de garantir que les données à caractère personnel demeurent protégées lorsqu'elles sont transférées en dehors de l'espace économique européen (EEE). Il simplifie la tâche des responsables du traitement en prévoyant diverses « sphères de sécurité » sous la forme de décisions relatives au caractère adéquat du niveau de protection, d'un système rationalisé de règles d'entreprise contraignantes pour les multinationales, de clauses contractuelles approuvées et d'une autorisation par l'autorité

chargée de la protection des données. Il prévoit également diverses dérogations à l'article 44.

Toutefois, les dérogations, en particulier à l'article 44, paragraphe 1, point h), demeurent très étendues et pourraient s'appliquer à de nombreuses situations. Conformément à l'avis précédent du groupe de travail (WP 114), ces dérogations ne devraient être applicables que dans la mesure où le traitement n'est pas massif, pas répétitif et pas structurel.

De plus, l'article 42 introduit la possibilité de recourir à des instruments non contraignants pour encadrer les transferts internationaux, qui sont soumis à l'autorisation des autorités chargées de la protection des données. Or, le caractère contraignant a toujours été considéré comme une exigence importante dans les outils qui encadrent actuellement les transferts internationaux (par exemple, clauses contractuelles types, règles d'entreprise contraignantes, sphère de sécurité, niveau de protection adéquat assuré dans les pays tiers). Dès lors, le groupe de travail propose de supprimer l'article 42, paragraphe 5, à l'exception de la dernière phrase. Le renvoi figurant à l'article 34 doit donc être adapté en conséquence.

Concernant l'article 41, paragraphe 6, il conviendrait de préciser si les termes « sans préjudice des articles 42 à 44 » signifient qu'en cas de décision négative relative au caractère adéquat du niveau de protection prise par la Commission, les transferts de données vers le pays tiers concerné sont néanmoins possibles en vertu de l'ensemble de ces articles. Pour finir, lorsque la Commission constatera par voie de décision qu'un pays tiers, ou un territoire ou un secteur de traitement de données dans ce pays tiers ou l'organisation internationale en question assure un niveau de protection adéquat (article 41), ledit transfert ne nécessitera aucune autre autorisation. Toutefois, comme mentionné auparavant, le groupe de travail suggère vivement d'inclure l'obligation pour la Commission de consulter le comité européen de la protection des données au sujet des décisions relatives au caractère adéquat du niveau de protection.

Divulgations non autorisées par la législation de l'UE

Le groupe de travail souligne la nécessité d'inclure dans le règlement le recours obligatoire aux traités d'entraide judiciaire en cas de divulgations non autorisées par la législation de l'Union ou des Etats membres. Il estime que l'absence de disposition sur le recours

obligatoire aux traités d'entraide judiciaire, lorsqu'ils existent, laisserait notamment la voie ouverte à de larges transferts de données à caractère personnel pour une catégorie vaste et illimitée de « motifs importants d'intérêt général », conformément à l'article 44, paragraphe 1, point d), y compris lorsque ces transferts revêtent un caractère massif, fréquent et structurel. Lorsque le jugement d'une cour ou d'un tribunal ou la décision d'une autorité administrative d'un pays tiers exige d'un responsable du traitement ou d'un sous-traitant qu'il transfère des données de l'UE vers ce pays tiers et qu'il n'existe aucun traité d'entraide judiciaire ou autre accord international en vigueur entre le pays tiers demandeur et l'Union ou le ou les Etats membres, le transfert desdites données devrait être interdit. Le groupe de travail souligne que lorsqu'un traité d'entraide judiciaire est en vigueur, l'autorité compétente au titre dudit traité (ou d'un accord international analogue) devrait être l'autorité traitant la demande, laquelle devrait, si nécessaire, consulter l'autorité chargée de la protection des données.

Droit à réparation et responsabilité

Le groupe de travail salue la disposition introduite à l'article 77, paragraphe 1, pour garantir que toute personne ayant subi un dommage du fait d'un traitement illicite ou de toute action incompatible avec le règlement a le droit d'obtenir du responsable du traitement ou du soustraitant réparation du préjudice subi. Il salue également le fait que l'article 77, paragraphe 2, garantisse que, lorsque plusieurs responsables du traitement ou sous-traitants ont participé au traitement, il n'incombe pas à la personne concernée de déterminer lequel d'entre eux porte la responsabilité du préjudice. Il estime toutefois qu'il est nécessaire de préciser (dans un considérant) que le terme « préjudice » ou « dommage » ne signifie pas simplement un préjudice matériel mais également une souffrance (un préjudice qui n'est pas matériel).

Si une décision prise par une autre autorité chargée de la protection des données (par exemple, l'autorité dont relève l'établissement principal) affecte la personne concernée ou lui cause un préjudice, cette dernière devrait être en mesure d'intenter une action contre cette décision devant les juridictions administratives de son pays de résidence. La solution telle qu'elle est proposée par la Commission européenne, à savoir que soit la personne concernée soit l'autorité chargée de la protection des données puisse intenter une action contre l'autre autorité sur le territoire de cette dernière, est loin d'être satisfaisante. Le groupe de travail demande qu'un système permette aux personnes concernées d'intenter une action contre une décision administrative devant la juridiction administrative de leur pays de résidence.

Amendes

Le groupe de travail salue l'instauration d'amendes importantes, parce que celles-ci permettront aux autorités chargées de la protection des données d'assumer leur rôle d'autorité répressive et qu'elles pourront, par leur effet dissuasif, contribuer à un plus grand respect de l'instrument de la part des responsables du traitement.

L'article 79, paragraphe 1, prévoit que chaque autorité de contrôle soit « habilitée » à infliger des sanctions administratives. Le considérant 120 soutient cette disposition en indiquant que l'autorité de contrôle « devrait avoir le pouvoir » de sanctionner les infractions administratives. Toutefois, les paragraphes 4 à 6 de l'article 79 indiquent que l'autorité de contrôle « inflige une amende » dans les situations décrites. Le groupe de travail est d'avis que les autorités chargées de la protection des données devraient disposer d'une marge d'appréciation pour décider des situations dans lesquelles elles infligent une amende, puisque de

nombreux facteurs influent sur la nature de l'infraction et doivent être pris en compte lorsqu'il est décidé d'infliger une amende. Il suggère dès lors de modifier en conséquence le libellé de l'article 79, paragraphes 4 à 6.

Le groupe de travail apprécie l'effet d'harmonisation produit par l'article 79, qui détermine à quelle amende maximum une infraction donne lieu, puisque cela permettra une plus grande cohérence des amendes infligées dans l'Union européenne. Néanmoins, il suggère d'expliciter à l'article 58, paragraphe 2, la possibilité de recourir au mécanisme de contrôle de la cohérence, prévu à la section 2 du chapitre VII, pour résoudre les divergences d'application des sanctions administratives, comme le prévoit également le considérant 120.

Par ailleurs, le groupe de travail comprend que lorsque plusieurs autorités chargées de la protection des données sont compétentes, elles sont toutes habilitées à infliger une amende en vertu de l'article 79 du règlement. Cela soulève cependant des questions quant au principe non bis in idem (interdiction de la double incrimination).

En outre, le groupe de travail pense que du fait du seuil introduit en cas de premier manquement non intentionnel au règlement, de nombreux responsables du traitement échapperaient, dans la pratique, à son application, et il estime donc que ce seuil devrait être supprimé. Si un seuil devait être introduit, il serait en tout état de cause plus approprié de tenir compte du nombre de personnes concernées affectées (de manière négative) que du nombre de salariés du responsable du traitement.

