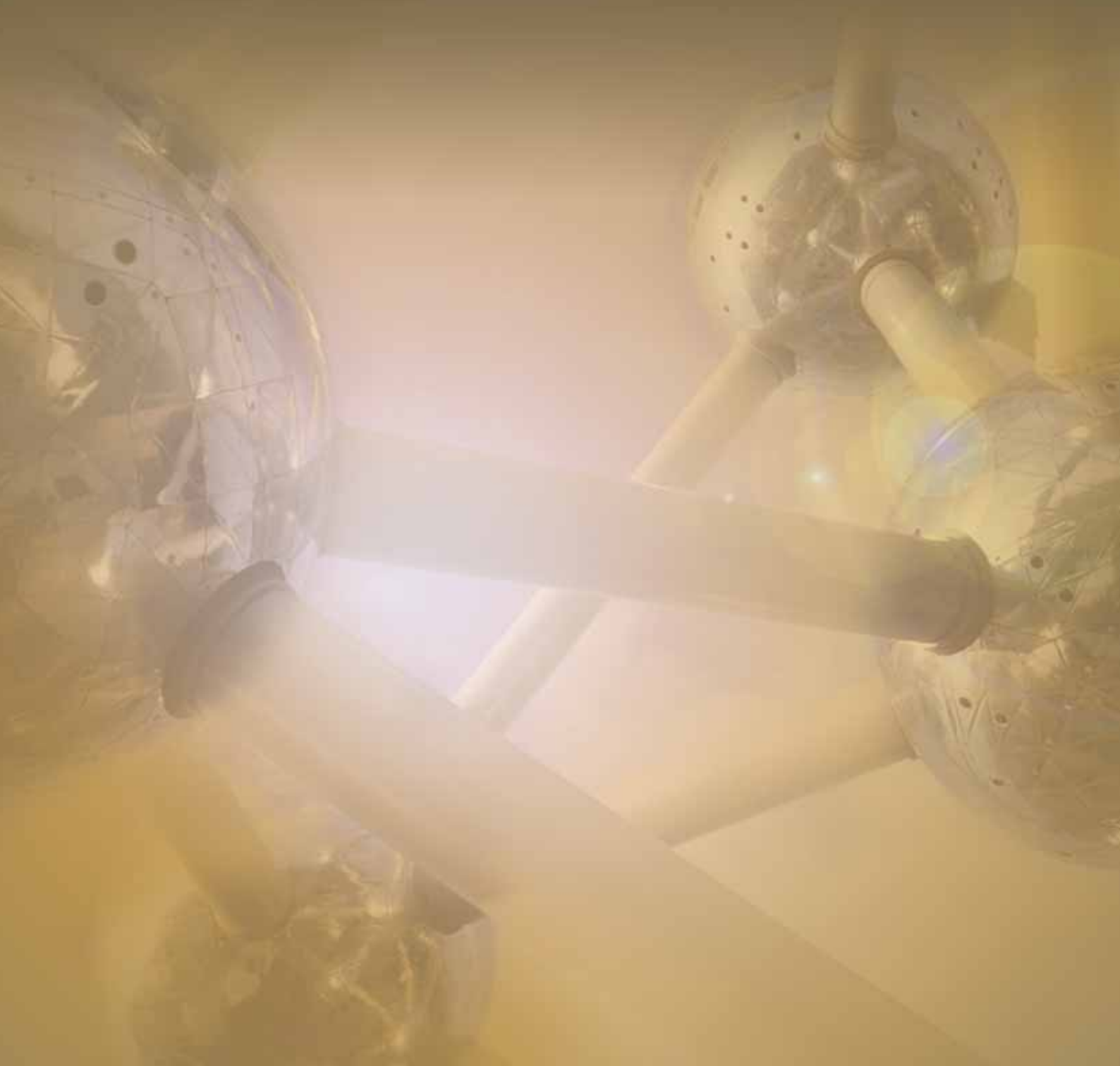
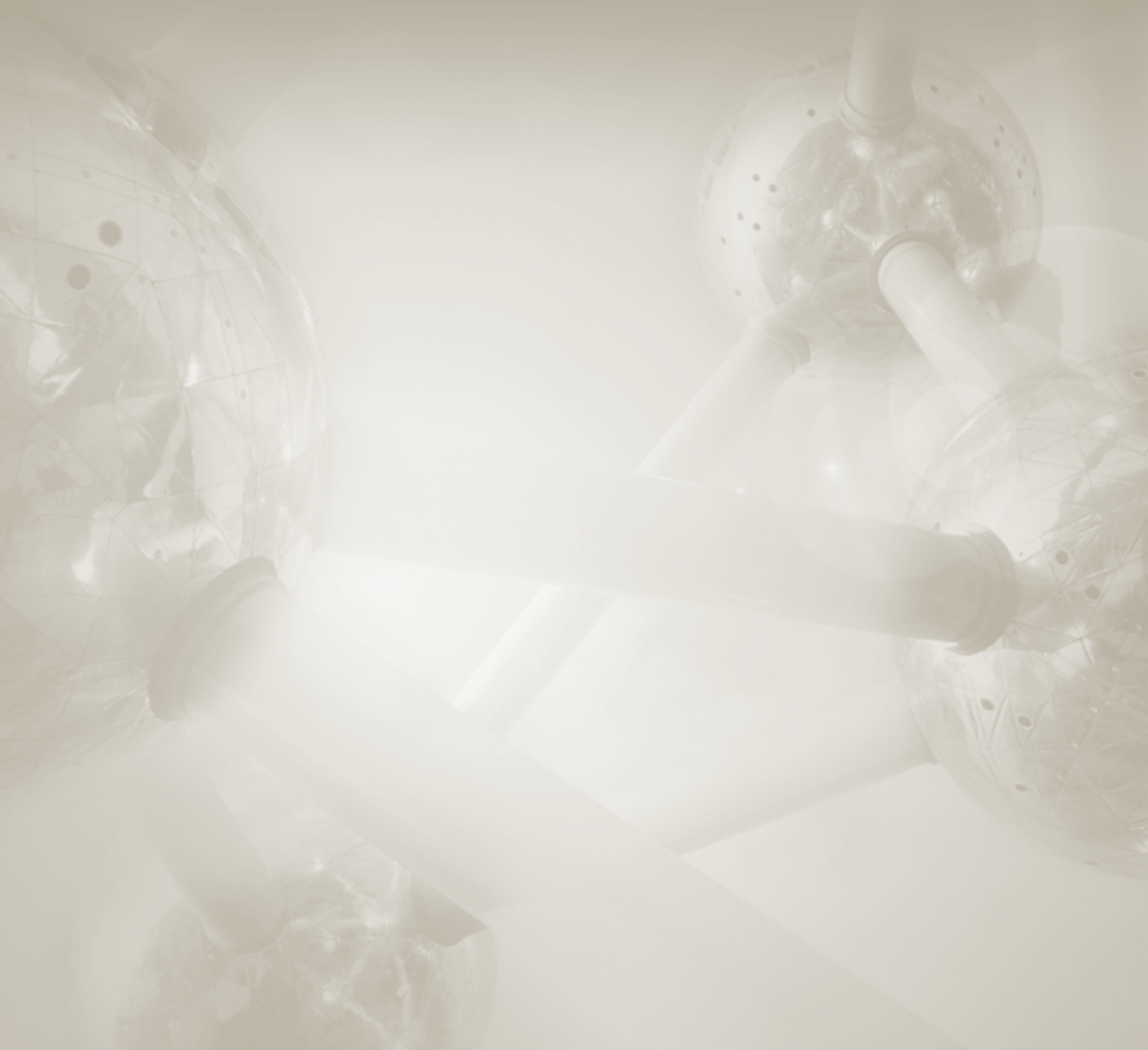


Rapport Annuel 2008





Rapport annuel 2008



Préface

L'arbre cacherait-il la forêt ? À force de se concentrer sur les détails du fonctionnement quotidien de la Commission et de son Secrétariat, nos rapports annuels n'omettraient-ils pas d'esquisser les grandes tendances qui se dessinent lentement mais sûrement au fil des ans. Cette année, j'ai donc décidé de m'arrêter sur quelques-unes de ces "tendances".

Lors des séances de la Commission des 19 mars et 2 avril 2008, nous nous sommes ainsi penchés sur l'avant-projet de loi portant création et organisation de la plate-forme eHealth.

Pour la Commission, l'examen de cet avant-projet de loi représentait un exercice aussi important que délicat. Le monde des soins de santé est en effet de plus en plus confronté au problème du traitement respectueux et transparent des données à caractère personnel.

Si le secret professionnel constitue un des principes phares des soins de santé, ce n'est pas par hasard. Le serment d'Hippocrate constitue non seulement un texte de base classique de la déontologie médicale, il est aussi la plus ancienne règle qui accorde une place centrale au respect de la vie privée.

L'époque où les relations entre le médecin et ses patients étaient des relations personnelles sans équivoque, un colloque singulier, est belle et bien révolue.

Le travail d'équipe, la spécialisation, l'élargissement, le suivi, le rapportage et la justification des soins inhérents à l'échange électronique des données relatives aux patients font du secret médical un secret plus que jamais "partagé". Les données à caractère personnel contenues dans tous ces flux de données doivent donc être protégées et ceci au niveau de nombreuses personnes et de nombreuses transactions. À cela s'ajoute encore qu'on dispose aujourd'hui de données parfois très nombreuses et détaillées qui permettent non seulement de remonter de plus en plus loin dans les générations mais aussi de procéder à des prédictions très concrètes. Ces évolutions représentent autant de défis, non seulement sur le plan de l'éthique et de la déontologie mais aussi sur celui des techniques d'échange des données en général et de la protection de la vie plus particulièrement.

La constatation que la législation BeHealth se limitait à ne proposer qu'une base générale acceptable pour ce type de traitement de données a débouché sur l'identification de la nécessité de pren-

dre un nouveau départ dans ce domaine, basé sur d'autres points de vue et d'autres techniques. Entretemps, on s'est aussi rendu compte que le format "banque carrefour" permettait de résoudre une partie des problèmes liés à la sécurité de ces échanges. Bien sûr : *"the proof of the pudding is in the eating"*. Pour voir s'il répond vraiment aux attentes et aux exigences en matière de garantie, de performance et de protection de la vie privée, il nous faudra donc attendre son application concrète. La Loi eHealth qui prévoit un débat d'évaluation deux ans après son entrée en vigueur est une bonne initiative mais aussi une initiative à suivre.

Lors des séances citées plus haut, la Commission a aussi accepté l'utilisation du numéro du Registre national. Ce faisant, la Commission a abandonné son ancien point de vue, celui qui lui faisait exiger un identifiant de santé spécifique et refuser un identifiant général unique comme le numéro du Registre national. Ce qui a fait changer la Commission d'avis, c'est l'efficacité et la précision liées à l'utilisation de cet identifiant ainsi que les garanties maximales qu'il offre en termes d'identification unique. Un autre élément important dans ce cadre a aussi été le fait que les systèmes d'identification basés sur d'autres identifiants ne se sont pas avérés jusqu'ici apporter le niveau de protection qu'on en attendait.

Sur le plan législatif, la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth (M.B. 13 octobre 2008) peut être considérée comme un des actes législatifs les plus importants.

Sur le plan de la police et de la justice, après des années de discussion, 2008 a vu approuver une nouvelle réglementation européenne concernant cet important troisième pilier : l'Arrêté-cadre 2008/977/JI du Conseil du 27 novembre 2008 ne sera pas, certes, le nouveau texte de référence mais il a au moins le mérite d'exister. Il ne lui reste plus maintenant qu'à faire ses preuves. Tout cela, dans l'attente, bien sûr, de l'entrée en vigueur du Traité de Lisbonne censé mettre de l'ordre dans la répartition des piliers.

En 2008, les choses ont aussi bougé au niveau régional : outre le Décret du Parlement flamand du 18 juillet 2008 relatif à l'échange électronique de données administratives, je mentionnerai aussi la création de la première instance publique flamande de protec-

tion de la vie privée, la Commission de contrôle, dans le cadre du système de traitement des informations relatives à la santé, par l'Arrêté ministériel du 4 novembre 2008. Cette évolution dote chaque niveau administratif de ses propres contrôleurs. On ne peut pas dire que la création de cette nouvelle instance enchante la Commission. Ceci, d'une part parce qu'elle exigera la mise en place d'une coordination et d'autre part parce ce qu'elle implique des risques de chevauchements et d'hiatus. La Commission demande donc la mise en place au niveau politico-institutionnel, de la possibilité de mener une politique de la protection de la vie privée intégrée et cohérente qui respecte les compétences et les points de vue de chacun.

Le fait qu'après le secteur public, les entreprises aussi s'intéressent de plus en plus à la protection de la vie privée est une nouvelle tendance, significative aussi. En 2008, la Commission a reçu nettement plus de demandes du secteur privé. Cette situation traduit l'intérêt croissant pour les questions relatives à la protection de la vie privée et le confort. Cette année, la Commission a aussi porté un intérêt particulier aux questions structurées du monde économique. Des rencontres ont été organisées avec ADM Legal et l'Institut belge des juristes d'entreprise et la Commission a également participé à plusieurs journées d'étude et de formation professionnelle destinées aux juristes.

L'avis de la Commission est aussi de plus en plus sollicité sur des problèmes relevant du secteur non public : les limites et les possibilités du marketing direct ont ainsi été étudiées en détail et, pour la première, fois ce sujet a fait l'objet d'une enquête structurée menée auprès des différents protagonistes du secteur. Ce projet est toujours en cours et pourra déboucher sur une initiative conjointe.

L'intérêt porté par les organismes non publics au traitement des données à caractère personnel a très certainement aussi été aiguë par l'affaire SWIFT. Pour de nombreux consultants et responsables d'entreprise, cette affaire a clairement montré qu'outre la pure compliance et la seule sécurité, la vie privée, vaut, elle aussi, la peine d'être protégée dans le cadre du traitement des données. Un élément très important de cette évolution a été le fait que le 9 décembre 2008, la Commission a pu décider d'arrêter la procédure de recommandation et qu'elle a pu inscrire la déclaration de certains traitements de données à caractère per-

sonnel par SWIFT dans le registre public.

Sur le terrain aussi, l'utilisation des nouvelles technologies soulève de plus en plus de questions, surtout en ce qui concerne la biométrie et le cybercontrôle. On a besoin d'informations précises mais par honnêteté, force nous est de concéder que même la Commission et son Secrétariat ne sont pas toujours en mesure d'apporter une réponse technique ou juridique acceptable pour tous, voire même seulement raisonnable, à toutes les questions individuelles ou plus générales qui lui sont soumises.

En 2008, nous nous sommes aussi attentivement penchés sur les nombreuses questions soulevées dans le domaine de la recherche scientifique. Ces questions ont mené à une discussion avec le monde de la recherche à des fins statistiques, à l'élaboration d'un code relatif aux demandes d'informations au Registre national, à la publication d'un vade-mecum de la recherche scientifique en général, à l'organisation d'une journée d'étude sur la recherche historique avec CEGES-SOMA en collaboration avec les Archives générales du Royaume et à une réunion d'information avec des institutions scientifiques, parmi lesquelles des universités, sur le traitement des données à caractère personnel dans la recherche, dans le cadre de laquelle, il ne faut en tout cas pas oublier le monde déjà cité de la recherche médicale.

En octobre 2008, la Commission et son Secrétariat ont intensivement participé à la trentième Conférence mondiale sur la protection de la vie privée et des données à caractère personnel organisée par les autorités de contrôle françaises et allemandes à Strasbourg. Lors de cette conférence, nous avons, une fois de plus, été confrontés au fait que ce récent domaine de travail dans notre société reçoit de plus en plus de questions sur de nombreux processus et de nombreuses pratiques sociétales et ceci dans le cadre d'une préoccupation croissante d'autonomie et de dignité humaine. Parce que finalement, c'est bel et bien de cela qu'il s'agit : protéger et renforcer la spécificité de chaque être humain et de son environnement, quels que soient son aspect, son pouvoir, sa richesse, son art, ses connaissances, son origine ou sa nationalité. Contribuer, pas à pas, à cette noble mission, c'est ce qui nous motive!