Recours juridictionnels

Le groupe de travail salue l'inclusion d'un ensemble de règles complet sur les recours juridictionnels ouverts aux personnes concernées, y compris la possibilité pour les organisations ou associations d'exercer les droits des personnes concernées vis-à-vis des responsables du traitement et des sous-traitants. Toutefois, de l'avis du groupe de travail, plusieurs aspects du chapitre VIII exigent un éclaircissement.

Vu l'étendue du champ d'application de l'article 73, paragraphe 1, en vertu duquel toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité chargée de la protection des données dans tout État membre, le groupe de travail estime que la personne concernée devrait, en principe, saisir l'autorité chargée de la

protection des données de son pays de résidence ou du pays où est établi le responsable du traitement ou le sous-traitant, comme le groupe de travail l'a également indiqué ci-dessus à propos du guichet unique pour les personnes concernées.

En outre, lorsque l'autorité chargée de la protection des données qui reçoit la réclamation semble ne pas être la bonne au vu du fond de l'affaire, le groupe de travail estime que cette autorité devrait avoir l'obligation de coopérer avec l'autorité « guichet unique » de la personne concernée et l'autorité du lieu où est établi le responsable du traitement. Dans ce cas, l'autorité chargée de la protection des données auprès de laquelle la réclamation a été introduite serait tenue d'informer la personne concernée de l'évolution de l'affaire, indépendamment du fait qu'elle soit compétente ou non quant au fond de l'affaire. Il s'agit d'un corollaire de la nécessité de désigner un guichet unique pour les personnes concernées (voir ci-dessus).

En ce qui concerne l'article 74, paragraphe 2, le groupe de travail estime qu'il conviendrait de préciser quelle autorité chargée de la protection des données est compétente pour « donner suite à une réclamation, en l'absence d'une décision nécessaire pour protéger [les] droits [de la personne concernée] ». Lorsqu'une autorité chef de file serait visée par un recours, l'autorité compétente pour donner suite à la réclamation serait, conformément à l'article 51, paragraphe 2, celle de l'Etat membre où le sous-traitant/responsable du traitement a son établissement principal, et dans tout autre cas il s'agirait de l'autorité compétente conformément à l'article 51, paragraphe 1. Il conviendrait donc de préciser à l'article 74, paragraphe 2, que l'obligation de donner suite renvoie à l'autorité de contrôle compétente « [...] au sens de l'article 51, paragraphe 1 ou paragraphe 2 ».

De plus, l'article 74, paragraphe 4, dispose qu'une personne concernée affectée par une décision prise par l'autorité chargée de la protection des données d'un Etat membre autre que celui dans lequel ladite personne a sa résidence habituelle peut demander à l'autorité de l'Etat membre dans lequel elle a sa résidence habituelle d'intenter une action contre l'autorité de l'autre Etat membre. Si le groupe de travail comprend ce qui motive l'introduction d'une disposition de ce type, qui veille à ce que les personnes concernées puissent exercer leurs droits vis-à-vis d'une autorité chargée de la protection des données dans un autre Etat membre, il considère néanmoins qu'elle est contraire à l'obligation générale faite aux autorités chargées de la protection des données de coopérer et de se prêter mutuellement assistance dans les affaires transfrontières, conformément aux articles 55 et 56, et au fait qu'en cas de désaccord entre lesdites autorités, le comité européen de la protection des données doit être saisi de l'affaire. Dès lors, le groupe de travail souligne la nécessité d'examiner attentivement d'autres possibilités de recours juridictionnel pour la personne concernée à l'encontre d'une décision prise par une autorité à son détriment, qui soient cohérentes avec les principes du règlement.

L'article 75, paragraphe 2, prévoit la possibilité pour les personnes concernées d'intenter une action contre un responsable du traitement ou un sous-traitant devant les juridictions de l'Etat membre dans lequel le responsable du traitement ou le sous-traitant dispose d'un établissement, ou d'intenter une telle action devant les juridictions de l'Etat membre dans lequel la personne concernée a sa résidence habituelle. Le groupe de travail estime que la possibilité d'intenter une action devant les juridictions de tout Etat membre dans lequel le responsable du traitement ou le sous-traitant a un établissement, indépendamment

du fait qu'il s'agisse de l'établissement principal ou de l'établissement dans lequel les décisions pertinentes en matière de traitement des données sont prises, peut poser problème.

Bien que l'article 75, paragraphe 4, indique que les Etats membres doivent mettre à exécution les décisions définitives rendues par les juridictions des autres Etats membres, il n'est pas certain qu'une décision prise par une juridiction dans un Etat membre où le responsable du traitement ou le sous-traitant n'a pas son établissement principal soit réellement exécutoire. Ce point exige une clarification.

En outre, même si le groupe de travail salue le fait qu'ait été incluse à l'article 75, paragraphe 2, la possibilité d'intenter une action contre un responsable du traitement devant les juridictions de l'Etat membre dans lequel la personne concernée a sa résidence habituelle - par analogie avec la notion de protection du consommateur conformément au règlement Bruxelles I -, dans le but de renforcer la position des personnes concernées, on ne voit pas clairement comment serait exécuté le jugement d'une juridiction de l'Etat membre dans lequel la personne concernée a sa résidence habituelle si le responsable du traitement ou le sous-traitant est établi dans un autre Etat membre.

Tant l'article 74, paragraphe 5, que l'article 75, paragraphe 4, prévoient que les Etats membres mettent à exécution les décisions définitives des juridictions visées dans ces articles. Ces dispositions sont comparables à des obligations similaires énoncées à l'article 111 de la convention d'application de l'accord de Schengen. Comme indiqué ci-dessus, on ne sait pas exactement en vertu de quelles règles de procédure et par quelles autorités nationales les décisions rendues par les juridictions d'un Etat membre seraient exécutées dans un autre Etat membre. En outre, en ce qui concerne la détermination de ce qui constitue une décision « définitive », une harmonisation plus poussée pourrait se révéler indispensable (Système d'information Schengen – affaire AU/FR).

Eglises et associations religieuses

Le groupe de travail comprend que l'article 85 oblige les églises et les associations religieuses qui ont à l'heure actuelle des régimes juridiques distincts à les mettre en conformité avec le règlement. Cela ne confère aucunement aux églises et aux associations religieuses la possibilité d'adopter, dans les États membres où les dispositions

constitutionnelles ne permettent pas une telle mise en conformité, un régime juridique distinct qui serait incompatible avec le règlement.

En ce qui concerne la directive

Choix de l'instrument

Le groupe de travail prend note du choix explicite fait par la Commission européenne de ne pas présenter un instrument unique pour la protection des données dans tous les domaines, et de présenter une directive pour être l'instrument réglementant la protection des données dans le domaine de la police et de la justice pénale, au niveau élevé et constant visé par la Commission en la matière. Toutefois, le groupe de travail note également que la proposition actuelle entraînerait un abaissement des normes en matière de protection des données dans plusieurs États membres. Cette perspective est pour lui inacceptable et il prie donc le législateur européen de veiller à ce que les garanties les plus élevées en matière de protection des données en vigueur dans l'Union européenne soient considérées comme le strict minimum pour la proposition de directive. La directive ne devrait pas être interprétée de manière à justifier la suppression de garanties supplémentaires en matière de protection des données prévues par la législation actuelle de certains Etats membres.

Cohérence

Bien que différents instruments soient proposés, les aspects « fondamentaux » des dispositions doivent être cohérents, en particulier en ce qui concerne les principes, obligations et responsabilités, droits et pouvoirs, et les outils mis à la disposition des autorités de contrôle. En effet, compte tenu du caractère sensible des traitements qui font l'objet de la directive, il serait inacceptable que des normes moins élevées s'appliquent à ce domaine. Bien entendu, il est nécessaire de prévoir des limitations et des exceptions, notamment en ce qui concerne les droits des personnes concernées, mais il doit être clair qu'il s'agit d'exceptions et que les aspects « fondamentaux » demeurent les mêmes.

Champ d'application

Le groupe de travail note et salue le fait que la directive ait abandonné la distinction entre le traitement de données à caractère personnel dans les affaires nationales et celui dans les affaires transfrontières, qui était prévue dans la décision-cadre 2008/977/JAI. Cette limitation de l'applicabilité de la législation européenne aux affaires strictement transfrontières a été critiquée par le groupe de travail dans le passé.

Le champ d'application de la directive doit être aussi clair que possible. Toutefois, le texte proposé soulève diverses questions, dont les suivantes.

Le groupe de travail note la difficulté qu'il y a à distinguer le champ d'application de la directive du champ d'application du règlement. La directive s'applique si les autorités compétentes traitent des données à caractère personnel 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. Dans toutes les autres circonstances, c'est le règlement qui s'applique, en tant qu'instrument général de protection des données à caractère personnel. Toutefois, il y a lieu de tenir compte des différentes pratiques des Etats membres lorsqu'ils définissent les activités de leurs autorités qui se rattachent à des fins répressives ou simplement administratives (par exemple, dans les domaines des douanes, de l'immigration, de l'environnement). Par conséquent, les deux instruments, la directive et le règlement, seraient susceptibles de s'appliquer à une même institution. Il faut éviter les situations dans lesquelles une même opération de traitement,

par exemple en lien avec le maintien de l'ordre public, serait, dans un pays, couverte par le règlement, tandis que dans d'autres Etats membres ce seraient les lois basées sur la directive qui s'appliqueraient. Cela pose particulièrement problème si les deux instruments manquent de cohérence, comme c'est le cas actuellement. De ce point de vue, il faut davantage de cohérence entre les deux instruments et une plus grande clarté serait nécessaire en ce qui concerne la définition des « autorités compétentes ». Le groupe de travail estime qu'il faut définir clairement quelles sont les missions, dont les autorités compétentes sont investies par la loi, auxquelles s'applique la directive.

Le groupe de travail est d'avis qu'il faut préciser davantage dans quelle mesure la directive s'applique au domaine de la procédure pénale. Il note que la directive s'applique au traitement des données aux fins de la poursuite des infractions pénales (article premier). Dans le même temps, le groupe de travail comprend qu'il faut entendre par l'article 17 (et le considérant 82) que les Etats membres peuvent décider de ne pas aligner leurs règles nationales en matière de procédure pénale sur les droits prévus aux articles 11 à 16, du moins dans les cas qui concernent les procédures judiciaires. Les différences qui existent en matière de procédure pénale nationale, toutefois, ne permettent pas de déterminer facilement de quelle phase des poursuites il est question lorsque la directive, à l'article 17, indique que, « lorsque les données à caractère personnel figurent dans une décision judiciaire ou un casier judiciaire faisant l'objet d'un traitement lors d'une enquête judiciaire ou d'une procédure pénale, les droits […] sont exercés conformément aux règles nationales de procédure pénale ». Le groupe de travail invite le législateur européen à s'assurer qu'il ne puisse subsister aucun doute quant au fait que la directive s'applique aux procédures pénales et à la poursuite d'infractions pénales, également pour éviter les cas dans lesquels une protection des données ne serait pas assurée dès qu'un procureur ou un juge d'instruction participe à une opération répressive ou à une enquête, conformément à la convention 108 du Conseil de l'Europe.

En outre, le groupe de travail estime que l'article 44, paragraphe 2, requiert une clarification quant au sens et à l'intention à prêter aux termes « dans l'exercice de leurs fonctions juridictionnelles ». Il convient de préciser quelle doit être la relation entre l'autorité chargée de la protection des

données et les juridictions et dans quelles circonstances des missions de contrôle peuvent être effectuées.

Principes de traitement des données

En ce qui concerne les principes, la directive n'intègre pas d'éléments importants relatifs à la conservation des données à caractère personnel (notamment des durées de conservation), à la transparence envers les personnes physiques, à la mise à jour des données à caractère personnel et à la vérification du caractère adéquat, pertinent et non excessif des données conservées. Il manque également des dispositions en matière de responsabilité qui exigeraient du responsable du traitement qu'il prouve son respect de l'instrument. Le libellé de l'article 4 devrait être rendu concordant avec le libellé figurant dans le règlement (article 5).

Le groupe de travail suggère en outre d'inclure des dispositions limitant l'accès aux données au personnel dûment autorisé des autorités compétentes qui en a besoin pour l'exécution de ses missions.

Outre les observations formulées ci-dessus concernant le manque de cohérence avec le règlement, le groupe de travail salue la distinction proposée entre les différentes catégories de personnes concernées devant faire l'objet d'un traitement. Il note en particulier la distinction devant être faite entre les données relatives à des suspects, des victimes, des témoins, etc. De même, il salue la distinction devant être faite en fonction de la qualité et la précision des données traitées par les services répressifs. Le groupe de travail regrette toutefois que ces distinctions soient limitées par l'ajout des termes « dans la mesure du possible » aux articles 5 et 6, termes qu'il propose de supprimer. Par ailleurs, il s'inquiète de l'ampleur de la catégorie de personnes concernées classées « divers » [article 5, paragraphe 1, point e)] dont les données peuvent faire l'objet d'un traitement. Le groupe de travail suggère de reformuler cette catégorie pour veiller à ce que les données de personnes non soupçonnées ne puissent être traitées que pendant une durée limitée et dans des conditions strictes. La directive devrait préciser que des règles plus strictes doivent s'appliquer en termes de délais et de contrôle aux catégories de personnes concernées mentionnées à l'article 5, paragraphe 1, points b) à e).

En ce qui concerne la licéité du traitement (article 7), la raison de l'insertion des dispositions des points b), c) et d) n'est pas claire. Ces dispositions semblent en contradiction avec l'article premier, paragraphe 1, qui définit l'objet de la directive. Le groupe de travail considère qu'on ne saurait autoriser des traitements qui ne sont pas conformes à l'objet général de la directive. Ainsi, il faut soit supprimer les dispositions des points b), c) et d), soit adapter l'article premier, paragraphe 1, afin de permettre ces traitements.

Le groupe de travail estime que des dispositions particulières devraient être introduites à propos du traitement des données à caractère personnel concernant des enfants, comme le prévoit le règlement. En particulier, il faudrait obliger les Etats membres à prévoir des seuils d'âge en deçà desquels les données ne devraient pas être traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière sans que cela ne soit dûment justifié, en particulier si des catégories particulières de données doivent être collectées. De plus, il faudrait que les Etats membres prévoient pour les données concernant les enfants des durées de conservation plus courtes dans les fichiers de la police et de la justice.

La disposition sur les catégories particulières (article 8) est légèrement plus étendue que dans la décision-cadre

2008/977/JAI. Le groupe de travail s'interroge sur les conséquences que cela peut avoir, et se demande notamment si les dérogations énoncées au paragraphe 2 pourraient donner lieu, dans la législation nationale, à une clause générale indiquant que toutes les données sensibles peuvent être traitées. Dans ce cas, l'interdiction générale ne sert à rien. De plus, bien que les données génétiques soient mentionnées, aucun considérant distinct ni article ne traite du traitement de ce type de données. Une telle disposition constituerait pourtant une garantie importante par ce qui est de l'utilisation des données génétiques et de leurs durées de conservation.