Willem Debeuckelaere
Président

Table des matières

Première partie : la Commission	8		
1 La mission de la Commission	9		
2 Les domaines d'activité de la Commission	11		
2.1 Réglementation et encadrement normatif	11		
2.2 Politique de respect des dispositions légales	11		
2.3 Information	11		
2.4 Assistance	12		
2.5 Traitement des plaintes	12		
2.6 Au niveau international	13		
3 La composition de la Commission	14		
3.1 Membres effectifs	14		
3.2 Membres suppléants	14		
4 La structure de la Commission	15		
4.1 Profil des membres	15		
4.2 Mandats des membres	15		
4.3 Fonctions des membres	15		
4.4 Rôle du président	15		
4.5 Comités sectoriels	15		
4.6 Secrétariat	15		
5 La structure de l'administration	16		
6 Le plan de gestion de la Commission	17		
6.1 Nouvelle vision/mission	17		
6.2 Intégration des comités sectoriels	17		
6.3 Un Règlement d'ordre intérieur pour le Comité sectoriel de la Banque-Carrefour des Entreprises	17		
6.4 Contrôle de la vie privée – Évaluation	18		
6.5 Information au public	18		
6.6 Vie privée & recherche scientifique	18		
7 Les principales activités nationales de la Commission	19		
7.1 Autorités et organes publics	19		
7.1.1 L'échange électronique de données administratives	19		
7.1.2 Les données conservées par certains centres de prêt public sur leurs lecteurs	19		
7.1.3 La gestion des accès et des utilisateurs	20		
7.1.4 Les listes d'inscription des écoles secondaires de la communauté française	21		
7.1.5 L'Intégrateur de services fédéral	22		
7.1.6 La geografische Data-Infrastructuur Vlaanderen	23		
7.1.7 Le Centraal Referentieadressenbestand	23		
7.2 Démographie et diversité	24		
7.2.1 La Generations and Gender Panel Study	24		
7.2.2 Le monitoring des groupes à potentiel du VDAB	25		
7.2.3 Étude sociologique sur les (candidats-) locataires	26		
7.3 Recherche et développement	27		
		7.3.1	Réutilisation des données administratives à des fins de recherche 28
		7.3.2	Code de bonne conduite pour les chercheurs qui travaillent avec des données du registre national 29
		7.4	Justice et sécurité 29
		7.4.1	Proposition de loi sur les certificats de bonne vie et mœurs 30
		7.4.2	Modification de loi sur la conservation des données pour enquête sur des faits punissables 31
		7.4.3	Communication de données sur des personnes condamnées au pénal 31
		7.4.4	Développements de la Loi caméras 32
		7.5	Sport et vie privée 33
		7.6	Droit de propriété et vie privée 34
		7.7	Transport et mobilité 34
		7.7.1	Accès au fichier de données de la DIV 35
		7.7.2	Création d'un nouveau fichier central de données relatives aux véhicules 35
		7.8	Listes négatives et vie privée 37
		7.9	Technologie de l'information et de la communication 38
		7.9.1	Les activités du Bureau de Normalisation 38
		7.9.2	La plateforme de concertation sur la protection des informations 38
		7.10	Finances et vie privée 39
		7.10.1	Exonération partielle des obligations imposées par la Loi vie privée pour la CBFA 39
		7.10.2	Modification dans la réglementation de la Centrale des crédits aux particuliers (CCP) 39
		7.10.3	Recherche des titulaires de comptes et coffres dormants 39
		7.11	Amélioration des services de la Commission 40
		7.11.1	Note juridique sur le marketing direct 40
		7.11.2	Traduction du site web en anglais 41
		8	Les principales activités internationales de la commission 42
		8.1	Conférences internationales 42
		8.1.1	Conférence européenne des Commissaires à la protection des données – "What outlook for privacy in Europe and beyond?" 42
		8.1.2	Conférence mondiale des Commissaires à la protection des données - "Protecting privacy in a borderless world" 42
		8.1.3	Conférence de l'AFAPDP 44
		8.2	Groupe de travail Article 29 45
		8.2.1	Groupe de travail Article 29-Groupe de protection des données 45
		8.2.2	Technology Subgroup 47
		8.3	Comité consultatif de la Convention 108 48
		8.4	IWGDPT 48
		8.5	WPPJ 49
		8.6	Organes de contrôle communs 49
		8.6.1	Schengen 49
		8.6.2	Europol 51
		8.7	L'affaire SWIFT 52
		9	Les activités de la Commission en chiffres 53
		9.1	Réglementation et normalisation 53
		9.2	Politique de respect des dispositions légales 53
		9.3	Information 54
		9.4	Assistance 55

9.5	Traitement des plaintes	56
9.6	Tableaux et graphiques	57
9.6.1	Autorisations et avis	57
9.6.2	Plaintes et information : les dossiers IP en chiffres	60
9.6.3	Crédit à la consommation : les dossiers IC en chiffres	65
9.6.4	Accès indirect : les dossiers I3 en chiffres	68
9.6.5	Déclarations et registre public : les dossiers I8 en chiffres	72
9.6.6	Contrôle : les dossiers C en chiffres	75
9.6.7	Les déclarations en chiffres	78
9.6.8	Appels téléphoniques traités par le front office	81
9.6.9	Analyse comparative : 2007 - 2008	83
Deuxième partie: les comités sectoriels		84
1	La composition des comités sectoriels	85
1.1	Comité sectoriel du Registre national	85
1.2	Comité sectoriel de la Sécurité Sociale et de la Santé	86
1.3	Comité sectoriel pour l'Autorité Fédérale	86
1.4	Comité sectoriel de la Banque-Carrefour des Entreprises	87
1.5	Comité de surveillance sectoriel Phenix	87
1.6	Comité de surveillance statistique	87
2	Les principales activités des comités sectoriels	89
2.1	Comité sectoriel de la Banque-Carrefour des Entreprises	89
2.2	Commission loco le Comité de surveillance statistique	89
2.3	Comité sectoriel du Registre national	90
2.4	Comité sectoriel pour l'Autorité Fédérale	92
2.5	Comité sectoriel de la Sécurité Sociale et de la Santé	94
3	Les activités des comités sectoriels en chiffres	98
3.1	Le Comité sectoriel de la Sécurité Sociale et de la Santé	98
3.2	Le Comité sectoriel pour l'Autorité Fédérale	98
3.3	Le Comité sectoriel du Registre national	98
3.4	Le Comité sectoriel de la Banque-Carrefour des Entreprises et le Comité de surveillance sectoriel Phenix	98
3.5	Tableaux et graphiques	99
3.5.1	Avis et autorisations du Comité sectoriel de la Sécurité Sociale et de la Santé	99
3.5.2	Avis et autorisations de la Banque-Carrefour des Entreprises	99
3.5.3	Avis et autorisations du Comité sectoriel pour l'Autorité Fédérale	99
3.5.4	Avis et autorisations du Comité sectoriel du Registre national : les dossiers RN en chiffres	99

Première partie : la Commission

1 La mission de la Commission

La Commission est un organe indépendant.

Elle gère le traitement de données à caractère personnel.

Elle s'adapte aux évolutions de son temps.

Ses mots d'ordre sont rapidité et dynamisme.

La Commission de la protection de la vie privée, dont la dénomination officielle est parfois abrégée en "Commission vie privée", est un organe de contrôle indépendant chargé de veiller à la protection de la vie privée lors du traitement de données à caractère personnel.

Elle a été créée suite à l'adoption par la Chambre des Représentants de Belgique de la Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (Loi vie privée).

Les compétences de la Commission sont vastes et générales. Elle est compétente pour toute forme de traitement de données à caractère personnel, quel que soit le domaine dans lequel s'opère le traitement et quelle qu'en soit la nature : secteur privé ou secteur public, traitement automatisé ou non, etc.

Face aux traitements de données de plus en plus nombreux, à la demande faite aux services publics d'être de plus en plus rapides, au développement de l'e-gouvernement et à la demande de délais d'avis ou d'autorisation de plus en plus courts, la Commission n'a de cesse d'adapter au mieux son mode de fonctionnement.

Tout en répondant aux attentes d'un environnement en mutation rapide et dynamique, la Commission veille aussi au respect de la nécessité de son indépendance et de son autorité, des points qui ont d'ailleurs fait l'objet de la Loi du 26 février 2003 (Moniteur belge du 26 juin 2003) qui visait à accroître son efficacité et ses performances.

Le rôle de la Commission

Sans sa réflexion et ses actes, la Commission de la protection de la vie privée se veut déterminante dans le maintien de l'équilibre du droit fondamental à la protection de la vie privée. Elle reconnaît la nécessité pour notre société de la connaissance de collecter et de traiter des données à caractère personnel en vue de développements tant sociaux qu'économiques et cherche donc, dans le cadre de ses décisions et de ses activités de surveillance du respect de la vie privée à trouver le juste équilibre entre d'une part les besoins sociaux et économiques et d'autre part le droit fondamental au respect de la vie privée des citoyens. La Commission a parfaitement conscience que tout traitement de données implique des risques sur le plan de la protection de la vie privée et souligne donc l'importance de diffuser des informations de sensibilisation aussi bien aux personnes dont les données sont traitées qu'aux responsables des traitements ainsi que de prévoir des garanties, et ceci plus spécialement sur le plan de la protection de l'information. La Commission est par ailleurs attentive au fait que le recours aux technologies de traitement des données à caractère personnel représente un facteur très important dans notre société actuelle en termes d'augmentation du bien-être et de la prospérité des citoyens.

La Commission s'est fixé pour objectif de tout mettre en œuvre pour que les citoyens aient confiance dans ces technologies. Elle rappelle à ce propos la responsabilité de chacun d'agir de manière consciente aussi bien avec ses propres données à caractère personnel qu'avec celles des autres. A cet effet, elle poursuit ses actions de sensibilisation à un comportement conscient et sûr au niveau de la communication et

le traitement des données à caractère personnel. Elle entend également souligner l'importance de garantir et de respecter les droits des personnes concernées dans le cadre du traitement de leurs données à caractère personnel et veut se servir de son ascendant pour encourager les responsables de traitements de données – tant publics que privés – à prendre toutes les mesures qui doivent l'être sur la base d'une analyse approfondie des risques afin de garantir le droit fondamental au respect de la vie privée et familiale.

Dans ce cadre, la Commission vise la reconnaissance de son rôle de leader tant national qu'international. Elle veut marquer de son sceau la conception et l'élaboration de normes pertinentes en matière de sécurité de l'information et de protection de la vie privée ainsi que de leur respect et de leur promotion par le biais de mécanismes de contrôle appropriés.

Afin de formuler une réponse adaptée au caractère de plus en plus international des traitements de données à caractère personnel, la Commission entend se servir de sa position de centre de référence national pour collaborer intensivement avec des partenariats internationaux, et plus spécifiquement des partenariats européens qui développent des activités destinées à protéger les données à caractère personnel. Dans ce cadre, elle veille aussi à l'intégration ad hoc de l'impact de l'internationalisation sur les traitements de données nationaux.

2 Les domaines d'activité de la Commission

Se profiler comme un leader reconnu au niveau national et international.

Faire office de centre de référence.

Développer ses cinq domaines d'activité.

La Commission a pour ambition constante de jouer un rôle de leader en matière de protection de la vie privée, et ceci tant à l'échelon national qu'à l'échelon international. Elle se veut un centre de référence incontournable offrant un maximum de services aussi efficaces que performants.

Pour cette raison, elle participe à l'élaboration de normes pertinentes en matière de sécurité de l'information et de protection de la vie privée. Elle est chargée de développer et de surveiller ces normes et veille à leur bonne application.

Ces différentes tâches destinées à maintenir l'équilibre nécessaire se répartissent en cinq grands domaines d'activité.

La Commission de la protection de la vie privée émet des avis sur la législation et la normalisation, mène une politique d'encadrement normatif, diffuse des informations et offre un soutien informatif, aide les personnes concernées à exercer leurs droits et à respecter leurs obligations, traite les plaintes relatives à des traitements de données qui lui sont soumises et intervient en tant que médiateur le cas échéant pour contribuer à garantir l'équilibre entre le droit fondamental à la protection de la vie privée de chacun et le traitement de données à caractère personnel.

2.1 Réglementation et encadrement normatif

Dans ce domaine, les activités sont surtout axées, d'une part sur les autorités et/ou instances compétentes (avis – article 29 Loi vie privée, recommandations – article 30, § 1^{er} de la Loi vie privée) et, d'autre part sur les responsabilités en matière

de traitement (recommandations relatives au traitement ultérieur – article 21 de l'Arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et codes de conduite).

En siégeant dans des groupes de travail nationaux et internationaux (p. ex. le Groupe de travail Article 29, le Groupe de Berlin, la Conférence des Commissaires ou d'autres organes de contrôle en matière de protection de la vie privée, ...) et de par ses contacts avec des organisations similaires à l'étranger, la Commission met son empreinte sur les processus décisionnels en matière de protection de la vie privée.

2.2 Politique de respect des dispositions légales

Ce pilier couvre un large éventail de tâches et n'est pas seulement axé sur les instances publiques compétentes, mais aussi sur les responsables de traitement. Les compétences de la Commission en matière d'autorisation consistent à accorder à une instance d'un secteur déterminé responsable d'un traitement l'autorisation de procéder à ce traitement et d'obtenir la communication de données à caractère personnel. Toujours à l'égard de ces mêmes responsables, la Commission assume également des tâches de contrôle et d'inspection, émet des recommandations (article 30, § 2 de la Loi vie privée) et évalue les mesures de sécurité qui ont été prises.

2.3 Information

Un troisième pilier d'activité de la Commission est celui de

la mission d'information dont elle est investie, aussi bien à l'égard des instances publiques que des responsables de traitement ou encore des personnes concernées. On retrouve dans ce domaine d'activité : le rapport annuel destiné au Parlement et l'élaboration d'un plan de gestion, la rédaction de son Règlement d'ordre intérieur, la tenue d'un registre public et de manière plus générale, une tâche d'information à l'égard du public (site web, conférences, réponses orientées client, sensibilisation, ...).

Il convient encore de souligner qu'au sein de ces différents domaines d'activité, la Commission ne se limite pas nécessairement au territoire national. Ses actions ont aussi souvent une dimension internationale et la Commission joue un rôle d'information et de sensibilisation important sur la scène internationale.

2.4 Assistance

Ce quatrième domaine d'activité concerne la mission d'information de la Commission. Dans ce cadre, elle s'adresse à tous les groupes cibles :

- les autorités ;
- le secteur privé ;
- le citoyen ;
- le responsable du traitement de données (il peut s'agir d'une personne physique ou d'une personne morale).

Dans ce domaine, les tâches de la Commission comprennent :

- la communication des informations demandées par toute personne, qu'elle soit concernée par un traitement de données ou responsable d'un/de traitement(s) de données ;
- l'exercice du droit d'accès et de rectification (accès indirect) ;
- le traitement des déclarations ;
- la tenue à jour du registre public ;
- la dispense d'informations dans le cadre du traitement des plaintes ;
- la communication des informations demandées par des par-

- ticuliers ou des responsables de traitement de données ;
- l'élaboration d'un rapport annuel destiné au Parlement.

En répondant aux demandes de concertation informelle préalable qui permet de tenir compte des exigences de la Loi vie privée dès la phase de développement des projets, la Commission aide tant les instances publiques que les responsables de traitement. La Commission aide également les personnes dont les données sont traitées à exercer leurs droits, notamment en les informant sur leurs droits et sur la procédure à suivre.

Dans le cadre des échanges internationaux de données, la Commission apporte son soutien aux instances qui exercent des activités transfrontalières, e.a. en collaborant à des groupes de travail internationaux dans lesquels sont élaborées des règles contraignantes relatives à la protection des données à caractère personnel (p. ex. l'élaboration des *Binding Corporate Rules*, ...). A ce niveau, comme au niveau national, la Commission soutient les personnes dont les données sont traitées et intégrées dans des flux de données transfrontières.

2.5 Traitement des plaintes

Ce domaine d'activité concerne plus particulièrement les citoyens dont les données sont traitées. Il englobe le traitement des plaintes et l'éventuelle procédure de médiation qui peut y être liée. Lorsque les droits d'un citoyen dont les données font l'objet d'un traitement ne sont pas respectés par le responsable du traitement, la Commission intervient à la demande de l'intéressé pour faire respecter ses droits (droit d'opposition, de rectification, d'accès indirect, ...). Pour cela, la Commission met en œuvre les moyens dont elle dispose (déclaration au procureur du Roi, action devant le tribunal civil, ...).

Lorsqu'il s'agit d'infractions internationales relatives à la protection des données, la Commission apporte son concours aux enquêtes internationales destinées à mettre en place des

solutions utiles qui demandent l'engagement de toutes les instances concernées par la protection des données.

2.6 Au niveau international

La Commission fait face à une internationalisation croissante.

Elle siège dans des organismes de contrôle internationaux.

Elle participe à des groupes de travail européens.

Elle fait partie du Groupe de travail Article 29.

Les interventions de la Commission dans ces cinq domaines d'activité ont souvent une portée internationale.