Compte tenu de la dérogation énoncée à l'article 8, paragraphe 2, il existe un danger réel que des niveaux différents de protection des données à caractère personnel (données sensibles) soient autorisés au titre de la directive. Le groupe de travail suggère dès lors que le législateur européen modifie cet article par une définition plus précise des garanties appropriées exigées, afin de permettre une application harmonisée. De plus, le groupe de travail recommande d'ajouter au paragraphe 2 qu'il ne peut être recouru aux exceptions que dans le respect des conditions énoncées à l'article 4.

Droits des personnes concernées

Le groupe de travail note et salue le fait qu'en vertu de l'article 11, paragraphe 1, et de l'article 13, paragraphe 1, davantage d'informations pourraient être communiquées aux personnes concernées, du moins dans certains Etats membres. Etre informé de la nature des données traitées et du motif de leur traitement est l'un des aspects clés du droit à la protection des données. Toutefois, il y a lieu de relever, également, que les limitations apportées à l'obligation d'informer la personne concernée et au droit d'accès, prévues à l'article 11, paragraphe 5, et à l'article 13, paragraphe 2, posent problème. Le groupe de travail considère ces limitations et dérogations comme étant trop vastes et de nature trop générale, puisqu'elles permettent aux Etats membres de soustraire des catégories entières de données de l'obligation de fournir des informations. Les droits des personnes concernées (et pas seulement leurs intérêts, comme indiqué au chapitre II) s'en trouveraient considérablement limités. La directive devrait donc préciser que toute limitation des droits des personnes concernées ne peut être justifiée qu'au cas par cas, en tenant dûment compte des circonstances du cas particulier et du fait que chacune de ces restrictions (et pas seulement les omissions) doit être

pleinement justifiée. En outre, le groupe de travail estime qu'une limitation du droit d'accès et d'information devrait également signifier que, dans certains cas, les personnes concernées peuvent tout de même être partiellement informées du traitement de leurs données.

En ce qui concerne les limitations apportées aux droits, il y a lieu de préciser que le responsable du traitement devrait apprécier au cas par cas si la limitation des droits doit être appliquée, et que toute limitation doit être conforme à la charte des droits fondamentaux de l'Union européenne et à la convention de sauvegarde des droits de l'homme et des libertés fondamentales, et en accord avec la jurisprudence de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme, et en particulier respecter le contenu essentiel de ces droits et libertés. Le groupe de travail recommande d'insérer ce libellé à l'article 13.

La directive semble être cohérente avec le règlement en ce qui concerne le droit à rectification, le droit d'introduire une réclamation, le droit de recours contre l'autorité nationale chargée de la protection des données, le responsable du traitement et le sous-traitant, et le droit à réparation et la responsabilité.

Toutefois, la directive ne prévoit aucun droit d'opposition au traitement des données à caractère personnel. Il existe de nombreuses situations dans lesquelles, par exemple, des personnes concernées, victimes ou témoins devraient pouvoir faire procéder au marquage de leurs données pour limiter tout traitement ultérieur à l'issue de l'action en justice.

De même, dans la directive les responsables du traitement sont priés de répondre « sans retard indu » aux demandes des personnes physiques exerçant leurs droit d'accès, droit à rectification et droit à l'effacement. On ne voit pas clairement pourquoi les délais imposés dans le règlement ne peuvent pas également s'appliquer en l'espèce. De plus, les modalités selon lesquelles les personnes physiques peuvent exercer leurs droits devraient être davantage alignées sur les procédures décrites dans le règlement.

<u>Obligations des responsables du traitement</u>

Les obligations qui incombent aux responsables du traitement sont cohérentes avec celles prévues dans le règlement en ce qui concerne les sous-traitants, les accords avec les responsables conjoints du traitement, la coopération obligatoire avec l'autorité nationale chargée de la protection des données et les missions du délégué à la protection des données. Toutefois, au titre de la directive, le responsable du traitement n'est pas tenu d'informer la personne physique s'il prévoit de transférer des données à caractère personnel vers un pays tiers, et on ne voit pas clairement ce qui a motivé d'exclure cette obligation, en particulier au vu du fait que les Etats membres ont la possibilité de restreindre les droits des personnes physiques dans certaines circonstances.

De plus, le libellé de la directive n'est pas cohérent avec le règlement en ce qui concerne la protection des données dès la conception et la protection des données par défaut, le groupe de travail ne pouvant expliquer ce manque de cohérence. L'un des aspects de la prise en compte du respect de la vie privée dès la conception consiste à déterminer les risques du traitement au début du processus pour pouvoir les atténuer. Dès lors, le groupe de travail conseille vivement d'insérer dans la directive des dispositions exigeant une analyse d'impact relative à la protection des données, y compris pendant la procédure législative. Il estime que ces dispositions sont particulièrement importantes dans le domaine du traitement de données à caractère personnel en matière

répressive, compte tenu des risques accrus que représente ce traitement pour les personnes physiques. Les obligations relatives à la documentation sont également moins détaillées que dans le règlement. Il faudrait que les autorités compétentes concernées par la directive soient au moins tenues de consigner les coordonnées de leur délégué à la protection des données et les durées de conservation.

Le groupe de travail relève que les exigences relatives à la sécurité des données ne sont pas très détaillées et donc plutôt faibles par rapport aux normes actuelles. À titre d'exemple, les dispositions sur les obligations en matière de sécurité ne comprennent aucune protection contre les pertes ou dommages accidentels, comme le prévoit le règlement. Le groupe de particulier parce que cet aspect figure tant dans la directive actuelle (95/46/CE) que dans la décision-cadre sur la protection des données (2008/977/JAI).

Les dispositions sur la notification des violations devraient également être cohérentes d'un instrument à l'autre, le groupe de travail admettant toutefois les différences qui existent dans le secteur répressif en ce qui concerne la notification des personnes physiques. Par exemple, il peut arriver qu'il ne soit pas possible d'informer des personnes physiques d'une violation dans les délais spécifiés, ceci pouvant porter préjudice à des enquêtes ou opérations menées par les services répressifs. L'autorité chargée de la protection des données peut également jouer un rôle particulier dans l'appréciation de la nécessité d'informer la personne physique et du moment opportun pour le faire, en tenant également compte du caractère approprié des mesures prises en termes de protection technologique.

Pour finir, les dispositions sur le profilage et le traitement automatisé (article 9) ne sont pas cohérentes avec le règlement, en ce que le libellé de la directive n'intègre pas certains éléments pertinents, comme l'évaluation du comportement.

Transferts internationaux

Principes généraux applicables aux transferts et aux transferts ultérieurs

L'article 33 contient des dispositions relatives aux transferts initiaux et aux transferts ultérieurs de données à caractère personnel vers des pays tiers ou des organisations internationales. Le groupe de travail estime qu'il faut clairement distinguer ces situations et prévoir davantage de restrictions pour les transferts ultérieurs, par exemple

l'existence d'un lien évident avec la finalité pour laquelle les données ont initialement été collectées et l'obtention du consentement préalable de l'autorité émettrice. En outre, le destinataire des données doit être une autorité compétente au sens de la directive.

Décisions négatives relatives au caractère adéquat du niveau de protection

Le groupe de travail ne voit pas clairement quelle serait la finalité des décisions négatives relatives au caractère adéquat du niveau de protection et comment elles fonctionneraient dans la pratique. Le libellé laisse entendre qu'une décision négative bloquerait tous les transferts internationaux vers le pays tiers, l'organisation internationale ou le secteur de traitement de données en question. L'article 34, paragraphe 6, et l'article 35, paragraphe 1, peuvent toutefois également être compris en ce sens que sont autorisés les transferts vers des pays dont le niveau de protection est déclaré inadéquat dès lors que l'autoévaluation du caractère adéquat réalisée par le responsable du traitement et/ou le sous-traitant donne un résultat satisfaisant et que des garanties appropriées ont été convenues. Le législateur européen est donc prié d'adapter les dispositions de manière à ce que l'on sache clairement quelles seraient les conséquences des décisions négatives relatives au caractère adéquat du niveau de protection et la manière dont elles fonctionneraient dans la pratique.

Transferts moyennant des garanties appropriées

La directive prévoit, à l'article 35, la possibilité de transférer des données à caractère personnel vers des pays tiers ou des organisations internationales alors que la Commission n'a pas encore adopté de décision quant au caractère adéquat du niveau de protection. Le groupe de travail estime que si ces transferts sont effectués sur le fondement d'une autoévaluation, l'autorité compétente doit veiller à ce que les garanties appropriées aient été prévues dans un instrument juridiquement contraignant. En outre, le groupe de travail estime que les éléments énoncés à l'article 26, paragraphe 2, de la directive 95/46/CE doivent être inclus et qu'il devrait au minimum en être tenu compte lors de l'autoévaluation. Le processus aboutissant à l'autoévaluation doit être documenté et la documentation doit être mise à la disposition des autorités chargées de la protection des données si elles en font la demande.

Dérogations

Le groupe de travail s'inquiète des dérogations prévues pour le transfert de données à caractère personnel en l'absence de décision relative au caractère adéquat du niveau de protection ou de garanties appropriées (article 36), et en particulier de celles énoncées aux points c), d) et e). Ces exceptions rendraient possibles de nombreux transferts internationaux dans des cas particuliers, dès lors qu'ils sont « nécessaires ».

Il faut préciser que toute dérogation doit être interprétée de manière restrictive, de sorte que les transferts effectués sur ce fondement constituent une exception plutôt que la norme. Il faudrait également éviter que le libellé des dispositions puisse signifier que le simple fait de déclarer, sans autre explication, que le transfert visé doit être jugé nécessaire suffit pour invoquer ces dérogations, et qu'il autorise ainsi de nombreux transferts internationaux effectués au cas par cas, en l'absence de toute garantie relative à la protection des données à caractère personnel relatives à la personne concernée. Le groupe de travail estime dès lors que le libellé de l'article 36, points c), d) et e) devrait restreindre la possibilité de transferts internationaux dans des cas particuliers.

En outre, le groupe de travail note l'absence d'obligation destinée à garantir que soit documenté le recours à l'une quelconque des dérogations prévues à l'article 36. Cela serait pour le contrôleur difficile, voire impossible, de vérifier si les conditions auxquelles les dérogations sont subordonnées ont bien été remplies par le responsable du traitement et/ou le sous-traitant. Nous proposons donc d'inclure cette obligation en ajoutant : « 2. Le recours à ces dérogations doit être documenté et la documentation doit être mise à la disposition de l'autorité de contrôle si elle en fait la demande ».

Pour finir et d'une manière générale, en ce qui concerne les transferts internationaux pour lesquels aucune décision relative au caractère adéquat du niveau de protection n'est disponible, le groupe de travail estime que les États membres devraient pouvoir décider de l'opportunité de faire intervenir les autorités chargées de la protection des données dans les transferts internationaux et de la mesure de leur intervention.

Pouvoirs des autorités chargées de la protection des données et coopération

Le groupe de travail regrette que les dispositions portant sur les pouvoirs des autorités chargées de la protection des données ne soient pas très détaillées, ni cohérentes avec celles du règlement. Plus particulièrement, la directive ne comporte aucune disposition relative à l'accès aux locaux, contrairement au règlement. La capacité conférée à l'autorité de contrôle d'accéder aux locaux du responsable du traitement lorsque cela est nécessaire devrait s'appliquer à tous les secteurs.

La directive prévoit une assistance mutuelle entre les autorités chargées de la protection des données, sans toutefois mentionner les délais prévus dans le règlement. Il risque d'y avoir une incohérence et il devrait être tenu compte, pour les deux instruments, de l'avis donné sur les délais prévus dans le règlement. De même, pour veiller à la cohérence des deux instruments, la directive devrait inclure offrir la possibilité aux autorités chargées de la protection des données de participer à des opérations conjointes.

Eléments manquants

Le groupe de travail regrette, dans la directive, l'absence de dispositions sur la fixation de délais, le contrôle et d'autres garanties, comme la limitation de l'utilisation des données pour les infractions graves, etc. Le groupe de travail prend note de l'article

37 qui prévoit l'obligation pour le responsable du traitement d'informer le destinataire de toute limitation du traitement et de prendre toutes les mesures raisonnables afin de garantir que ces limitations soient respectées. Toutefois, l'article 37 ne s'applique qu'aux transferts vers des pays tiers. Aucune indication n'est fournie sur les raisons de l'absence, dans la directive, d'une règle similaire pour le transfert de données à caractère personnel entre Etats membres de l'Union. Dans ce cas, les États membres destinataires devraient également être tenus de respecter toute limitation de traitement imposée par l'Etat membre effectuant le transfert. Le groupe de travail est surpris que la directive fasse, à cet égard, un pas en arrière par rapport à la décision-cadre 2008/977/JAI.

Le groupe de travail note l'absence d'obligation pour les autorités compétentes qui ont transmis des données d'informer le destinataire que les données transmises étaient incorrectes ou avaient été transmises de manière illicite. Cette obligation est cruciale dans un domaine où les informations de nature répressive circulent librement. L'article 39, paragraphe 2, offre aux Etats membres la possibilité de décider que l'autorité chargée de la protection des données qui contrôle l'application du règlement soit la même que celle qui contrôle l'application de la directive. Compte tenu des situations nationales, en particulier dans les pays disposant d'autorités locales chargées de la protection des données, le groupe de travail préférerait en effet qu'une seule autorité chargée de la protection des données soit responsable du contrôle du respect des deux instruments. Cela assurerait une cohérence dans l'application des règles.

Pour finir, le groupe de travail regrette que la directive ne comporte aucune disposition sur le transfert vers des entités privées ou d'autres autorités qui ne sont pas considérées comme des autorités compétentes au titre de la directive. Dès lors, le groupe de travail demande instamment au législateur européen d'introduire une disposition autorisant le transfert de données de nature répressive vers des entités privées uniquement dans des circonstances strictement définies par la législation.

Fait à Bruxelles,
le 23 mars 2012

Pour le groupe de travail
Le président
Jacob KOHNSTAMM

International Working Group on Data Protection in Telecommunications - Working Paper on Cloud Computing - Privacy and data protection issues - "Sopot Memorandum"

51st meeting,
23-24 April 2012,
Sopot (Poland)

Scope

This working paper specifically examines the processing of personal data in cloud computing environments.

The working paper does not examine a situation in which all end users, the controller, the processor and all of its subcontractors are subject to the same data protection legislation and are physically located within the same jurisdiction and all data processing and data storage takes place within this jurisdiction. This paper is also of less relevance, where the cloud service is totally under the control of the cloud service user.

Finally, the working paper only deals with the use of cloud services by companies and public authorities which move existing procedures "into the cloud", not with the use of such services by individuals.