C'est ainsi que la Commission, non seulement siège via ses représentants dans divers organes de contrôle internationaux (Schengen, Europol, etc.) mais participe aussi activement, aux côtés de ses homologues, à des activités organisées au sein d'organisations et de groupes de travail européens et internationaux traitant des aspects politiques et normatifs de la vie privée, notamment : le Groupe de travail Article 29, ou Groupe 29, constitué à l'échelle de l'Union européenne, le Groupe de Berlin, la Conférence des Commissaires ou des organes de contrôle en matière de protection de la vie privée.

Plus l'internationalisation des échanges et des transferts de données s'intensifie, plus le rôle et le statut de la Commission seront appelés, eux aussi, à s'internationaliser.

3 La composition de la Commission

Les membres de l'actuelle Commission ont débuté leurs activités le 2 décembre 2004, après avoir prêté serment entre les mains du Président de la Chambre des Représentants, Monsieur Herman De Croo. Depuis, quelques changements sont intervenus dans la composition de la Commission, notamment suite à la démission de certains des membres initialement désignés.

3.1 Membres effectifs

M. Willem Debeuckelaere (N)	Président
M. Stefan Verschuere (F)	Vice-président
Mme Mireille Salmon (F)	Conseillère à la Cour d'appel de Bruxelles
M. Serge Mertens de Wilmars (F)	Administrateur-gérant de la SPRL Mirea et consultant en organisation
Mme Anne Vander Donckt (N)	Notaire
M. Frank Robben (N)	Administrateur général de la Banque-Carrefour de la sécurité sociale (BCSS) et de la plateforme eHealth
M. Peter Poma (N)	Juge de paix - Canton de Brasschaat
Mme Anne Junion (F)	Avocate

3.2 Membres suppléants

Mme Nicole Lepoivre (F)	Présidente honoraire du tribunal du travail de Huy Présidente suppléante
M. Bart De Schutter (N)	Professeur ordinaire émérite à la Vrije Universiteit Brussel (VUB) Vice-président suppléant Vice-président du Working Party on Police and Justice (WPPJ)
M. Jan Remans (N)	Rhumatologue
M. Rudy Trogh (N)	Chef du personnel de la Banque Nationale de Belgique (BNB)
M. Eric Gheur (F)	Administrateur-gérant de la SPRL Galaxia I.S.E. et consultant en sécurité de l'information
Mme Françoise D'Hautcourt (F)	Directrice du Centre des Technologies pour l'Enseignement de l'ULB
M. Frank Schuermans (N)	Conseiller membre effectif au Comité permanent de contrôle des services de police (Comité P) Substitut du procureur général près la Cour d'appel de Gand
M. Yves Roger (F)	Président du Comité sectoriel de la Sécurité Sociale et de la Santé

4 La structure de la Commission

La Commission est constituée de seize membres.

Leur mandat est fixé à six ans.

Le Président est un magistrat.

La haute direction s'occupe de la gestion quotidienne de la Commission et de sa représentativité.

La Commission comprend des comités sectoriels.

Elle bénéficie de l'aide d'un Secrétariat.

4.1 Profil des membres

La Commission compte seize membres :

- un président ;
- un vice-président ;
- six membres effectifs ;
- huit membres suppléants.

Tous peuvent se prévaloir d'une expertise en matière de protection de la vie privée et de gestion des données à caractère personnel.

La Commission doit impérativement compter parmi ses membres : un juriste, un informaticien et deux personnes pouvant justifier d'une expérience professionnelle dans le domaine de la gestion des données à caractère personnel, respectivement dans le secteur public et dans le secteur privé.

Le mandat de président est réservé à un magistrat.

4.2 Mandats des membres

Les seize membres de la Commission sont tous désignés pour un mandat de six ans renouvelable.

4.3 Fonctions des membres

Le président et le vice-président sont les seuls à exercer leur fonction à temps plein ; les autres membres ne sont tenus que de prendre part aux séances de la Commission qui ont lieu, en principe, toutes les trois semaines.

4.4 Rôle du président

Les principales fonctions du président sont :

- il assume la haute direction de la Commission ;
- il définit sa politique ;
- il représente la Commission à l'échelle nationale et internationale* ;
- il assure sa gestion quotidienne ;
- il préside les réunions de la Commission ;
- il préside de droit les comités sectoriels ;
- il joue à tout le moins un rôle de coordinateur à l'égard des présidents des différents comités sectoriels.

* Il est à noter que la représentation de la Commission au sein de groupes de travail et d'organismes de contrôle internationaux peut également être confiée à d'autres membres.

4.5 Comités sectoriels

Plusieurs comités sectoriels en charge de secteurs spécifiques fonctionnent au sein de la Commission. Ils sont généralement composés pour moitié de membres de la Commission.

4.6 Secrétariat

Les tâches de la Commission, aussi nombreuses que variées, requièrent une préparation minutieuse et un important travail d'analyse préalable. En raison de l'étendue et de la complexité de leurs tâches, la Commission et les comités sectoriels sont aidés par une administration, baptisée "Secrétariat" par la loi belge.

5 La structure de l'administration

Elle prépare, soutient et exécute.

Elle élabore les dossiers.

La haute direction de cette administration que représente le Secrétariat est confiée par la loi au président de la Commission et sa direction générale est assurée par un administrateur. L'administration est divisée en trois sections, chacune dirigée par un chef de section.

Organisation du Secrétariat

La mission de l'administration par rapport à la politique générale de la Commission peut se résumer en trois mots : préparation, soutien et exécution.

Le Secrétariat intervient ainsi dans l'élaboration des dossiers, et plus particulièrement dans ceux relatifs aux divers projets d'avis, de recommandation ou d'autorisation. Ils sont préparés par un agent spécialisé dans le domaine concerné en étroite concertation avec le commissaire rapporteur chargé de superviser la rédaction du projet.

Dans un souci de gérer les dossiers individuels des citoyens de la manière la plus efficiente possible, l'administration opère un tri entre les affaires courantes susceptibles d'être réglées rapidement dans le cadre d'un traitement de première ligne et celles qui nécessitent un examen plus approfondi, donc souvent plus long.

6 Le plan de gestion de la Commission

Le plan de gestion détermine les compétences et confie au président la haute direction de la Commission et l'élaboration de sa politique, la représentation de la Commission aux niveaux national et international, la gestion journalière de la Commission et la direction des services par délégation à l'administrateur, la présidence des assemblées de la Commission ou des sous-groupes et enfin, la présidence de plein droit du/ des comité(s) sectoriel(s) et, le cas échéant, la coordination entre les Présidents des différents comités sectoriels.

Les principaux points intéressants en 2008 ont été les suivants.

6.1 Nouvelle vision/mission

En 2008, la Commission était à mi-chemin de son mandat. Un moment opportun pour une rétrospective sur ses premières années de fonctionnement en tant qu'organe collatéral de la Chambre des Représentants. Elle s'est donc interrogée sur la pertinence actuelle de sa vision et de sa mission telles qu'elles avaient été formulées en 2003. A la lumière de cet examen, il est apparu opportun et même recommandé d'y ajouter la nécessité d'une protection efficace et adéquate et d'attirer l'attention sur les aspects techniques et organisationnels des traitements de données, d'insister sur le rôle de la Commission dans la politique d'encadrement normatif ainsi que de donner quelques explications sur la législation internationale et la collaboration croissantes en matière de protection de la vie privée.

6.2 Intégration des comités sectoriels

En vertu de l'article 31bis de la Loi vie privée, les organes de protection spécifiques déjà institués par la loi et les organes de protection spécifiques que le législateur estime nécessaires ou a l'intention de créer à l'avenir dans un certain nombre

de domaines, sont désormais intégrés dans la Commission.

Il existe donc actuellement six comités sectoriels, dont un doit encore être constitué :

- le Comité sectoriel de la Sécurité Sociale et de la Santé (CS SS & S) ;
- le Comité sectoriel du Registre national (CS RN) ;
- le Comité sectoriel pour l'Autorité Fédérale (CS AF) ;
- le Comité sectoriel de la Banque-Carrefour des Entreprises (CS BCE) ;
- le Comité de surveillance sectoriel Phenix (CS Phenix) ;
- le Comité de surveillance statistique (CS STAT).

La composition du nouveau Comité sectoriel SS & S a été décidée le 21 novembre 2008.

Des candidatures ont été reçues pour le comité de surveillance sectoriel statistique mais la procédure de négociation n'a pas abouti.

Un juriste expert en la matière est désigné comme secrétaire pour chaque comité sectoriel et un agenda de réunion complet est dressé.

En ce qui concerne l'exercice pratique des compétences, les activités du CS STAT sont assurées par la Commission à proprement parler conformément à l'article 16 de l'Arrêté royal du 7 juin 2007 qui stipule que la Commission exerce les compétences du comité jusqu'à sa constitution.

6.3 Un Règlement d'ordre intérieur pour le Comité sectoriel de la Banque-Carrefour des Entreprises

Le Règlement d'ordre intérieur du CS BCE a été approuvé le 11 juin 2008. Il a été publié au Moniteur belge du 30 octo-

bre 2008. Il repose sur la même trame que les autres comités sectoriels et c'est logique puisque l'objectif poursuivi est que tous les comités dont l'administration de la Commission assure le soutien fonctionnent de manière similaire. Cet objectif s'inscrit dans le cadre des préoccupations formulées dans le plan de gestion en ce qui concerne la collaboration entre les différents maillons de la Commission.

6.4 Contrôle de la vie privée - évaluation

Ce qu'on appelle le contrôle de la vie privée constitue un élément important du Règlement d'ordre intérieur. Cela signifie que lors du processus décisionnel et de l'examen du dossier, une attention particulière est accordée au cadre matériel et légal, et surtout au contrôle des principes qui régissent les traitements de données à caractère personnel et à leur impact sur la vie privée des personnes concernées.

Il est, en effet, indispensable que la Commission et son administration fonctionnent conformément à la vision développée dans le plan de gestion et exprimée dans les objectifs qui stipulent expressément que la Commission souhaite agir dans une optique sociale et veiller à la défense équitable de la protection de la vie privée face aux ambitions légitimes des autorités, des services et des entreprises fonctionnels et bien organisés.

En 2008, la Commission a entamé une évaluation systématique des initiatives législatives sur lesquelles elle a émis un avis.

6.5 Information au public

Un des buts stratégiques énoncés par la Commission dans son plan de gestion est de contribuer à une meilleure information du public (responsable du traitement et citoyen), d'une part en répondant aux demandes d'informations par le

biais des services de la section Relations externes et, d'autre part en mettant l'information à la disposition du public dans le cadre d'une stratégie de communication active.

Le site web est un des canaux utilisés par la Commission pour réaliser cet objectif. Les informations proposées sur ce site sont régulièrement enrichies et actualisées. En 2008, une rubrique importante intitulée "International" y a été ajoutée et des informations intéressantes pour les visiteurs étrangers y ont été publiées en anglais.

6.6 Vie privée & recherche scientifique

En 2008, la Commission a plus spécialement étudié les rapports entre la protection de la vie privée et la recherche scientifique. Dans ce cadre, 2 journées d'étude ont été organisées: le 27 novembre 2008 la Commission a présenté sa brochure "Vie privée : le vade-mecum du chercheur" au monde scientifique et le 5 décembre 2008, la Commission a participé à une journée d'étude consacrée à la législation relative à la protection de la vie privée et à la recherche historique. La Commission veut approfondir cette dynamique et envisage d'organiser une journée d'étude internationale sur ce thème en 2010.

7 Les principales activités nationales de la Commission

7.1 Autorités et organes publics

En 2008, le secteur public a demandé l'avis de la Commission à plusieurs reprises. Ces demandes d'avis ont été introduites par des instances de divers niveaux et concernaient, e.a. les thèmes suivants :

- l'échange électronique de données administratives ;
- les données conservées par certains centres de prêt public sur leurs lecteurs ;
- la gestion des accès et des utilisateurs ;
- les listes d'inscription des écoles secondaires de la Communauté française ;
- l'Intégrateur de services fédéral ;
- la Geografische-Data-Infrastructuur Vlaanderen ;
- le Centraal Referentieadressenbestand.

7.1.1 L'échange électronique de données administratives

Avis n° 01/2008 du 16 janvier 2008 :

- administrations flamandes ;
- contrôle de l'échange électronique des données ;
- création d'une Commission flamande de surveillance de l'échange électronique de données administratives.

A la demande du ministre flamand de la Fonction publique, des Relations extérieures, des Médias et du Tourisme, la Commission a émis un avis sur un projet de décret relatif à l'échange électronique de données administratives.

Étant donné que le décret visait avant tout à combler une lacune qui avait d'importantes répercussions sur la protection de la vie privée, et plus précisément l'absence d'un contrôle approfondi de l'échange électronique de données entre des services dépendant des Communautés et des Régions, cette initiative a été accueillie favorablement par la Commission.

Cette dernière a néanmoins regretté que cette tâche de contrôle n'ait pas été confiée à un comité sectoriel au sein de la Commission mais plutôt à la Commission flamande autonome de surveillance de l'échange électronique de données administratives. A cet égard, la Commission a souligné :

- que cette option compliquerait l'échange des données entre les différents niveaux des autorités et ;
- que du fait des compétences concurrentes de la Commission flamande de surveillance et de la Commission vie privée, elle risquait d'aboutir à des avis divergents sur un même problème, ce qui ne serait pas une bonne chose dans la perspective de la Loi vie privée.

La Commission a également souligné que le texte proposé :

- ne contenait aucune disposition garantissant l'indépendance de la Commission flamande de surveillance ;
- parlait bien de la création d'un lien avec la Commission dans son exposé des motifs mais que ce dernier point n'était concrétisé dans aucune disposition décrétole ;
- ne mentionnait nulle part quelle serait la composition de la Commission flamande de surveillance.

Le décret finalement approuvé par le Parlement flamand le 9 juillet 2008 a tenu compte de manière non négligeable des remarques formulées par la Commission. Afin de garantir son indépendance, la Commission flamande de surveillance a été instituée par le Parlement flamand et un lien étroit a été mis en place avec la Commission en stipulant que 3 membres de la Commission flamande de surveillance doivent également être membres (suppléants) de la Commission vie privée.

7.1.2 Les données conservées par certains centres de prêt public sur leurs lecteurs

Avis n° 30/2008 du 3 septembre 2008 :

- création d'une base de données centrale des lecteurs/

abonnés ;

- déclaration par les instances de prêt concernées ;
- perception et distribution correctes de la rémunération pour prêt public.

Le 3 septembre 2008, la Commission s'est prononcée favorablement par voie d'avis sur le projet de la ministre de la Culture et de l'Audiovisuel de la Commission française de constituer une base de données des lecteurs/abonnés des bibliothèques publiques.

La finalité de la constitution d'une telle base de données est d'établir la déclaration prévue à l'article 7 de l'Arrêté royal du 25 avril 2004 relatif aux droits de rémunération pour prêt public des auteurs, en vue d'assurer une perception et une répartition correctes de la rémunération pour prêt public.

La Commission a tout d'abord constaté le caractère proportionné de la constitution d'une telle base de données centrale au vu des critères légaux de détermination du montant forfaitaire dû par les bibliothèques au titre de la rémunération des auteurs pour prêt public.

La Commission a ensuite adressé les recommandations usuelles relatives à la limitation des données centralisées aux données strictement nécessaires pour la réalisation de la finalité poursuivie ainsi qu'à la désignation expresse des éventuels tiers disposant d'un droit d'accès légitime eu égard à la finalité liée à la constitution de la base de données.

Enfin, l'intention de la ministre compétente de doter son projet de constitution d'une base de données d'un cadre légal a été accueillie favorablement par la Commission dans la mesure où cette initiative favorise la prévisibilité et la transparence des traitements de données. La Commission a également rappelé à ce propos que la Loi vie privée exigeait dans son article 1^{er}, § 4 que le responsable du traitement soit explicitement désigné.

7.1.3 La gestion des accès et des utilisateurs

Recommandation n° 01/2008 du 24 septembre 2008 :

- autorité fédérale et régionale ;
- développement d'un système coordonné ;
- bases de données authentiques validées.

Le Comité sectoriel du Registre national reçoit régulièrement des demandes d'autorisation d'utilisation du numéro du Registre national dans le cadre de la gestion des accès et des utilisateurs. Le Comité a constaté à ce niveau que les données à caractère personnel sont souvent enregistrées mais pas validées. Cette situation entraîne un risque réel qu'une personne ait accès à des données auxquelles elle n'est en fait pas habilitée à avoir accès. Étant donné que cette problématique dépasse les compétences du Comité sectoriel du Registre national, ce dernier a décidé de demander l'avis de la Commission à ce sujet.

Suite à cette demande, la Commission a émis une recommandation qui énonce plusieurs règles pratiques en matière de gestion des accès et des utilisateurs dans le secteur public :

- il est souhaitable de développer un système basé sur le principe des "cercles de confiance" ;
- il faut prévoir un bon enregistrement, ce qui implique, dans la mesure du possible, le contrôle de l'identité de l'utilisateur qui se connecte, de ses caractéristiques et de ses autorisations d'accès à l'aide de documents/sources authentiques (qui offrent les garanties nécessaires au niveau du caractère exact et actuel des informations qu'ils contiennent, ou en d'autres termes, des sources authentiques validées) ;
- l'authentification électronique de l'identité doit se faire, de préférence, à l'aide de la carte d'identité électronique ;
- la gestion des accès comprend l'enregistrement et la vérification des autorisations :
 - o l'enregistrement implique que le fournisseur du service électronique introduise les autorisations dans

une source authentique en y spécifiant les traitements autorisés, les services concernés, les conditions (par exemple caractéristiques, mandats, ...) à respecter ainsi que la durée des autorisations. Certains utilisateurs (exemple les gestionnaires locaux) peuvent, à leur tour, accorder les autorisations qui leur ont été octroyées à d'autres utilisateurs qu'ils doivent désigner en les introduisant dans une source d'autorisations,

- o la vérification implique la consultation des sources authentiques d'autorisations pertinentes.

7.1.4 Les listes d'inscription des écoles secondaires de la Communauté française

Avis n° 42/2008 du 17 décembre 2008 :

- inscription simultanée dans plusieurs écoles ;
- comparaison des listes d'inscription ;
- libération de places pour les candidats sur liste d'attente.

Afin de déceler les élèves figurant en ordre utile d'inscription dans plusieurs établissements d'enseignement et d'inviter les parents à exercer un choix permettant de libérer des places pour les candidats en attente, le Gouvernement de la Communauté française a envisagé la mise en place d'un dispositif visant à réaliser la consolidation des fichiers des différents établissements concernés en deux phases. La première phase de cette consolidation se ferait au sein même de chacun des quatre réseaux d'enseignement et la deuxième phase serait réalisée plus tard entre les réseaux.

Saisie en urgence de cette question, la Commission a tout d'abord estimé qu'un tel traitement était admissible au vu à la fois des compétences de la Communauté française en matière de politique de l'enseignement et des obligations positives y afférentes, c.-à-d., notamment, celle d'assurer le libre choix des parents, celle du droit à l'enseignement, celle de l'égalité des élèves et des parents devant la loi ou le décret et enfin, celle de tenir compte des instruments juridiques

internationaux tels que la Convention européenne des droits de l'homme et des libertés fondamentales, de la Convention relative aux droits de l'enfant et de la Charte des droits fondamentaux de l'Union européenne.

La Commission a ensuite examiné la proportionnalité du traitement envisagé plus spécialement sous trois angles d'incidence :

- la loyauté (à cet égard, la Commission a suggéré que le Gouvernement de la Communauté française adresse une circulaire à tous les établissements concernés) ;
- l'absence d'incompatibilité au regard des attentes raisonnables des intéressés de la possibilité pour l'administration d'utiliser les informations collectées pour la bonne exécution de ses missions et l'exercice le plus juste possible des droits fondamentaux de chacun ;
- les données traitées et leur conservation (suppression immédiate des listes consolidées des données des enfants qui ne font l'objet que d'une seule inscription utile et qui ne figurent sur aucune liste d'attente).

Si les données devaient être considérées comme des données sensibles au sens de l'article 6 de la Loi vie privée – ce qui paraît contestable – l'interdiction de les traiter ne s'y appliquerait pas puisque le traitement de ces données est autorisé par une loi - un décret - pour "un autre motif important d'intérêt public" (article 6, § 2, 1) de la Loi vie privée). La Commission a cependant suggéré d'appliquer les conditions posées aux traitements de données sensibles mentionnées à l'article 25 de l'Arrêté royal du 13 février 2001 portant exécution de la Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

La Commission a aussi recommandé de procéder à une consolidation non pas en deux phases comme initialement envisagé par la Communauté mais bien en une seule phase et ceci sur la base des arguments suivants :

- le bât blesse au niveau du libre choix effectif des parents, pas au niveau de la spécificité des réseaux ;

- cette consolidation en une seule phase garantit à chaque enfant d'être inscrit dans une école à un moment donné commun ;
- cette manière de procéder permet de maîtriser des situations qui semblent discriminatoires : à côté de certains enfants inscrits dans plusieurs d'écoles, d'autres ne le sont dans aucune et se verraient contraints de s'inscrire en urgence à la rentrée là où des disponibilités apparaîtraient soudain qui ne correspondraient pas à ce qu'ils sont en droit d'attendre et peut-être d'obtenir ;
- enfin, le système proposé par la Communauté conduit nécessairement à multiplier les fichiers et les traitements (et donc les risques et les conflits), tout en n'apportant aucune solution définitive au cours des étapes intermédiaires. Au cours de la deuxième phase (comparaison entre les réseaux) il faut donc tenir compte de la totalité des fichiers intermédiaires (et en tout cas de la totalité des élèves inscrits) consolidés ou non (il s'avère en effet impossible d'éliminer un élève d'un fichier "intranréseau" puisqu'on ne sait pas s'il n'est pas aussi inscrit dans un autre réseau).

Quelle que soit la solution qui sera retenue par le Gouvernement de la Communauté française, la Commission a recommandé que la comparaison des listes des différents réseaux soit placée sous la surveillance d'une structure regroupant des représentants de chacun des réseaux et que si l'administration de la Communauté devait être chargée de réaliser cette opération – puisque celle-ci ressortit à ses compétences et parce qu'elle est déjà outillée pour le faire – il serait par ailleurs indiqué que cette tâche soit confiée à un service et à des agents qui ne disposent d'aucune compétence en matière de supervision des écoles de la Communauté et de leur personnel. Si le Gouvernement de la Communauté française en exprime le souhait, la Commission se déclare prête à déléguer un de ses membres pour siéger au sein de cette structure, ceci sous réserve des compétences accordées aux membres de la Commission et du propre pouvoir de contrôle de cette dernière.

En conclusion, la Commission a émis un avis favorable sur le projet de confronter les fichiers d'inscription des élèves dans le 1^{er} cycle de l'enseignement secondaire dans les établissements scolaires organisés ou subventionnés par la Communauté à la condition expresse qu'il soit tenu compte des observations émises et a recommandé de procéder à cette comparaison en une seule phase et, à défaut de l'adoption de ce scénario, d'apprécier les risques liés à la comparaison en deux phases et de prendre toutes les mesures nécessaires pour les maîtriser.

7.1.5 L'Intégrateur de services fédéral

Avis n° 41/2008 du 17 décembre 2008 :

- service électronique intégré et personnalisé ;
- création d'une instance de coordination au niveau fédéral ;
- point de contact en matière de concertation avec les autres niveaux des pouvoirs publics.

Le président du Comité de direction du Service public fédéral Technologie de l'Information et de la Communication (Fedict) a demandé à la Commission d'émettre un avis sur un avant-projet de loi relative à l'institution et à l'organisation d'un Intégrateur de services fédéral.

L'évaluation de cette initiative pour laquelle la Commission avait déjà plaidé par le passé a été positive. Les points forts de cet avant-projet sont e.a. :

- qu'il a été opté pour une intégration des services moins dangereuse en termes de protection de la vie privée qu'une intégration des données ;
- que le terrain d'action de l'intégrateur de services fédéral est clairement défini, ce qui exclut tout "shopping" entre les différents intégrateurs de services ;
- qu'il prévoit la possibilité de ne faire traiter le processus d'intégration que par un seul comité sectoriel.

Ces points forts n'ont cependant pas empêché la Commission d'estimer que plusieurs points du texte étaient encore

susceptibles d'être améliorés. Elle a ainsi souligné que :

- déclarer que le concept de "donnée authentique" est crucial pour déterminer une source authentique, c'est vague ;
- le principe de la collecte unique ne peut pas court-circuiter l'article 4, § 1^{er}, 2° de la Loi vie privée (finalité et compatibilité) ;
- l'exception au principe d'interdiction de l'octroi de droits complémentaires par l'intégrateur de services fédéral brille par son manque de précision et semble ouvrir la voie à la méconnaissance des articles 4 et 5 de la Loi vie privée ;
- la transparence à l'égard du citoyen doit être intégrée en donnant à ce dernier la possibilité de vérifier qui a consulté ses données dans des sources authentiques.

7.1.6 La Geografische Data-Infrastructuur Vlaanderen

Avis n° 32/2008 du 24 septembre 2008 :

- infrastructure commune pour les données géographiques ;
- consolidation des points forts dans le cadre réglementaire ;
- adaptation à la Directive INSPIRE.

Le projet de décret soumis pour avis à la Commission avait pour objectif la mise en place d'un cadre réglementaire actualisé pour le développement d'une infrastructure de données géographiques (ci-après GDI - Geografische Data-Infrastructuur). Ce projet poursuivait un double objectif : d'une part consolider les points forts de l'infrastructure de données géographiques en Flandre et d'autre part apporter un certain nombre d'améliorations conceptuelles. Son but était aussi de répondre aux nouvelles obligations imposées par la Directive INSPIRE.

Ce projet présentait toutefois plusieurs manquements sur le plan de la protection de la vie privée. C'est ainsi, notamment que les finalités de ce projet n'étaient pas suffisamment déterminées. Ce projet ne contenait aucune règle ni d'utili-

sation, ni d'accès aux données appelées à figurer dans cette infrastructure et n'accordait manifestement aucune attention non plus à l'application du principe de proportionnalité, ceci pas plus au niveau de la nature des données à traiter qu'au niveau de leur quantité ou de leur durée de conservation.

La Commission a également constaté que certains traitements de données censés avoir lieu dans le cadre de ce projet, tomberaient également dans le champ d'application du Décret du 18 juillet 2008 *relatif à la circulation électronique de données administratives* et qu'il subsiste toujours un conflit de compétence entre ces deux textes législatifs.

Pour ces raisons, la Commission a émis un avis défavorable sur cet avant-projet.

7.1.7 Le Centraal Referentieadressenbestand

Avis n° 36/2008 du 26 novembre 2008 :

- fichier contenant des adresses et positions d'adresses ;
- source de données géographiques authentiques pour les instances publiques ;
- géré par l'administration flamande en collaboration avec les communes.

Ce projet de décret soumis pour avis à la Commission concernait le Centraal Referentieadressenbestand (Fichier central d'adresses de référence – FCAR). Ce fichier est destiné à contenir tous les numéros de maison et tous les noms de rue de Flandre ainsi que leur position d'adresse.

Dans le cadre de son examen de ce dossier, la Commission a constaté que, de manière globale, le projet qui lui avait été soumis répondait aux conditions imposées par la Loi vie privée et elle a donc émis un avis positif à la condition qu'il soit tenu compte de deux remarques.

La première de ces remarques était que les auteurs du projet devaient réfléchir à une politique d'archivage adaptée des

données contenues dans le Centraal Referentieadressenbestand.

La deuxième était que la Commission émettait de sérieux doutes quant à l'exception à l'obligation principale d'autorisation prévue dans le projet qui prévoyait que les instances ayant déjà obtenu une autorisation du Comité sectoriel du Registre national étaient automatiquement dispensées de l'autorisation préalable octroyée par la Commission flamande de contrôle pour l'échange électronique de données administratives. La Commission a précisé cette réserve comme suit : *"Le Comité sectoriel du Registre national octroie des autorisations d'accéder à des informations bien déterminées du Registre national, et ce pour des finalités déterminées. Ces autorisations ne valent que pour cet accès et non pour l'accès au FCAR."*

7.2 Démographie et diversité

Dans notre société actuelle, il n'est pas étonnant que la Commission reçoive des questions inspirées par les importants glissements observés au niveau de la composition de la population. Au cours de l'année écoulée, elle s'est ainsi prononcée sur :

- la Generations and Gender Panel Study ;
- le monitoring des groupes à potentiel du VDAB ;
- une étude sociologique sur les (candidats -) locataires.

7.2.1 La Generations and Gender Panel Study

Avis n° 02/2008 du 06 février 2008 :

- étude longitudinale internationale ;
- intentions en matière de formation/dissolution d'une famille, fécondité et retraite ;
- enquête auprès de différents groupes d'âge.

Le but de la *Generations and Gender Panel Study* (GGPS) est de réaliser une étude longitudinale sur la formation et la dissolution des familles ainsi que sur la fécondité et la retraite. Cette étude est destinée à sonder les intentions qui gouver-

nent ces évolutions et abordait également les thèmes de l'aide familiale, des soins aux personnes et de l'émancipation. La GGPS est une étude par panel composée de 3 vagues d'enquête prévues à trois ans d'intervalle. En Belgique, la GGPS a été confiée à la Direction générale Statistique et Information économique (DGSIE) du SPF Économie (<http://mineco.fgov.be/>).

La Commission a formulé une série de remarques pour avis destinées à la DGSIE sur le questionnaire, l'échantillon du Registre national, l'absence de consentement avant la prise de contact directe avec la personne concernée, le délai de conservation du fichier de communication et la transmission des données de recherche à des tiers.

Questionnaire

La Commission a constaté que la GGPS demande aux répondants de communiquer certaines données sensibles et relatives à la santé.

Dans le cadre de la Loi vie privée, le fait de poser ces questions ne pose aucun problème : le traitement de ce type de données à caractère personnel n'est en effet pas interdit lorsqu'il est effectué sur la base du consentement écrit de la personne concernée ou lorsqu'il est nécessaire à des fins de recherche scientifique. Avant que l'enquête ne puisse effectivement être effectuée, la personne concernée doit signer un formulaire dans lequel elle confirme son consentement exprès à la participation à l'étude.

Dans cet avis, la Commission a attiré l'attention sur l'article 24quinquies de la Loi statistique publique qui interdit à la Direction générale Statistique et Information économique de réaliser des études relatives à la vie privée, notamment à la vie sexuelle, aux opinions ou activités politiques, philosophiques ou religieuses, à la race ou à l'origine ethnique.

Echantillon

L'échantillon est basé sur le Registre national des personnes physiques.

La Commission constate que plusieurs sources légales prévoient l'accès de la DGSIE au Registre national, mais estime néanmoins que la coexistence de ces différents textes de loi ne favorise pas la bonne compréhension des droits d'accès de la DGSIE au Registre national et estime qu'il serait utile, qu'à terme, le Comité sectoriel du Registre national confirme une nouvelle fois l'accès de la DGSIE au Registre national dans une autorisation.

Absence de consentement avant qu'il ne soit directement pris contact avec la personne concernée

La Commission constate qu'il n'y aura pas de consentement écrit préalable et que seules les personnes qui auront confirmé par écrit leur volonté de participer à l'enquête seront contactées par l'enquêteur (comme cela a été le cas dans le cadre de l'étude pilote). Pour cette raison, la Commission demande que la DGSIE s'engage à respecter une série de conditions supplémentaires. Ces conditions sont celles qui ont été fixées ultérieurement dans un avis général d'initiative du 3 septembre 2008 relatif au code que les destinataires de données du Registre national s'engagent à respecter lors de l'exécution de leur mission de recherche scientifique.

Fichier de communication

La Commission estime que les données à caractère personnel contenues dans le fichier de communication doivent être détruites avant la fin de la troisième vague d'enquête, par exemple avant le début de la deuxième vague d'enquête pour les personnes qui n'ont pas participé à la première vague d'enquête ou avant le début de la troisième vague d'enquête pour les personnes qui n'ont pas participé à la deuxième

vague d'enquête. Etant donné qu'il s'agit d'une étude par panel, suivre des personnes qui n'ont pas participé à la première ou à la deuxième vague d'enquête dans les deuxième et troisième vagues respectivement n'aurait aucun sens.

Transmission de données de recherche à des tiers

La Commission estime que les données de recherche codées ne peuvent être communiquées à des tiers que par le biais d'un contrat de confidentialité conclu avec la DGSI après autorisation positive du Comité de surveillance statistique. En ce qui concerne l'équipe scientifique de la GGPS, cette autorisation a été accordée dans le cadre de la délibération STAT n° 11/2008 du 21 mai 2008.

7.2.2 Le monitoring des groupes à potentiel du VDAB

Avis n° 05/2008 du 27 février 2008 :

- politique d'égalité des chances ;
- données relatives aux origines et handicap professionnel ;
- collecte de données intégrées dans le fichier du personnel.