7 Annexes

General Background

"Cloud computing is an evolving paradigm."[26]

Cloud Computing (CC) is attracting increasing interest due to promises of greater economic efficiency, lower environmental impact, simpler operation, increased user-friendliness and a number of other benefits.

In September 2011, the National Institute of Standards and Technology (NIST) released Special Publication SP 800-145, in which it defined cloud computing as:

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models."[27]

The definition is, among other things,
"..... intended ..... to provide a baseline for discussion from what is cloud computing to how to best use cloud computing."[28]

The definition is an important contribution to the ongoing process of understanding what CC actually is. This understanding is developing rapidly. The NIST definition is an excellent starting point for further investigation of CC and how to use it. However, there is still uncertainty in relation to CC, especially when it concerns privacy, data protection and other legal issues. The recommendations in this paper are intended to help reduce that uncertainty.

The paper is structured to present the recommendations first. The second part of the paper provides additional background on cloud computing as well as the rationale behind the recommendations. For deeper insight, readers might benefit from reading this section first.

For the purposes of this paper, the cloud customer is deemed to be the data controller and the cloud service provider is deemed to be the data processor.[29]

The evolution of CC has highlighted a number of important issues, including:

a. there is not yet international agreement on common terminology;
b. the development of the technology is still in progress;
c. enormous amounts of data

[26] National Institute of Standards and Technology (NIST), Special Publication 800-145, The NIST Definition of Cloud Computing, September 2011, Page 2.
[27] National Institute of Standards and Technology (NIST), Special Publication 800-145, The NIST Definition of Cloud Computing, September 2011, Page 3.
[28] National Institute of Standards and Technology (NIST), Special Publication 800-145, The NIST Definition of Cloud Computing, September 2011, Page 2.
[29] Cf. paras. 39 and 40 below. The cloud service provider's subcontractors in connection with the processing of personal data are also considered processors.

are being accumulated and concentrated;
d. the technology is boundless and transboundary[30];
e. data processing has become global;
f. transparency is lacking with respect to cloud service provider processes, procedures and practices, including whether or not cloud service providers sub-contract any of the processing and if so, what their respective processes, procedures and practices are;
g. this lack of transparency makes it difficult to conduct a proper risk assessment;
h. this lack of transparency also makes it more difficult to enforce rules regarding data protection;
i. cloud service providers are under great pressure to quickly capitalise significant investment costs;
j. cloud customers are under increasing pressure to reduce costs, including those of their data processing, in part accelerated due to the global financial crisis; and
k. to keep low prices cloud service providers are more likely to offer standard terms and conditions.

These circumstances may lead to an increased risk of:

A. breaches of information security such as breaches of confidentiality, integrity or availability of (personal) data unnoticed by the controller;
B. data being transferred to jurisdictions that do not provide adequate data protection;
C. acts in violation of laws and principles for privacy and data protection;
D. the controller accepting standard terms and conditions that give the cloud service provider too much leeway, including the possibility that the cloud service provider may process data in a way that contradicts the controller's instructions;
E. cloud service providers or their subcontractors using the controllers' data for their own purposes without the controllers' knowledge or permission;
F. accountability and responsibility seemingly fading or disappearing in a chain of subcontractors;
G. the controller losing control of the data and data processing;
H. the controller or its trusted third party (e.g. auditor) being unable to properly monitor the cloud service provider;
I. data protection authorities being precluded from properly supervising the processing of personal data by the controller and the cloud service provider; and
J. the controller relying on unfounded trust in the absence of insight and monitoring, thereby potentially contravening the data protection legislation in force in the country of establishment.

The following recommendations are intended to help reduce risks associated with the use of cloud computing services and to promote accountability and proper governance[31], so that the benefits of utilising CC can be achieved, but not at the expense of the rights of the individual.

Recommendations[32]

General recommendations

The Working Group recommends that:

- Cloud computing must not lead to a lowering of data protection standards as compared with conventional data processing;
- Data controllers carry out the necessary privacy impact and risk assessments (if necessary, by using trusted third parties) prior to embarking on CC projects;
- Cloud service providers further develop their practices in order to offer greater transparency, security, accountability and trust in CC solutions in particular regarding information on potential data breaches and more balanced contractual clauses to promote data portability and data control by cloud users;

[30] Cf. para. 38.
[31] On pages 9-10 of Cloud Computing – Benefits, risks and recommendations for information security, November 2009, ENISA lists the top security risks, in random order, as: loss of governance, lock-in, isolation failure, data protection, insecure or incomplete data deletion, malicious insider. For details see the publication. Loss of governance is emphasised here.
[32] The list of recommendations is not exhaustive.

7 Annexes

- Further efforts be put into research, third party certification, standardisation, privacy by design technologies and other related schemes in order to achieve a desired level of trust in CC;
- Legislators reassess the adequacy of existing legal frameworks allowing cross-border transfer of data and consider additional necessary privacy safeguards in the era of CC[33], and
- Privacy and Data Protection Authorities continue to provide information to data controllers, cloud service providers and legislators on questions relating to privacy and data protection issues.

Additional guidance on best practices

1. CC implementation should take place in careful, measured steps, starting with non-sensitive and non-confidential information.
2. The processing of sensitive[34] data via CC raises additional concerns. Therefore without prejudice to national laws such processing requires additional safeguards.
3. **Location audit trails** should be made available to controllers and DPAs. The audit trail should be recorded automatically and show the physical locations in which personal data have been stored or processed and when[35].
4. **An automatically recorded copying and deletion audit trail** should be established, showing clearly which copies of personal data the processor or its subcontractors have created and deleted.
5. The location audit trail and the copying and deletion audit trails should also include backup.
6. Effective **technical measures** should be developed against personal data illegally being transferred to jurisdictions without sufficient data protection.
7. It should be ensured that **deletion** of personal data from disks and other storage media can be executed in an effective way, e.g. through **immediate overwriting with random data**[36].
8. It should be ensured that personal data at rest and in transit[37] are **encrypted** using recognised standard algorithms and contemporary key lengths. The encryption keys should not be used by, or be accessible to anyone other than the controller and cloud service provider. The encryption keys should not be used by, or be accessible to other customers of the cloud service provider. Data should not be available in unencrypted form longer and more extensively than

[33] Cf. International Conference of Data Protection and Privacy Commissioners: International Standards on the Protection of Personal Data and Privacy ("Madrid Resolution"), 5th November 2009; http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_M adrid/estandares_resolucion_madrid_en.pdf

[34] The concept of sensitive data carries different meanings in different legal cultures, cf. Art. 8 of Directive 95/46/EC, Art. 9 EU Draft General Data Protection Regulation and the FTC Report "Protecting Consumer Privacy in an Era of Rapid Change" (2012).

is absolutely necessary for the data processing process at hand. Methods rendering data unreadable to CC providers at any given time should be further explored[38]. It could be useful to explore options by which the controller can effectively and quickly cut off the cloud service provider or its subcontractors from decrypting data (an emergency brake).

9. There should be automatic **logging** of all uses of personal data by cloud providers and their subcontractors. The log should be easily accessible to the controller and be designed in a simple, readily understandable form. The cloud service provider and its subcontractors should ensure the integrity of the logs.