Dans le cadre de sa politique en matière d'égalité des chances et de diversité, le Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding (ci-après le VDAB – <http://vdab.be>) voulait se faire une idée de la présence des groupes à potentiel "personnes d'origine allochtone" et "personnes handicapées du travail" sur la base d'un enregistrement volontaire dans son fichier du personnel.

Le VDAB voulait donc savoir si le système de monitoring des groupes à potentiel visés contenu dans son fichier personnel était ou non conforme à la Loi vie privée.

La Commission a conclu que les données relatives à la diversité étaient suffisamment transparentes, sûres et proportionnelles et qu'elles étaient traitées sur une base

volontaire. Les finalités du traitement étaient légitimes et basées, entre autres, sur les droits et obligations décrétés du VDAB (Décret du 8 mai 2002 relatif à la participation proportionnelle sur le marché de l'emploi).

La Commission a néanmoins constaté une série d'imperfections dont elle a exigé qu'elles soient corrigées au plus tard au moment de l'opérationnalisation du système de monitoring :

- le membre du personnel doit pouvoir retirer un consentement ou un refus donné et dans ce cadre, les données modifiées par la personne concernée dans un sens ou un autre ne peuvent pas être archivées dans le système de manière permanente ;
- la période de mise en œuvre du système d'autoenregistrement est mal choisie car elle coïncide avec la période d'évaluation du personnel, ce qui peut donner l'impression aux membres du personnel appartenant aux groupes à potentiel concernés qu'ils sont mis sous pression pour communiquer leurs données ;
- étant donné que la politique d'égalité des chances et de diversité visée n'est pas axée sur certaines nationalités spécifiques, la Commission estime que le fait de demander d'emblée la nationalité du (des) grand(s)-parent(s) du membre du personnel est excessif ;
- aucun monitoring des membres du personnel qui n'appartiennent au groupe à potentiel "personnes d'origine allochtone" que sur la base de leur nationalité ne peut être mis en place si ces personnes ne se sont pas volontairement fait enregistrer en tant que telles pour les finalités de monitoring de ce projet ;
- étant donné le caractère sensible des données à demander, l'article 25 de l'Arrêté royal du 13 février 2001 doit être respecté ;
- la Commission recommande également de faire contrôler l'ensemble du projet par un conseiller en sécurité de l'information chargé e.a. des tâches d'un préposé à la protection des données ;
- le contrôle de la fiabilité et de la représentativité du système (en d'autres termes la vérification du nombre de

personnes appartenant aux groupes à potentiel qui encodent effectivement leurs données dans le système) ne peut pas être basé sur des données à caractère personnel.

7.2.3 Étude sociologique sur les (candidats-) locataires

Recommandation n° 02/2008 du 05 novembre 2008 :

- Société Wallonne du Logement ;
- registre électronique des candidats à la location d'un logement social ;
- étude sociologique sur les données de ce registre.

La Société Wallonne du Logement (SWL) a demandé à la Commission ses réactions et observations sur la gestion du formulaire unique de candidature à un logement et la réalisation d'une étude sociologique sur les caractéristiques des locataires et les candidats locataires.

Ce formulaire figure en annexe 4 de l'Arrêté du Gouvernement wallon du 6 septembre 2007 organisant la location des logements gérés par la Société wallonne du Logement (SWL) ou par les sociétés de logement de service public.

La Commission a estimé que les éléments fournis ne permettent pas de déterminer comment fonctionne le registre informatisé des candidatures coordonné par la SWL et que sa ou ses finalités sont plutôt implicites, même si on peut supposer qu'il s'agit de procéder au classement des candidats locataires en vue de l'attribution d'un logement. La Commission recommande d'être plus explicite sur ce point (cf. l'article 4, § 1^{er}, 2° de la Loi vie privée). Elle constate qu'il n'est pas indiqué, par exemple, si une société du logement a accès, via ce registre informatisé, à toutes les candidatures ou seulement à celles qui concernent, entre autres, un de ses logements. La Commission a recommandé d'apporter un maximum de précisions sur le fonctionnement et l'accès aux données de ce registre. Les modalités majeures de fonctionnement devraient en outre faire l'objet d'un arrêté du

Gouvernement wallon.

La Commission a ensuite rappelé, sans prétendre à l'exhaustivité, quelques principes essentiels en matière de protection des données applicables aux traitements mis en œuvre.

Quant au contenu du formulaire, il apparaît que :

- des données d'ascendants ou de descendants, membres du ménage, sont traitées sans que celles-ci ne soient "visées" par les intéressés ;
- des données relatives à la santé sont collectées, notamment sur l'existence d'un handicap, d'une invalidité de guerre, d'une maladie professionnelle... alors que le traitement de ce type de données est, en principe, interdit. Dans plusieurs hypothèses, l'interdiction de principe du traitement de données relatives à la santé est levée, notamment, lorsque le traitement est rendu obligatoire par ou en vertu d'un décret pour des motifs d'intérêt public majeurs. A défaut de pouvoir se fonder sur cette hypothèse, le consentement écrit des intéressés est requis ;
- la Commission ne considère pas d'emblée les données "lieu de naissance" et "nationalité", comme des données sensibles au sens de la Loi vie privée mais la collecte de ces données doit néanmoins être pertinente. A cet égard, la Commission relève qu'il ne ressort pas de la réglementation actuelle que le lieu de naissance et la nationalité entrent en ligne de compte pour l'attribution d'un logement.

La SWL évoque un objectif de mixité sociale et de lutte contre les discriminations dans le secteur du logement. A cet égard, la Loi du 10 mai 2007 tendant à lutter contre certaines formes de discriminations et la Loi du 10 mai 2007 modifiant la Loi du 30 juillet 1981 tendant à réprimer certains actes inspirés par le racisme et la xénophobie disposent que la distinction fondée sur un des critères protégés (nationalité, état civil, naissance, etc.) ne constitue pas une discrimination lorsqu'elle est objectivement justifiée par un but légitime et que les moyens de réaliser ce but sont appropriés et nécessaires. La détermination précise de la ou

des finalités et des critères d'attribution garde donc toute son importance dès lors qu'on envisage le traitement de données "potentiellement sensibles" ou discriminatoires. La Commission recommande donc une adaptation des textes (décret et/ou arrêté) dans le sens d'une meilleure détermination des finalités et des données traitées.

La réalisation d'une étude sociologique sur les caractéristiques des locataires et candidats-locataires ne peut pas être considérée d'emblée comme un traitement compatible avec la finalité initiale de la collecte des données. A cet égard, il est intéressant de noter que la Commission a déjà estimé (avis n° 18/2008 du 30 avril 2008) que l'examen de la compatibilité d'un traitement ultérieur par un responsable relevant du secteur public doit d'abord s'appuyer sur des dispositions légales et réglementaires qui décrivent suffisamment le traitement ultérieur et le type de données qui peuvent être traitées, leur origine et les finalités du traitement. L'adoption d'une disposition décrétole ou réglementaire "ad hoc" pourrait permettre de considérer qu'un tel traitement ultérieur n'est pas incompatible avec le traitement initial. En dehors de cette hypothèse, dans son chapitre II, l'Arrêté royal du 13 février 2001 portant exécution de la Loi vie privée fixe les conditions pour qu'un traitement ultérieur à des fins statistiques ou scientifiques puisse être réputé compatible.

7.3 Recherche et développement

La recherche et le développement revêtent une importance croissante dans tous les secteurs. L'année dernière, la Commission a donc, elle aussi, été confrontée à ce thème. Dans ce cadre, elle a rédigé :

- un avis sur la réutilisation des données administratives à des fins de recherche ;
- un code de bonne conduite pour les chercheurs qui travaillent avec des données du Registre national.

7.3.1 Réutilisation des données administratives à des fins de recherche

Avis n° 20/2008 du 11 juin 2008 :

- finalités de recherche du SOOI-UGent ;
- couplage du numéro du Registre national aux fichiers administratifs existants ;
- exemption de l'obligation d'information.

Le Steunpunt O&O-indicatoren de l'Université de Gand (SOOI-UGent) s'est vu confier pour mission par le Gouvernement flamand la mise en place d'un suivi plus permanent des doctorats effectués en Flandre, de la mobilité intersectorielle et internationale des chercheurs et de l'influence d'un doctorat sur la carrière des doctorants sur le marché du travail.

Le ministre flamand compétent a demandé à la Commission :

- si des données issues des banques de données administratives des cinq universités flamandes peuvent être utilisées pour d'autres finalités que celles pour lesquelles elles ont été recueillies initialement, à savoir la réalisation des finalités de recherche du SOOI-UGent ;
- si le SOOI-UGent peut utiliser le numéro d'identification du Registre national pour procéder au couplage de ces fichiers de données administratives en vue de la réalisation de ces finalités de recherche ;
- si le SOOI-UGent est dispensé de l'obligation d'information liée à l'utilisation de données à caractère personnel.

La Commission a constaté que le couplage des données ne devrait pas être effectué par le SOOI-UGent mais par une cellule distincte au sein du SOOI-UGent et qu'il y a donc une barrière entre, d'une part la cellule au sein du SOOI-UGent où les données non codées en provenance des universités flamandes seront rassemblées et couplées et, d'autre part la cellule de recherche qui ne recevra de la cellule couplage que des données anonymisées destinées à l'analyse et l'étude scientifique et/ou statistique.

En ce qui concerne la première question, la Commission a demandé la mise en place, dans l'année, d'un "trusted third party" spécifique pour le projet de recherche SOOI et a émis le souhait qu'en attendant sa mise en place, il soit tenu compte, d'une série de remarques concernant le statut et la composition de la cellule de couplage interne :

- un contrôle externe du processus de couplage "interne" doit être organisé ;
- la cellule de couplage doit au moins être gérée par un organe dans lequel sont représentés les fournisseurs des informations et surtout les différents types de personnes concernées par les informations ;
- la cellule de couplage doit être considérée comme un responsable du traitement autonome (et pas comme un sous-traitant des différents fournisseurs de données), et endosse donc à ce titre, en vertu de la Loi vie privée, une propre responsabilité ;
- la cellule de couplage doit anonymiser les données pour que la cellule de recherche ne puisse pas, elle-même, établir de lien entre les informations obtenues et une personne physique identifiée ou identifiable.

En ce qui concerne la deuxième question, la Commission a souligné qu'après cet avis le Comité sectoriel du Registre national réétudierait la possibilité de coupler les données sur la base du numéro de Registre national. Ce point a finalement été traité dans la délibération RN n° 31/2008 du 30 juillet 2008.

Quant à la dernière question traitée dans cet avis, la Commission a estimé que la cellule de couplage ne doit pas informer la personne concernée, ceci du fait que les données qui doivent être anonymisées ne constituent pas des données sensibles au sens des articles 6 à 8 compris de la Loi vie privée et que cette anonymisation demanderait, qui plus est, des efforts disproportionnés.

7.3.2 Code de bonne conduite pour les chercheurs qui travaillent avec des données du Registre national

Avis n° 27/2008 du 03 septembre 2008 :

- communication des données du Registre national ;
- recherche scientifique sur des échantillons de la population ;
- enquêtes orales et téléphoniques.

Les procédures strictes en matière de protection de la vie privée mises en place par la Commission ces dernières années inquiétaient les chercheurs. Le caractère lourd des conditions d'accès aux données du Registre national, surtout, leur a même fait craindre de ne plus pouvoir faire de la recherche scientifique responsable. La Commission a pris cette critique à cœur et pour arriver à une solution, elle a mis en place une concertation à la fois au niveau interne et avec le monde de la recherche.

Cette concertation a mené à la rédaction d'un code qui a été repris dans l'avis cité plus haut sur la portée duquel nous allons nous arrêter plus en détail.

Dans le cadre de la réalisation d'une recherche scientifique basée sur un échantillon de la population, si la finalité de la recherche est une finalité d'intérêt général, toute institution de droit belge est en droit d'obtenir la communication de données d'identification du Registre national après en avoir obtenu l'autorisation du Comité sectoriel du Registre national.

L'enquête écrite constitue la règle, l'enquête orale l'exception. Si le chercheur ne peut ou ne souhaite pas travailler avec un questionnaire écrit, il doit en faire la demande auprès du Comité sectoriel du Registre national et motiver son choix.

Lorsqu'il s'agit de questionnaires écrits destinés à une

enquête unique, le Registre national se charge lui-même de l'envoi des questionnaires accompagnés d'une lettre d'introduction et des documents fournis par l'organisme de recherche. Les envois ultérieurs peuvent également se faire en suivant la même procédure. Dans ce cas, le Registre national ne transmet à l'organisme de recherche que les informations nécessaires pour lui permettre d'effectuer une analyse des refus de répondre et ceci, qui plus est, uniquement sous forme codée.

S'il s'agit d'enquêtes orales dans le cadre desquelles des données d'identification s'avèrent nécessaires, le Registre national transmet les données à caractère personnel appropriées à l'organisme de recherche à condition que celui-ci s'engage à respecter les dispositions suivantes :

- la personne concernée ne peut pas être sollicitée plus qu'elle ne le souhaite ;
- l'organisme de recherche doit adopter un comportement correct et professionnel ;
- les données d'identification doivent faire l'objet d'une protection particulière, éventuellement par le biais du recours à un tiers de confiance ;
- les rapports et publications réalisés sur la base des données de recherche obtenues à l'aide de données du Registre national ne peuvent contenir que des données anonymes.

7.4 Justice et sécurité

L'utilisation des données judiciaires, de par leur caractère par nature sensible, intéresse particulièrement la Commission. En 2008, elle a ainsi étudié dans ce domaine :

- une proposition de loi sur les certificats de bonne vie et mœurs ;
- une modification de loi sur la conservation des données pour enquête sur des faits punissables ;
- la communication de données sur des personnes condamnées au pénal ;
- les développements de la Loi caméras.

7.4.1 Proposition de loi sur les certificats de bonne vie et mœurs

Avis n° 20/2008 du 27 février 2008 :

- base légale des certificats ;
- sécurité des enfants ;
- évaluation basée sur les faits repris dans l'enquête judiciaire.

Le 4 février 2008, le Président de la Chambre des Représentants a soumis une proposition de loi relative aux certificats de bonne conduite, vie et mœurs pour avis à la Commission.

La Commission a tout d'abord rappelé le contexte légal : la Loi du 8 août 1997 relative au Casier judiciaire central crée un casier judiciaire central et prévoit le remplacement des casiers judiciaires communaux par un accès direct des administrations communales à certaines données du casier judiciaire central au moyen d'une liaison informatisée. Cette connexion informatique devait permettre, conformément aux articles 595 et 596 du Code d'instruction criminelle, la délivrance d'extraits du casier judiciaire en remplacement des certificats de bonnes conduites, vie et mœurs. Du temps où l'adoption d'un arrêté royal, les articles 595 et 596 du Code d'instruction criminelle ne sont toujours pas entrés en vigueur.

La proposition de loi soumise pour avis à la Commission répond à deux objectifs :

- donner aux certificats de bonnes conduites, vie et mœurs une base légale à titre temporaire jusqu'à l'adoption d'un arrêté royal ;
- assurer la sécurité des enfants par une vérification de l'existence ou non d'instructions ou d'informations judiciaires en cours.

Elle prévoit deux modèles de certificat selon l'usage auquel ce certificat est destiné :

- Le Modèle 1 est destiné aux administrations publiques,

aux particuliers et organismes privés, dans tous les cas qui ne requièrent pas l'obtention d'un certificat de modèle 2 ;

- le Modèle 2 est le certificat qui doit être demandé pour avoir accès à une activité qui relève de l'éducation, de la guidance psycho-médico-sociale, de l'aide à la jeunesse, de la protection infantile, de l'animation ou de l'encadrement de mineurs.

Les deux modèles doivent reprendre certaines informations enregistrées dans le casier judiciaire. La proposition de loi prévoit toutefois que le Modèle 2 contient, en plus des informations du casier judiciaire, un avis motivé donné sous la forme de la mention "est ou n'est pas de bonne conduite". Pour apposer cette mention, le chef de corps de la police locale peut consulter la Banque de données nationale générale policière (BNG).

La Commission :

- a souligné que la personne concernée est privée de la possibilité de contester les motifs pour lesquels figurerait sur son certificat la mention "n'est pas de bonne de conduite" puisqu'il n'y a aucune mention de ces motifs ;
- a constaté qu'aucun recours spécifique n'est prévu, et qu'étant donné l'absence de motivation formelle de la décision, ni la personne, ni les juridictions ne pourront avaliser ou sanctionner les motifs sur lesquels repose la décision ;
- s'est interrogée sur le rôle du chef de corps de la police locale : soit il appose la mention dès qu'une information apparaît dans la BNG (alors que la culpabilité de la personne concernée n'est pas établie), soit il appose la mention après avoir porté une appréciation (alors qu'il n'a pas de vision globale du dossier) ;
- a attiré l'attention sur le fait que les informations encodées dans la BNG ne sont pas toujours mises à jour ou suffisamment précises.

La Commission émet dès lors un avis favorable sur le Modèle 1 ainsi que sur les mentions du casier judiciaire qui

doivent figurer sur le Modèle 2, mais elle émet un avis défavorable sur l'avis motivé qui doit figurer sur le Modèle 2.

7.4.2 Modification de loi sur la conservation des données pour enquête sur des faits punissables

Avis n° 24/2008 du 02 juillet 2008 :

- transposition de la Directive européenne 2006/24/CE ;
- harmonisation des obligations des fournisseurs de communications électroniques ;
- conservation des données par ces fournisseurs dans le cadre d'une enquête sur des faits punissables.

Ces projets concernaient des propositions de transposition de la Directive européenne 2006/24/CE sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.

Les finalités de cette directive consistent dès lors à harmoniser les obligations imposées aux fournisseurs en matière de conservation de certaines données et à garantir que ces données soient disponibles à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne.

Pour diverses raisons, la Commission a émis un avis défavorable sur les deux projets. La principale raison de cet avis défavorable a été l'absence de la mention des éléments essentiels en matière de conservation des données dans l'avant-projet de loi et le projet d'arrêté royal notamment le type des données conservées, leur délai de conservation, leur mode de conservation, la justification de leur conservation, le type de faits criminels dont la répression justifie l'utilisation des données conservées, le champ d'application des projets et leur finalités, etc.

7.4.3 Communication de données sur des personnes condamnées au pénal

Avis n° 28/2008 du 03 septembre 2008 :

- questions parlementaires demandant des explications au ministre de la Justice ;
- droit à l'information du parlement ;
- droit à l'information de la presse.

Le ministre de la Justice reçoit de plus en plus de questions sur des personnes condamnées. Ces questions posées par des parlementaires dans le cadre de l'exercice de leur contrôle parlementaire et par les membres de la presse concernent des données relatives aux condamnations à proprement parler, aux faits et aux conditions liées à la décision relative à l'exécution de la peine.

Le ministre de la Justice a donc demandé le point de vue de la Commission sur le rapport entre le droit à la protection de la vie privée et le droit à l'information dans le cadre de l'exercice du contrôle parlementaire et le droit à l'information de la presse.

Dans son avis, la Commission a estimé qu'il ne ressortit pas à ses compétences d'interpréter la portée des droits constitutionnels et moins encore de régler les rapports entre le droit à la protection de la vie privée et le droit à l'information. Son avis se limite donc à reprendre une série de principes sur ces droits respectifs et à proposer quelques lignes de conduite.

Le droit à l'information implique que tout parlementaire a le droit de poser des questions écrites ou orales à un ministre. Conformément au règlement de La Chambre et du Sénat les questions concernant un cas personnel sont en principe irrecevables. Le ministre pourrait donc invoquer ces dispositions pour refuser de répondre à une question sur des données relatives à des personnes condamnées au pénal mais il peut aussi choisir d'invoquer le droit constitutionnel à l'information pour répondre à l'auteur de la question.

Conformément à la Loi vie privée, une interdiction de principe interdit le traitement des données judiciaires mais une exception est prévue pour les traitements qui se font sous la surveillance d'une autorité publique si ce traitement s'avère nécessaire pour l'exercice de ses tâches. Cette exception s'applique donc aux traitements des données judiciaires par le ministre. L'évaluation du caractère nécessaire de ce traitement à l'exercice de ses tâches relève toutefois d'un jugement d'opportunité et la Commission ne se prononce donc pas sur ce point.

L'interdiction de traitement des données judiciaires à caractère personnel ne s'applique pas non plus aux traitements de données à caractère personnel destinés à des finalités exclusivement journalistiques lorsque ce traitement concerne des données à caractère personnel rendues notoirement publiques par la personne concernée ou en étroite corrélation avec le caractère public de la personne concernée ou du fait dans lequel est impliquée la personne concernée. Dans ce cas, non plus, la Commission n'est pas compétente pour juger si, pour exercer ses tâches, le ministre doit répondre aux questions de la presse sur des personnes condamnées au pénal. Encore une fois, tout dépend des circonstances.

Qui plus est, la Commission a également fait référence à la disposition constitutionnelle qui stipule qu'un jugement est prononcé en audience publique. Toutes les données prononcées par le juge en audience publique sont donc déjà, en principe, publiques et disponibles pour les membres de la presse pour autant qu'ils aient été présents à l'audience, bien sûr. La Commission estime en outre que c'est à la magistrature qu'il revient de prime abord de communiquer la teneur d'un jugement, et ceci par le biais du magistrat de presse.

Enfin, la Commission a lancé au ministre la bouée stratégique suivante : lorsqu'un "cas personnel" fait référence à un problème ou une question d'ordre plutôt légistique, stratégique ou structurel, le ministre peut communiquer des données à caractère personnel pour permettre une meilleure

compréhension du problème. Mais, quoi qu'il en soit, c'est toujours au ministre qu'il revient de juger au cas par cas si une question dépasse ou non le cadre individuel, personnel et/ou casuistique. Lorsque ce n'est pas le cas, la Commission estime qu'une certaine réserve reste de mise.

7.4.4 Développements de la Loi caméras

Quelques développements observés en 2008 dans le domaine de la surveillance par caméras :

- arrêté d'exécution de la Loi caméras ;
- indication de la surveillance par caméras à l'aide d'un pictogramme ;
- déclaration des caméras de surveillance.

La nouvelle Loi caméras est en vigueur depuis le 10 juin 2007 (Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance). Cette loi stipule explicitement que la Loi vie privée reste d'application sur tous les aspects que la Loi caméras ne règle pas expressément.

Depuis l'entrée en vigueur de cette loi, la Commission a reçu différentes questions et plaintes concernant son application. Le nombre des déclarations thématiques (aussi bien pour les lieux fermés que pour les lieux ouverts) concernant les caméras de surveillance est en augmentation constante. À côté de cela, la Commission entretient également des contacts réguliers avec le Service public fédéral Intérieur, également compétent dans cette matière.

En ce qui concerne la législation, plusieurs nouveautés ont été introduites depuis l'entrée en vigueur de la Loi caméras.

En 2007, la Commission avait déjà émis un avis sur le pictogramme obligatoire conformément à la Loi caméras (avis n° 22/2007 du 13 juin 2007). Entretemps, cet arrêté royal a été publié au Moniteur belge du 21 février 2008, avec pour titre Arrêté royal du 10 février 2008 définissant la manière de signaler l'existence d'une surveillance par caméra. Son texte peut

être consulté via le site web de la Commission. Le 17 décembre 2008, la Commission a émis un avis sur un projet de modification de cet arrêté royal (avis n° 40/2008 du 17 décembre 2008). Concrètement, ce projet modifie légèrement les dimensions du pictogramme obligatoire.

Du fait notamment de la spécificité de la déclaration des caméras de surveillance, la procédure de déclaration prévue par la Loi caméras diffère légèrement de celle prévue par la Loi vie privée. Cette différence a été précisée par le biais d'un arrêté d'exécution comme le prescrit la Loi caméras. Concrètement, il s'agit de l'Arrêté royal du 2 juillet 2008 *relatif aux déclarations d'installation et d'utilisation de caméras de surveillance* (publié au Moniteur belge du 15 juillet 2008). La Commission s'est prononcée à ce sujet dans son avis n° 07/2008 du 27 février 2008. Cet arrêté royal peut également être consulté sur le site web de la Commission.

La Loi caméras stipule que le visionnage d'images en temps réel dans un lieu ouvert n'est admis que sous le contrôle des autorités compétentes pour permettre aux services de police d'intervenir immédiatement en cas d'infraction, de dommage ou d'atteinte à l'ordre public et de guider ces services au mieux dans leur intervention. La Loi prévoit aussi que les catégories de personnes habilitées à visionner ces images en temps réel peuvent être élargies. La Commission s'est prononcée sur ce point dans son avis 04/2008 du 27 février 2008. Au moment de la clôture de ce rapport annuel, le projet d'arrêté royal désignant ces catégories de personnes n'avait toutefois pas encore été publié au Moniteur belge.

Enfin, début 2008, il a aussi été proposé, par le biais d'un projet de loi portant des dispositions diverses, d'apporter des modifications à la Loi caméras à proprement parler. La Commission a émis un avis sur le texte initial du projet de loi (avis n° 08/2008 du 27 février 2008), mais les modifications de la Loi caméras proposées dans le projet de loi n'ont finalement pas été retenues. Le but de ces modifications était, entre autres, de régler une série de problèmes pratiques au

niveau de la déclaration et de l'indication de la surveillance par caméras mobiles par les services de police.

7.5 Sport et vie privée

En 2008, la World Anti-Doping Agency (WADA – Agence mondiale antidopage) a élaboré un standard international en matière de protection de la vie privée des sportifs dans le cadre des contrôles antidopage. La Commission a émis un avis sur ce projet de standard.

Avis n° 12/2008 du 19 mars 2008 :

- respect des règles de protection de la vie privée par les instances de contrôle ;
- cinquième Standard d'harmonisation des méthodes de travail des organisations antidopage ;
- comparaison avec la Loi belge sur la protection de la vie privée.

La Commission a constaté qu'étant donné que le standard proposé impose des normes minimales manifestement inspirées des instruments internationaux existants en matière de vie privée, il vise incontestablement une amélioration de la protection de la vie privée du sportif. Elle a par conséquent réservé un accueil favorable à cette initiative.

Elle a néanmoins comparé cet instrument à la Loi vie privée et il est ressorti de cette comparaison que le texte du Standard international pour la protection des renseignements personnels déroge à cette loi sur plusieurs points. La Commission a également souligné que les autorités belges qui seront éventuellement chargées de l'exécution de ce standard dans le droit interne devront tenir compte du fait que ce Standard impose des conditions minimales qui devront, le cas échéant, être complétées par l'imposition de mesures de protection plus strictes adaptées à législation belge relative à la protection de la vie privée.

7.6 Droit de propriété et vie privée

Dans la grande majorité des cas, la notion de "copropriété forcée" concerne des propriétaires d'appartements qui sont aussi automatiquement propriétaires d'une partie du bâtiment dans lequel ils habitent. Dans cette situation courante, les données relatives au propriétaire et à sa propriété sont considérées comme des données à caractère personnel auxquelles s'applique la Loi sur la protection de la vie privée. Des questions se posent sur cette application spécifique de la Loi vie privée auxquelles la Commission a répondu dans un avis d'initiative.

Avis n° 22/2008 du 11 juin 2008 :

- fixation d'un responsable de traitement en cas de copropriété ;
- légalité de la communication d'informations aux copropriétaires ;
- texte de référence pour certaines règles professionnelles ou codes de conduite.

La Commission est régulièrement interrogée via son Secrétariat sur l'application de la Loi vie privée dans le domaine de la copropriété forcée d'immeubles bâtis. Ces questions émanent tantôt des syndicats (professionnels ou non), tantôt des copropriétaires eux-mêmes.

L'avis émis a porté :

- d'une part, sur la détermination de la responsabilité des traitements réalisés dans le cadre ou à l'occasion de la gestion de la copropriété ; à cet égard, la Commission a estimé que l'association des copropriétaires doit manifestement être considérée comme le responsable des différents traitements de données à caractère personnel opérés par le syndic, mandataire ;
- d'autre part, sur la légalité de certains traitements spécifiques, à savoir, plus particulièrement :
 - o la communication par le syndic aux copropriétaires des nom et adresse d'autres copropriétaires à l'ensemble des copropriétaires ou à certains d'entre eux ;

selon la Commission, l'état d'indivision le permet sans que le demandeur ne doive expliciter davantage sa demande. La Commission a néanmoins suggéré aux syndicats de rappeler, à cette occasion, l'obligation de respecter la finalité de la communication,

- o la communication par le syndic à l'ensemble des membres de l'association des copropriétaires du compte de chaque copropriétaire ; à cet égard, la Commission considère que la présentation par le syndic d'un tableau de répartition des dépenses et charges par lot, en ce compris des dépenses privatives et de l'état de la dette de chaque membre, n'est pas en soi disproportionnée au regard de la Loi vie privée ; chaque locataire doit aussi pouvoir vérifier le décompte qui lui est présenté par son propriétaire sans néanmoins avoir accès aux données des comptes individuels des autres copropriétaires ou autres locataires.

Enfin, la Commission encourage l'élaboration d'éventuels codes de conduite professionnels ou sectoriels et a suggéré que les copropriétés adoptent en assemblée générale des résolutions précises quant aux pouvoirs éventuellement conférés au conseil de gérance et aux missions dévolues du syndic et à certaines de leurs modalités, par exemple, lors de la présentation des comptes à l'assemblée générale ou d'une autorisation d'intenter une action en justice contre un des copropriétaires.

7.7 Transport et mobilité

La Direction pour l'Immatriculation des Véhicules (DIV) gère un fichier central qui contient toutes les données pertinentes sur un véhicule et son propriétaire. Dans ce cadre, l'année dernière, la Commission a émis les avis suivants :

- accès au fichier de données de la DIV ;
- création d'un nouveau fichier central de données relatives aux véhicules.

7.7.1 Accès au fichier de données de la DIV

Avis n° 37/2008 du 26 novembre 2008 :

- perception des rétributions de stationnement par les instances privées ;
- identification des mauvais payeurs par le biais de leur plaque d'immatriculation ;
- accès direct aux données de la DIV par les entreprises d'exploitation de parkings.

Le 26 novembre 2008, dans son avis n° 37/2008, la Commission a rendu un avis positif sur le projet de loi relative à l'accès direct des entreprises d'exploitation de parkings à la DIV.

Ces dernières années, aussi bien la Commission que le Comité sectoriel pour l'Autorité Fédérale (ci-après "le Comité") avaient déjà émis un avis sur cette problématique. En 2003, la Commission avait émis un avis défavorable "concernant l'accès direct et indirect au répertoire par des sociétés privées et des huissiers de justice, si ces derniers n'interviennent pas dans le cadre d'une procédure judiciaire". Dans sa délibération n° 02/2007 du 7 février 2007, le Comité signalait, quant à lui, l'absence de toute base légale spécifique permettant de transférer le pouvoir de perception d'une redevance à une instance privée.

Ce projet de loi avait pour objectif "de créer un fondement légal clair en matière d'accès à la DIV par les communes et leurs concessionnaires en matière de stationnement sur la voie publique, en vue de permettre l'identification des personnes qui ne s'acquittent pas de la redevance de stationnement à l'aide de la plaque d'immatriculation." Dans sa demande, le demandeur précisait aussi expressément que "ce projet de loi ne concerne toutefois nullement la problématique de la base légale du répertoire d'immatriculation des véhicules. Cette problématique fera l'objet d'un projet de loi global relatif à la base de données centrale des véhicules déjà pendant devant la Commission". L'objectif visé était celui de l'encadrement légal prévu de la source authentique des données relatives aux véhicules, traité par la Commission dans ses avis n° 23/2008 du 11 juin 2008 et n° 42/2006 du 18 octobre

2006. La Commission a pris acte de cette limitation.

La Commission a émis un avis favorable sur ce projet de loi, à condition que la procédure d'autorisation au niveau du Comité prévue à l'article 36bis de la Loi vie privée soit suivie. La Commission a également rappelé que ce projet de loi ne concerne qu'un aspect partiel seulement de l'ensemble de cette problématique et que d'autres points doivent encore être réglés : la DIV ne repose, elle-même, toujours pas sur une base légale suffisante, la communication de données à caractère personnel en provenance de la DIV doit être autorisée et pour satisfaire aux dispositions de la Loi vie privée, les conditions de cette communication doivent être stipulées dans les marchés publics et les conventions de concession conclues avec les concessionnaires.

Aujourd'hui, ce projet de loi a été intégré dans les articles 14 à 16 compris de la Loi du 22 décembre 2008 portant des dispositions diverses.

7.7.2 Création d'un nouveau fichier central de données relatives aux véhicules

Avis n° 23/2008 du 11 juin 2008 :

- base légale de la réforme du répertoire des véhicules ;
- utilisation des données relatives aux véhicules dans le domaine pénal et fiscal ;
- protection et autorisation d'échange des données relatives aux véhicules.

Le 18 octobre 2006, la Commission a émis un avis (n°42/2006) défavorable sur l'avant-projet de loi portant création d'une source authentique des données relatives aux véhicules. Le 19 février 2008, le ministre de la Mobilité a demandé l'avis de la Commission sur une version modifiée de cet avant projet.