Controller

10. In the agreement with the cloud service provider, the controller should secure a complete list of information in advance about all physical locations in which, throughout the duration of the agreement, data may be stored or processed by the cloud service provider and/or its subcontractors, including backup **(principle of location transparency)**.
11. In the agreement, the controller should ensure that neither the cloud service provider nor its subcontractors transfer data to locations other than the physical locations listed in the contract, regardless of their reason for so doing, and regardless of whether the data are encrypted. This should be supported by technical measures whose existence and dependability the controller has an actual ability to inspect.
12. The controller should ensure that the agreement with the cloud service provider does not contain ambiguities or room for interpretations which undermine the principle that the cloud service provider only processes personal data according to the controller's instructions. Should cloud service providers be able to unilaterally change the agreement the controller should have the right to terminate the contract and to transfer the data to a different cloud service provider.
13. The agreement should explicitly state that the cloud service provider may not use the controller's data for the cloud service provider's own purposes.
14. The controller should have the opportunity to inspect or have inspected all locations that process personal data wholly or partially in the present or have done so in the past, or may do so in the future under the agreement. The agreement should specify that the controller has the right to obtain full insight into all aspects of the cloud service provider and its subcontractors that the controller deems necessary to ensure compliance with the agreement, including ensuring that processing of personal data is done according to instructions, is done legally and in a suitably secure manner.
15. In the agreement, the controller should secure the right to let a trusted third party (e.g., a recognized auditing firm)[39] wholly or partially monitor the processing of personal data by the cloud service provider and its subcontractors, if any.
16. Prior to the use of CC, the controller should perform a **risk assessment** based on insight into the specific conditions and circumstances under which personal data will be processed by the cloud service provider and its subcontractors, if any. The risk assessment should include all of the locations

---

[35] E.g. the location audit trail could provide a clear overview of when the individual personal data are checked in and checked out at the individual locations, as well as when and to which location they are transferred.

[36] Deletion by dereference of data and later overwriting by reuse of the storage areas is generally not sufficient, as it opens the possibility that data become accessible again by renewed reference before or during the reuse of the storage areas.

[37] For data in transit end-to-end encryption should be applied. It must be ensured that personal data in transit is protected against active (e.g. replays, traffic injection) and passive attacks (e.g. eavesdropping). Furthermore, access to data in rest by unauthorised parties must be prevented via corresponding technical and organizational mechanisms (e.g., access control, encryption of the data).

[38] An example of research in this area is the Sealed Cloud initiative, which is presented in the preprint paper Sealed Cloud - a novel approach to defend insider attacks by Hubert A. Jäger and Arnold Monitzer. The preprint is available from http://uniscon.de/pdf/Sealed_Cloud_Jaeger_Monitzer.pdf

[39] For more on trusted third parties, refer to section 44.

at which personal data are processed or stored. If the cloud service provider uses subcontractors for parts of the processing, the risk assessment should also include all locations used by the subcontractors.

17. The controller should regularly review and update the risk assessment as long as personal data are processed by the cloud service provider.
18. Before use of CC, the controller should consider ensuring that there is a real exit option with the cloud service provider, including an active role in the transfer of data by the cloud service provider, in order not to become dependent on the cloud service provider (lock-in).
19. The controller should consider whether it is necessary to secure access to at least one usable copy of data outside of the cloud service provider's (and its subcontractors') control, reach or influence. If this is deemed necessary, the copy should be accessible and usable by the controller independently of the cloud service provider's and its subcontractors' participation.
20. The controller should be able to fully fulfil its obligations towards data subjects and Data Protection Authorities in case of a **data breach** and take appropriate actions accordingly. As such, the controller should make clear agreements with the cloud service provider regarding a prompt and complete notification of the controller and/or Data Protection Authority in case of such a data breach.
21. The controller should contractually oblige the cloud service provider to implement effective and prompt procedures so that the data subjects can exercise their rights of access, rectification, erasure or blocking of data.

Cloud service provider

22. The cloud service provider should establish full transparency for the controller regarding the locations used for data processing and storage of personal data by the cloud service provider and its subcontractors, if any.
23. The cloud service provider should establish full transparency regarding the subcontractors used and what processing they perform for the cloud service provider.
24. The cloud service provider should provide transparency

in contractual matters and refrain from offering CC on standard terms and conditions that allow for unilateral contract changes.

25. Cloud service provider and their subcontractors, if any, are encouraged to follow best practice and allow an impartial third party to conduct a comparison and assessment thereof (benchmarking).
26. Standard terms and conditions offered to certain market segments, e.g. small and medium enterprises should be drafted in such a way that respect of privacy and appropriate safeguards are taken into account.

Auditing

27. Given the possibility of very large accumulations of personal data by the cloud service provider, the cloud service provider should be subject to third-party audits in addition to the audit performed by the controller in the controller's own interest. The auditor should be fully independent of the cloud service provider and should pay special attention to the security aspects of processing of personal data. In particular, the auditor should check whether measures regarding the following are in place and functioning properly: location audit trail (see section 3), copying and deletion audit trails (see section 4), deletion (see section 7), and logging (see section 9). Further, the auditor should check that the following are in place and functioning properly: measures to prevent the illegal transmission of data to jurisdictions with insufficient data protection (see section 6) and measures to prevent the transmission of data to other locations than those explicitly agreed with the customer (see sections 10 and 11). Lastly, the auditor should ensure that it is not possible for the cloud service provider or its subcontractors, if any, to circumvent these measures undetected.

Background for the recommendations

28. CC is a relatively **new paradigm** for data processing, evolving from what, for lack of a better term, is now being referred to as **traditional data processing**. Many years of solid experience with traditional data processing have accumulated, whereas there is no similar solid experience with CC.
29. The consequence of the **paradigm shift** is that basic assumptions, experiences, ideas, theories and models for data processing no longer correspond to the practice, and therefore must be subjected to critical reflection, reassessment and possible revision. This also applies to privacy and data protection of personal data and how **risks** can be analysed, assessed and judged. What was best practice yesterday is not necessarily best practice today.
30. The **new situation** must be examined and implemented with **carefully measured steps**, particularly with regard to privacy and data protection, and protection of the rights of the data subject in a wider sense.
31. The **technical foundation** of CC is well-developed network technology and virtualisation of servers. This enables quick dynamic relocation of data and data processing among servers locally in the individual cloud data centre and globally among cloud data centres in countries around the world. The technology is highly scalable without creating limiting bottlenecks. The internet allows the end user to access the data regardless of where

Annexes

the cloud data centres are located.

32. The **economic driving force** behind CC is **economics of scale**. Consolidating data processing in large centres improves the utilisation of expensive resources such as: human knowledge, tangible capital (HW, SW, buildings), communication bandwidth and energy. In addition, due to their size and volume, cloud service providers have significant bargaining power when purchasing resources. Cloud service providers can therefore reduce unit costs and offer attractive prices to customers. The prerequisite for achieving economics of scale is many customers in "the store". To achieve sufficient volume, CC services are offered globally via the internet.
33. CC is considered to provide important opportunities for small and medium enterprises to have access to affordable and scalable computing resources. Due to the large number of relatively small entities, it is expected that cloud service providers will develop standard terms and conditions for this market segment.
34. CC is far more dynamic than traditional data processing. The location where data processing takes place can change dramatically. The current location of data and where it is processed can depend on a variety of factors to which end users and data controllers traditionally have given little thought, and into which they do not necessarily have the insight or ability to control. For example, cloud service providers often choose to locate their data centres across many countries and several continents, based on the availability of cheap electricity, a cool local climate and time zone differences, among other factors. Unpredictable circumstances can also impact the current location of data, such as interruptions in one data centre or a lack of capacity at peak periods (overflow). Copies of data can be transferred to other data centres to ensure online accessibility in case of interruptions in one data centre or for the purpose of making backups (redundancy).
35. CC is based on many cloud customers dynamically sharing a common pool of the cloud service provider's resources. This should only take place if it is possible to maintain **robust separation** of the

different cloud customers' data and their processing. Resource sharing entails an increased risk of large scale losses or unauthorised disclosure of data.[40] The risk is further enhanced by the fact that CC is driven by cost optimisation based on high volume (economics of scale). Cloud customers constitute a risk to each other. The more customers sharing the same resources, the greater the risk for each individual customer, and thus for cloud customers as a whole.