Par cet avant-projet modifié, le ministre avait pour objectif de mettre en place une base légale suffisante pour la réforme prévue du traitement "répertoire des véhicules". Ce traite-

ment est encore actuellement une application mainframe gérée par la Direction pour l'Immatriculation des Véhicules (DIV) de la Direction générale Mobilité et Sécurité routière du SPF Mobilité et Transports (www.mobilit.fgov.be). L'Arrêté royal du 20 juillet 2001 (Arrêté royal relatif à l'immatriculation de véhicules, Moniteur belge du 8 août 2001) constitue la base réglementaire actuelle de ce traitement et est complété par différents protocoles d'accord conclus entre la DIV et différents services.

Pour que l'avant-projet respecte l'évolution du principe de légalité et le principe de transparence de la jurisprudence (article 8 de la CEDH et article 22 de la Constitution), la Commission a conseillé au législateur de suivre les étapes suivantes dans la rédaction ultérieure de la réglementation relative à la source authentique :

- les flux de données existants en vertu de l'Arrêté royal du 20 juillet 2001 et les protocoles d'accord existants doivent être répertoriés avant de développer les flux de données existants et pouvoir ensuite leur donner une base légale suffisante dans l'avant-projet plutôt que de devoir se baser en partie sur l'AR du 20 juillet 2001, en partie sur les protocoles d'accords conclus et en partie sur la pratique administrative ;
- les éléments essentiels du traitement ne peuvent être réglés que dans l'avant-projet. La Commission a toutefois précisé à ce sujet que si la loi définit de manière suffisamment claire les futures utilisations potentielles (données potentielles, fournisseurs et destinataires potentiels), le Roi pourra exécuter ces dispositions par la suite.

Dans cet avis, La Commission a également rappelé que le Comité sectoriel pour l'Autorité Fédérale doit accorder une autorisation pour les flux de données électroniques via la DIV (article 36bis de la Loi vie privée). Dans ce cadre, la Commission ne s'est pas montrée partisane de la création d'un nouveau Comité sectoriel mobilité et transport mais a plutôt conseillé de viser la plus grande cohérence possible avec les

modèles et procédures existants des banques-carrefour et des instances qui les contrôlent (comités sectoriels).

En tenant compte de cette logique législative, la Commission a d'abord examiné les échanges de données existants et a ensuite fait des remarques complémentaires sur l'avant-projet.

En ce qui concerne les échanges de données existants, la Commission a estimé que :

- les finalités existantes et les finalités visées, les données à caractère personnel, les fournisseurs de données et les utilisateurs de données à caractère personnel doivent être définis dans la loi (article 22 de la Constitution) ;
- les échanges de données existants via des protocoles d'accord sont illégaux s'ils ne respectent pas le cadre légal existant (article 8 de la CEDH, article 22 de la Constitution, article 36bis de la Loi vie privée) ; bien que les accords administratifs puissent être un instrument légitime, ils doivent reposer sur une base réglementaire et s'avérer suffisamment transparents s'ils prévoient des échanges de données à caractère personnel et génèrent de ce fait des ingérences dans la vie privée (article 8 de la CEDH) ;
- l'absence de toute précision concernant les mesures de sécurité actuellement prévues dans la réglementation et les accords administratifs montre que la politique de sécurité de la DIV est défectueuse.

En ce qui concerne l'avant-projet, la Commission a rappelé les remarques faites dans son premier avis à ce sujet. Elle a en outre estimé que :

- le responsable du traitement doit être explicitement mentionné dans la loi et que les termes "responsable du traitement" doivent remplacer les autres termes tels que "service de gestion" pour permettre l'application correcte de la Loi vie privée ;
- un stockage centralisé et une journalisation soumis à un contrôle fédéral externe au niveau de la DIV semblent l'op-

tion qui offre le plus de garanties en matière de protection des données à caractère personnel.

En tenant compte de ces remarques, la Commission a émis un nouvel avis négatif sur cet avant-projet modifié.

7.8 Listes négatives et vie privée

La problématique de ce qu'on appelle les listes noires est toujours d'actualité. En 2008, la Commission a émis un neuvième avis sur la question.

Avis n° 34/2008 du 24 septembre 2008 :

- projet de loi sur l'encadrement réglementaire des listes négatives ;
- apport de nuances au point de vue formulé antérieurement ;
- indépendance totale.

Le 24 septembre 2008, la Commission a émis l'avis n° 34/2008 qui concernait une proposition de loi relative à l'encadrement des listes négatives. Ce n'était pas la première fois que la Commission adoptait un point de vue dans cette problématique et cet avis fait donc référence à huit autres avis émis entre 1998 et 2007 dans le même contexte. Tout au long de ces années, le point de vue de la Commission est toujours resté constant.

La Commission a rappelé à ce sujet que :

- les listes négatives (externes) sont en principe des ingérences dans la vie privée interdites, sauf dans les cas fixés par la loi (article 8 de la CEDH) ;
- seul le législateur dispose - sur la base de l'article 22 de la Constitution - de la compétence d'introduire un système général de collecte, traitement et transfert de données à caractère personnel à grande échelle pour plusieurs finalités avec la participation d'un grand nombre d'organismes publics ou privés. La Commission demande donc la mise en place d'un encadrement légal des listes négatives non

réglementées existantes, notamment des listes négatives de Datassur et Preventel ;

- les éléments essentiels des listes négatives doivent être fixés par une loi. Il s'agit surtout de la définition de la finalité, des conditions d'enregistrement, des situations et des conditions dans lesquelles le responsable peut valablement légitimer son traitement en vertu de l'article 5 f) de la Loi vie privée, de la nature des données, du délai de conservation et de la diffusion et de l'accès aux données ;
- les finalités des listes négatives doivent être clairement formulées. Les finalités "lutte contre la fraude" et "protection de la sécurité" ne sont pas suffisamment claires.

Quelques nuances doivent aussi être apportées au point de vue formulé précédemment. Ces nuances sont, entre autres, que la Commission préconise :

- de tendre vers une cohérence maximale avec les listes négatives réglementées dans le domaine du crédit à la consommation (sur la base de la Loi CCP du 10 août 2001) en excluant l'applicabilité de la nouvelle loi aux listes négatives existantes qui tombent dans le champ d'application de cette réglementation ;
- une obligation de déclaration des listes négatives pour lutter contre la discrimination ; une telle obligation existe déjà dans le secteur du crédit à la consommation ;
- un système d'autorisations uniques et de déclarations de conformité reposant sur une base légale comme c'est déjà largement le cas en France ;
- l'introduction d'une garantie de réciprocité au niveau de l'échange des données à caractère personnel avec les autres pays de l'UE qui appliquent des régimes beaucoup plus stricts, notamment les listes négatives multisectorielles ou les listes sectorielles *zero tolerance* ;
- une compétence d'exécution pour le Roi.

A ce niveau, une indépendance totale de la Commission (article 28 de la Directive 95/46/CE) par rapport aux points de vue extérieurs adoptés sur les listes négatives est également indispensable. La Commission a pris acte de l'argument avancé

par les représentants des organisations de consommateurs selon lequel l'Ombudsman des assurances dépendrait totalement des compagnies d'assurances et ne serait donc pas géré sur une base paritaire, comme c'est notamment le cas dans les services bancaires. Cela signifie qu'en tant qu'organe, l'Ombudsman ne satisfait pas à la condition d'indépendance totale prévue à l'article 28 de la Directive 95/46/CE. Étant donné que, conformément à la procédure prévue dans la proposition de loi, la Commission doit attendre l'avis externe du Conseil de la Consommation, elle a précisé qu'elle ne peut en aucun cas s'estimer liée par cet avis externe.

7.9 Technologie de l'information et de la communication

L'aspect technique de la protection de la vie privée et des données aussi a été à l'ordre du jour en 2008 et ceci dans le cadre des activités suivantes :

- les activités du Bureau de Normalisation ;
- la plateforme de concertation sur la protection des informations.

7.9.1 Les activités du Bureau de Normalisation

- révision des normes ISO ;
- examen de conformité à la législation relative à la protection de la vie privée.

Comme l'année dernière, cette année encore, le Secrétariat de la Commission s'est impliqué dans les travaux de normalisation en cours au sein du Bureau de Normalisation (NBN – <http://www.nbn.be>) et a participé aux travaux des *Working Groups* 1, 3 et 5 du Comité technique JTC1/SC27 (*Information Technology/Security Techniques*) concernant la révision des normes ISO susceptibles d'influer sur le respect de la vie privée, en veillant notamment à la cohérence de ces normes avec la Loi relative à la protection de la vie privée.

Cette année, ces travaux ont porté sur les normes ou projets suivants :

- ISO 24760 "A framework for identity management" ;
- ISO 29100 "A privacy framework" ;
- ISO 29101 "A privacy reference architecture".

7.9.2 La plateforme de concertation sur la protection des informations

- problématique commune en matière de protection des informations ;
- groupe de travail classification.

La Commission, représentée par un commissaire et des membres de son Secrétariat, a participé aux travaux de la plateforme de concertation sur la sécurité des informations.

Cette plateforme a été instituée par le Conseil des ministres fin 2005 afin d'aborder les problématiques communes aux différents organismes qui la composent en matière de sécurité des informations.

Les organismes participant à cette plateforme sont :

- le Service Général du Renseignement et de la Sécurité (SGRS) du ministère de la Défense ;
- l'Institut belge des services postaux et des télécommunications (IBPT) ;
- la Commission de la protection de la vie privée ;
- le Centre de crise du SPF Intérieur ;
- la Federal Computer Crime Unit ;
- la Direction Générale de Contrôle et de Médiation du SPF Économie ;
- le SPF Fedict ;
- la Banque Carrefour de la sécurité sociale ;
- l'Agence nationale de Sécurité (ANS) – Affaires Étrangères ;
- la Sûreté de l'État.

Au sein de cette plateforme, la Commission a spécialement collaboré cette année aux travaux du groupe de travail classification, présidé par l'Agence Nationale de Sécurité (ANS) chargé d'aborder toute une série de problèmes liés à la classification, notamment la révision des niveaux de classifi-

cation, l'habilitation des personnes ainsi que l'évaluation, la certification et l'homologation des systèmes qui traitent des informations classifiées.

7.10 Finances et vie privée

En 2008, une série de projets de textes législatifs ont été soumis au secteur financier de la Commission. Ces projets de textes traitaient de :

- la Commission bancaire, financière et des assurances (CBFA) bénéficie d'une exonération partielle des obligations imposées par la Loi vie privée ;
- une modification dans la réglementation de la Centrale des crédits aux particuliers (CCP) ;
- la recherche des titulaires de comptes et coffres dormants.

7.10.1 Exonération partielle des obligations imposées par la Loi vie privée pour la CBFA

Avis n° 26/2008 du 23 juillet 2008 :

- données en provenance de tiers ;
- traitement de données dans le cadre d'une procédure administrative de sanction ;
- secret professionnel de la CBFA.

La Commission a émis un avis favorable sur ce projet d'arrêté royal qui permet de déroger à certains articles de la Loi vie privée lorsque la Commission Bancaire Financière et des Assurances exerce des missions de police administrative.

7.10.2 Modification dans la réglementation de la Centrale des crédits aux particuliers (CCP)

Avis n° 35/2008 du 08 octobre 2008 :

- mises à jour des données de la CCP ;
- critères légaux de fixation de la date du premier défaut de paiement ;
- délai d'enregistrement des défauts de paiement.

Le Commission a émis un avis favorable sur le projet dont l'essentiel correspond à une demande du Comité d'accompagnement de la Centrale. Au lieu de faire commencer le délai maximum de conservation (10 ans) des données dans le volet négatif de la Centrale à compter de la date du premier enregistrement d'un défaut de paiement, c'est dorénavant la date de ce premier défaut de paiement qui sera prise en considération. Ce changement a pour objectif de ne pas pénaliser le consommateur dont le prêteur a tardé à communiquer les données à la Centrale et de ne pas défavoriser le consommateur qui a régularisé à un moment donné sa dette par rapport à un consommateur qui ne l'a jamais régularisée.

Un second changement important introduit par ce projet d'arrêté royal consiste à obliger les sociétés de recouvrement de créance, cessionnaires ou subrogées aux prêteurs, inscrites auprès du SPF Économie, à communiquer les informations à la Centrale en vue d'accroître la rapidité de la mise à jour des données de la Centrale. Il y va de l'intérêt du consommateur.

7.10.3 Recherche des titulaires de comptes et coffres dormants

Avis n° 31/2008 du 24 septembre 2008 :

- AR d'exécution de la Loi du 24 juillet 2008 ;
- données du Registre national et de la Banque Carrefour de la sécurité sociale ;
- accès indirect.

En date du 24 septembre 2008, la Commission s'est prononcée favorablement par voie d'avis sur l'avant-projet d'Arrêté royal portant application des articles 26 à 28, 31 et 36 de la Loi du 24 juillet 2008 portant dispositions diverses (I), lequel organise l'utilisation du Registre national et des données d'identification du registre Banque Carrefour de la sécurité sociale pour la recherche des titulaires de comptes et coffres dormants et des bénéficiaires de contrats d'assurance dormants. La Commission a rappelé la compétence d'autorisation de ses Comités du Registre national et de la Sécurité

Sociale et de la Santé en la matière.

Aux termes de la Loi programme du 24 juillet 2008, les établissements bancaires et compagnies d'assurances se sont vu confier la mission de rechercher les titulaires de comptes et coffres dormants ainsi que les bénéficiaires de contrats d'assurance dormants. L'avant-projet d'arrêté royal soumis à l'avis de la Commission organise l'accès aux registres précités.

La Commission a fait part de sa satisfaction au sujet la configuration prévue pour l'organisation des accès aux registres dans la mesure où ceux-ci ne seront pas directement mis à disposition des banques mais accessibles via un point central chargé de rassembler les requêtes d'accès motivées des établissements bancaires et compagnies d'assurances et d'adresser aux organismes bancaires respectifs les réponses à leurs requêtes dûment motivées. Ce type de configuration (accès au Registre national pour un secteur déterminé via un point central assurant un contrôle des accès sur le secteur) a déjà été recommandé par la Commission dans son avis 16/2008 du 9 avril 2008.

A ce sujet, la Commission a conseillé que des mesures soient adoptées par ce point central pour se prémunir contre tout accès illégitime aux données des registres concernés et contre tout détournement de finalité de la part des organismes bancaires et compagnies d'assurances concernés. Il conviendra ainsi de veiller à ce que les données soient communiquées aux seuls membres du personnel chargés, au sein des organismes concernés, de procéder aux recherches et contacts avec les titulaires et/ou bénéficiaires des comptes, coffres et assurances dormants. Une formation spécifique de ce personnel ainsi que l'exigence d'une motivation adéquate de leurs requêtes d'accès participera également à la gestion correcte des accès aux registres. Un login précis des accès devrait également être réalisé afin que, en cas d'exercice par les personnes concernées de leur droit d'accès visé à l'article 6 de la Loi du 19 juillet 1991 relative aux registres de la population,

une réponse adéquate (qui a demandé accès à quoi ?) leur soit fournie tant par le point central que par les établissements bancaires et compagnies d'assurances concernés.

La Commission a ensuite procédé à l'examen de la liste des données mises à la disposition des banques et compagnies d'assurances en requérant du demandeur de l'avis d'une part que l'accès aux données "nationalité" et "résidence principale" soit plus amplement justifié ou à défaut supprimé et d'autre part que des précisions relatives au contexte dans lequel certains types de consultations du Registre national pourront être opérés soient insérées dans le texte légal.

Enfin la Commission considère que, dans l'hypothèse où une compagnie d'assurances se trouve en situation d'impossibilité d'exécuter une clause bénéficiaire d'un contrat d'assurance vie pour défaut de détermination du bénéficiaire, il convient d'appliquer l'article 107 de la Loi du 25 juin 1992 sur le contrat d'assurance terrestre.

7.11 Amélioration des services de la Commission

Soucieuse d'être à la hauteur de sa vocation d'intermédiaire vis-à-vis de citoyens, des entreprises et du secteur public – tant sur la scène nationale qu'internationale – chaque année, la Commission continue à améliorer les services qu'elle propose. En 2008, les principaux efforts consentis dans ce domaine ont concerné :

- la note juridique sur le marketing direct ;
- la traduction de son site web en anglais.

7.11.1 Note juridique sur le marketing direct

- concertation avec les parties concernées ;
- adaptation de l'ancienne note ;
- délimitation plus précise de la notion de "marketing direct" sur la base de la Loi vie privée.