36. Knowledge about CC and insight into its risks are currently concentrated among relatively few large cloud service providers, who for commercial and competitive reasons appear to be reluctant to give the world insight into specific conditions and circumstances. The uneven distribution of knowledge and insight between cloud service providers and customers places the latter in a weak position when entering into agreements and makes it difficult for them to properly assess risks associated with the intended use of CC.
37. A thorough **risk assessment** must be based on **insight** into the concrete setup and circumstances of the cloud service provided at all of the locations where data processing will take place.
38. CC technology is **boundless** and **transboundary**. The global customer base, in tandem with the global distribution of cloud data centres and dynamic movement of data (and data processing), can result in data crossing national borders and changing jurisdictions with a corresponding lack of transparency. Personal data may end up in data centres in jurisdictions with inadequate data protection or personal data may be misused commercially or be accessed without authorisation by foreign powers[41].
39. A distinction must be made between the two mutually exclusive roles of controller and processor within data protection. The controller is the one who determines the purpose and means used for a specific act of data processing.
40. It is also widely acknowledged that a controller may allow the processing of personal data to be performed by a **processor** but only in accordance with the controller's explicit **instructions**.
41. A commonly recognised data protection principle is that the processor must not process personal data to a greater extent than that which follows from the explicit instructions from the controller.[42] For CC, this implies that a cloud service provider cannot unilaterally make a decision or arrange for personal data (and its processing) to be transmitted more or less automatically to unknown cloud data centres. This is true whether the cloud service provider justifies such a transfer as a reduction of operating costs, management of peak loads (overflow), load balancing, copying to backup, etc. Nor may the cloud service provider use personal data for his own purposes.[43]
42. Another generally recognised data protection principle requires that the controller implement appropriate **technical and organisational security measures** to protect data against accidental or unlawful destruction, loss or deterioration and against unauthorised disclosure, abuse or other processing in violation of the provisions laid down by the law. The same applies for processors.
43. Fulfilment of the controller's responsibility requires that the controller **monitor** the

---

[40] On pages 9-10 of Cloud Computing – Benefits, risks and recommendations for information security, November 2009, ENISA lists the top security risks, in random order, as: loss of governance, lock-in, isolation failure, data protection, insecure or incomplete data deletion and malicious insider. For further details, refer to the publication; here it should be emphasised that isolation failure is considered a top risk.

[41] Whilst personal data may be processed within one jurisdiction, the cloud provider, or parent company, may also be established within another jurisdiction thereby allowing foreign law enforcement powers access to the data within the cloud service even though that data physically resides outside the geographical boundaries of that country. An international agreement may be required to address this issue.

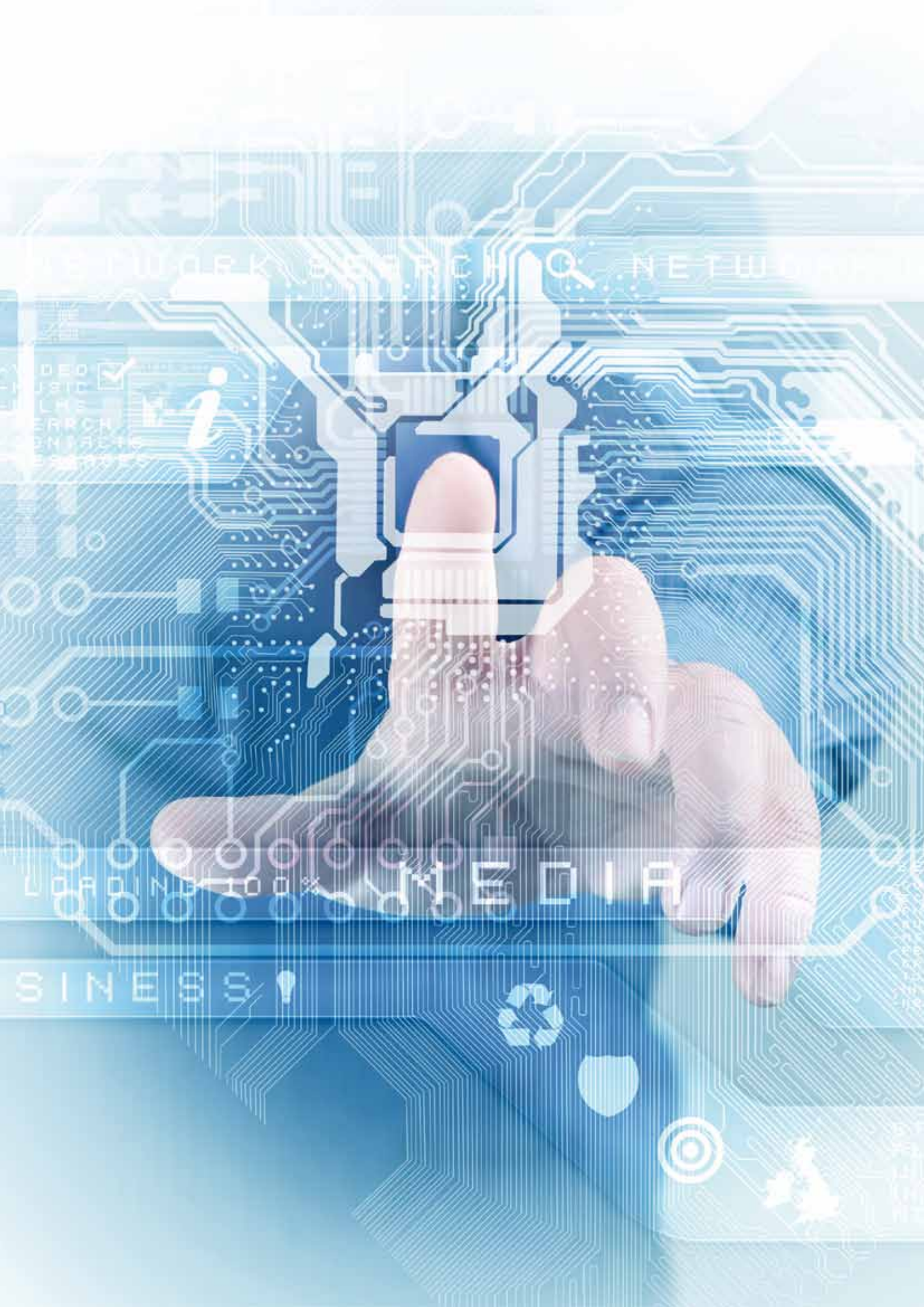
[42] Or by legislation.

[43] If cloud service providers process data without the knowledge of the controller, the cloud service provider should be seen as a co-controller and as such be held accountable for the unauthorised independent processing of data.

processing by the processor to ensure that it takes place according to the controller's instructions and that the processing is done with adequate security.

44. Without removing his liability, the controller can give explicit instructions that monitoring of processing by the processor be partially performed by a **trusted third party** (e.g. auditor). The prerequisite is that the third party has the necessary qualifications, is independent of the processor, has full access to and insight into the actual conditions and circumstances under which processing by the processor takes place and can reliably report his observations, assessments and conclusions to the controller.

The Working Group will continue to monitor developments in the area of cloud computing and update this paper as necessary.



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