Ces dernières années, différents points de vue écrits ont été

adoptés au nom de la Commission dans le cadre de procédures bilatérales de médiation concernant plusieurs grands responsables belges de traitements à des fins de marketing direct. On ne disposait cependant jusqu'ici d'aucune note exhaustive dans laquelle la Commission exprimait son point de vue actuel sur les nombreux aspects de cette matière.

Le 5 juin 2008, la Commission a donc pris l'initiative de publier une note juridique sur la problématique du marketing direct. Cette note est basée sur l'adaptation et la refonte complète d'une ancienne note sur le sujet. Sur la base d'une étude comparative de la situation au niveau d'autres commissions de la protection de la vie privée effectuée début 2008, la Commission a en outre également retenu neuf autres options supplémentaires.

Pour une meilleure protection de la vie privée dans le cadre des traitements à des fins de marketing direct :

- il est indispensable de faire une meilleure distinction entre le marketing direct sur une base (pré)contractuelle et les autres formes de marketing direct (article 5, b) de la Loi vie privée). Il faut donc faire une distinction entre le marketing direct utilisé dans le cadre d'une gestion normale de la clientèle (article 5 b) Loi vie privée) et les autres sources et formes de marketing direct à propos desquelles la Commission reçoit de nombreuses questions et plaintes ;
- les conditions d'invocation de l'intérêt pondéré en vue d'actions de marketing direct (article 5, f) de la Loi vie privée) ont été précisées ;
- l'article 5, f) Loi vie privée ne doit être considéré que comme une catégorie résiduaire des catégories 5, a) et 5, b) de l'article 5 de la Loi vie privée ;
- le consentement est posé comme une condition au courtoage d'adresses et au profilage à des fins de marketing direct, pour les traitements qui ne sont pas a priori légitimés par un contact direct avec la personne concernée (article, 5 b) de la Loi vie privée) ;
- la notion de (non-)respect du "principe de loyauté" a été expliquée à l'aide d'exemples concrets (article 4, § 1^{er}, 1^o de

la Loi vie privée) ;

- l'interprétation de la notion "utilisation incompatible" a été précisée (article 4, § 1^{er}, 2^o de la Loi vie privée) ;
- la Commission a rappelé l'obligation d'utiliser un délai de conservation des données relatives aux personnes avec lesquelles il n'existe aucune relation contractuelle directe (prospects) (article 4, § 1^{er}, 4^o et 5^o de la Loi vie privée) ;
- sur la base du principe de loyauté (article 4, § 1^{er}, 1^o de la Loi vie privée), la Commission préconise l'obligation de déclaration proactive au niveau de la source d'une action de marketing direct lorsqu'il n'y a pas de contact direct avec la personne concernée (par exemple en cas de commerce des données) ;
- la Commission invite à la prudence en cas d'utilisation de clauses d'information standards et insiste sur le caractère plus clair et plus compréhensible des informations.

7.11.2 Traduction du site web en anglais

- information et assistance au niveau international ;
- progressive et évolutive.

En raison de l'internationalisation croissante de son domaine d'activité, en 2008, la Commission a décidé de traduire son site web, principalement consacré à des thèmes belges et internationaux, en anglais pour le rendre accessible à un plus vaste public. Même si son contenu est sans cesse élargi et actualisé, la version anglaise n'est donc pas le reflet exact des pages proposées en français et en néerlandais. Les lecteurs intéressés peuvent avoir accès aux pages du site web en anglais en cliquant sur le bouton "anglais" en haut à droite de l'écran.

8 Les principales activités internationales de la Commission

8.1 Conférences internationales

- Conférence européenne des Commissaires à la protection des données ;
- Conférence mondiale des Commissaires à la protection des données ;
- Conférence de l'AFAPDP.

8.1.1 Conférence européenne des Commissaires à la protection des données – "What outlook for privacy in Europe and beyond?"

- évolutions de la notion de vie privée dans le contexte de la sécurité, de la notion de vie privée dans le monde des affaires, etc. ;
- déclaration sur la gestion intégrée des frontières de l'UE.

Les autorités de protection des données des États membres de l'Union européenne et du Conseil de l'Europe se réunissent tous les ans au printemps pendant deux jours. Des autorités régionales et locales ainsi que des Autorités de Contrôle Communes (ACC) relevant du troisième pilier de l'Union sont également présentes. Les débats, en réunions plénières, portent sur les meilleures pratiques et sur d'autres sujets d'intérêt commun, et la conférence s'achève habituellement par l'adoption d'une série de documents importants.

La Conférence 2008 a eu lieu à Rome les 17 et 18 avril et a traité entre autres des évolutions en matière de "Vie privée et sécurité", "Vie privée et monde globalisé des affaires", "Vie privée et technologies" et "Vie privée en Europe et au-delà". Cette conférence s'est achevée par l'adoption d'une déclaration relative à une série de mesures annoncées par la Commission européenne relatives à la gestion intégrée des frontières de l'Union. Il est notamment envisagé aux termes

de celles-ci de créer un système d'entrée/sortie comprenant l'enregistrement d'informations concernant les voyageurs, l'utilisation de données biométriques et, éventuellement, la création d'une base de données européennes destinée à stocker ces données. Bien que motivées par un objectif légitime - rendre les frontières de l'Union plus sûres tout en facilitant les déplacements des voyageurs - ces mesures impliquent des traitements de données à grande échelle susceptibles d'entraîner des intrusions significatives dans la vie privée. La Conférence souligne à cet égard la forte dépendance à l'égard des données biométriques, le manque de preuves appuyant la nécessité de nouveaux systèmes et l'absence d'évaluation des systèmes existants.

8.1.2 Conférence mondiale des Commissaires à la protection des données – "Protecting privacy in a borderless world"

- protection des mineurs ;
- protection de la vie privée sur les sites de réseaux sociaux ;
- protection de la vie privée dans un monde sans frontières ;
- représentation auprès d'organisations internationales ;
- introduction d'une journée internationale de la protection de la vie privée.

Comme chaque année, la Commission de la protection de la vie privée a participé à la Conférence internationale des Commissaires à la protection des données et de la vie privée. Cette conférence s'est déroulée à Strasbourg, du 15 au 17 octobre, à l'invitation de la Commission nationale de l'informatique et des libertés française (CNIL - www.cnil.fr) et de l'autorité de protection des données fédérale allemande (BFDI - <http://www.bfdi.bund.de>). Elle a réuni 600 participants de 60 pays

autour du thème de la protection de la vie privée dans un monde sans frontières.

Protection des mineurs

Parmi les nombreux sujets traités lors de cette conférence, la protection des mineurs et de leur vie privée était au cœur des débats. Les représentants se sont mis d'accord sur la nécessité d'une pédagogie à destination des jeunes pour leur apprendre comment naviguer sur internet tout en préservant leurs propres droits à la vie privée ainsi que ceux des autres internautes.

Une résolution adoptée au terme de la Conférence invite à cet effet les opérateurs de sites web à adapter leurs politiques de protection de la vie privée aux besoins des mineurs, en les informant en langage clair et simple des risques qu'ils peuvent courir en ligne.

Résolution sur la protection de la vie privée dans les services de réseaux sociaux

Les services de réseaux sociaux sont, depuis plusieurs années, devenus très populaires. Ces services offrent notamment à leurs abonnés les moyens d'interagir en fonction de profils personnels qu'ils ont eux-mêmes créés et qui encouragent à révéler des informations personnelles à un niveau sans précédent, sur soi et sur les autres. Si ces services de réseaux sociaux offrent une nouvelle gamme de possibilités de communication et d'échange en temps réel de toutes sortes d'informations, l'utilisation de ces services peut cependant menacer la vie privée de leurs utilisateurs – et celle d'autres personnes : ces nouveaux réseaux rendent en effet publiques (au niveau mondial même) quantités de données personnelles, y compris des images et des vidéos numériques. Entre autres risques, la Conférence relève celui des utilisations ultérieures, par exemple la pratique de consultation par les responsables des ressources humaines des profils d'utilisateurs candidats ou employés ou encore l'utilisation des informations contenues dans les profils ou des données

de connexion par les fournisseurs de réseaux sociaux pour envoyer des messages de marketing ciblés à leurs utilisateurs. La Conférence a également dénoncé les risques d'usurpation d'identité, favorisés par la large disponibilité des données personnelles dans les profils et le risque de piratage des profils par des tiers non autorisés.

La Conférence s'est déclarée convaincue de la nécessité de réaliser une campagne d'information poussée impliquant tous les acteurs publics et privés (des instances gouvernementales aux écoles, et des fournisseurs de services de réseaux sociaux aux associations de consommateurs et d'utilisateurs, incluant également la participation des Commissaires à la protection des données et de la vie privée eux-mêmes) pour prévenir les divers risques liés à l'utilisation des services de réseaux sociaux. Enfin, la Conférence a également formulé un série de recommandations qui s'adressent tant aux utilisateurs qu'aux fournisseurs de réseaux sociaux.

Le lecteur intéressé les trouvera sur le site de la Conférence: <http://www.privacyconference2008.org>

Les 3 résolutions suivantes s'inscrivent plus particulièrement dans le thème "Protéger la vie privée dans un monde sans frontière" :

Résolution sur l'urgence de protéger la vie privée dans un monde sans frontières et l'élaboration d'une proposition conjointe d'établissement de normes internationales sur la vie privée et la protection des données à caractère personnel

Cette Conférence a appelé à l'élaboration d'un instrument juridique universel contraignant en matière de protection des données et de la vie privée. Dans cette perspective, la Conférence a indiqué :

- qu'elle soutient les efforts du Conseil de l'Europe pour promouvoir le droit fondamental à la protection des données et de la vie privée et invite les États non membres du Conseil de l'Europe qui sont en mesure de le faire à considérer l'invitation qui leur est faite par le Conseil de

l'Europe d'adhérer à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention n° 108) et à son protocole additionnel ;

- qu'elle soutient les initiatives de l'APEC, de l'OCDE et d'autres organisations régionales et forums internationaux pour le développement de moyens effectifs de promotion de standards internationaux de protection des données et de la vie privée et ;
- qu'elle met sur pied un groupe de travail chargé d'élaborer - au départ des principes et droits relatifs à la protection des données à caractère personnel existant dans les différents environnements géographiques du monde – un ensemble de principes et de droits qui, reflétant et complétant les textes existants, permettraient d'atteindre un degré maximum d'acceptation internationale tout en garantissant un haut niveau de protection.

Le lecteur intéressé est invité à prendre connaissance de l'intégralité de cette résolution à l'adresse : <http://www.privacyconference2008.org>

Résolution concernant la création d'un Comité directeur relatif à la représentation lors de réunions des organismes internationaux

La Conférence a décidé de développer un mécanisme permettant sa représentation – soit celle des autorités de protection des données – au sein d'organismes internationaux gouvernementaux et non gouvernementaux afin de mieux promouvoir les principes universels de base de la protection des données et de la vie privée au niveau international. La Conférence crée à cet effet un comité permanent chargé d'étudier l'intérêt qu'il y aurait à obtenir le statut d'observateur auprès d'organismes internationaux tels que l'Organisation pour la coopération et le développement économiques (OCDE), l'Organisation internationale de normalisation (ISO), le Conseil de l'Europe (Comité consultatif de la Convention n° 108), l'Association de coopération économique Asie Pacifique (APEC), la Commission du droit

international des Nations-Unies, l'Union internationale des télécommunications et l'Unesco.

Le lecteur intéressé est invité à prendre connaissance de l'intégralité de cette résolution à l'adresse : <http://www.privacyconference2008.org>

Résolution visant la mise en place d'une journée ou d'une semaine internationale de la protection de la vie privée et des données personnelles

La Conférence a également résolu d'œuvrer à la mise sur pied d'une journée ou d'une semaine annuelle pendant laquelle la protection de la vie privée et des données personnelles serait célébrée et promue au niveau mondial. Si certaines initiatives régionales existent - telle la journée européenne de la protection des données initiée en 2007 par le Conseil de l'Europe avec l'appui de la Commission européenne - une approche annuelle mondiale fournirait d'excellentes occasions de sensibiliser les citoyens. La Conférence a également résolu de mettre en place un groupe de travail chargé de faire progresser cette initiative, laquelle pourrait voir le jour dès 2010.

Le lecteur intéressé est invité à prendre connaissance de l'intégralité de cette résolution à l'adresse : <http://www.privacyconference2008.org>

8.1.3 Conférence de l'AFAPDP

- collaboration et initiatives de formation dans les pays francophones ;
- sensibilisation.

C'est également à Strasbourg que l'Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP) a tenu sa seconde conférence. Répondant à l'invitation des organisateurs, le Secrétariat de la Commission y a développé, dans le cadre de la session ouverte consacrée à la sensibilisation et à la formation aux bonnes pratiques, la problématique de la prise en compte des dimensions techniques au cours d'une présentation intitulée : "Mobilité et géolocalisation".

De plus amples informations à ce propos sont disponibles à l'adresse suivante : http://www.privacyconference2008.org/index.php?page_id=69.

L'AFAPDP est une jeune association mise sur pied en 2006-2007. Elle poursuit l'objectif de favoriser la coopération et les actions de formation entre les pays de la francophonie dans le domaine de la protection des libertés et notamment, de celle des données personnelles. Elle s'est également donné pour mission de participer au dialogue relatif à la mise en œuvre de la protection de la vie privée et des données personnelles avec les organisations internationales telles que les Nations-Unies, l'Union européenne ou encore l'Association de coopération économique Asie – Pacifique (APEC). Elle a reçu le statut d'observateur aux travaux du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe (Convention n°108).

8.2 Groupe de travail Article 29

- Article 29 Groupe de protection des données
- Technology Subgroup

8.2.1. Groupe de travail Article 29 - Groupe de protection des données

- groupe de travail européen ;
- application harmonisée de la réglementation UE en matière de protection de la vie privée.

Le Groupe de travail Article 29, qu'est-ce que c'est ?

Le Groupe 29 est un groupe de travail européen sur la protection des données. Les "commissions vie privée" des 27 états membres de l'Union européenne y sont représentées ainsi que le Contrôleur européen à la protection des données (CEPD). La Commission de la protection de la vie privée en fait donc partie. Le Groupe 29 rend régulièrement des avis

sur des divers thèmes intéressant la protection de la vie privée et des données à caractère personnel dans le but de promouvoir une application harmonisée de la réglementation en cette matière dans les 27 États membres de l'Union.

Le Groupe 29 se réunit en assemblée plénière cinq fois par an à Bruxelles. Le travail préparatoire se fait toutefois tout au long de l'année au sein de divers groupes de travail auxquels participe le Secrétariat de la Commission de la protection de la vie privée.

Tous les avis auxquels il est fait référence dans les paragraphes qui suivent sont disponibles à l'adresse : http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_fr.htm (rubrique "Documents adoptés").

Le site web du Contrôleur européen de la protection des données : <http://www.edps.europa.eu/EDPSWEB/edps/pid/r?lang=fr>

Parmi les avis rendus en 2008 par le Groupe 29, nous avons retenu les suivants :

Mise à jour de l'Avis 2/2007 concernant l'information des passagers au sujet du transfert de données des dossiers passagers (Passenger Name Record – PNR) aux autorités américaines (groupe de travail "PNR")

En juillet 2007, l'Union européenne a conclu un nouvel accord avec les Etats-Unis d'Amérique sur la communication de données relatives aux passagers (données PNR) par les transporteurs aériens au ministère américain de la Sécurité intérieure (United States Department of Homeland Security – DHS). Suite à cet accord, les agences de voyage, les compagnies aériennes et autres organisations fournissant des prestations de services de voyage aux passagers effectuant un vol à destination et au départ des Etats-Unis, ont l'obligation de fournir, aux passagers, des informations concernant le traitement de leurs données personnelles. Dans le souci de simplifier leur tâche à cet égard et afin de s'assurer de la cohérence des informations fournies dans l'ensemble de l'Union européenne, le

Groupe 29 a établi des modèles de notes d'information.

Document de travail 1/2008 sur la protection des données à caractère personnel de l'enfant (principes généraux et cas particulier des écoles) (Groupe de travail "Mineurs et vie privée")

Comme l'adulte, l'enfant a droit au respect de sa vie privée. Cette protection inclut que les données le concernant soient traitées dans le respect des principes de la législation belge et européenne en matière de protection des données. Dans sa première partie, le document de travail contient des orientations générales sur la meilleure manière d'assurer cette protection. Les principes fondamentaux de la directive européenne 95/46/CE y sont explicités à la lumière de sa situation particulière en tant que mineur. Par exemple, le devoir d'assurer la plus grande transparence possible vis-à-vis de l'enfant lors du traitement de ses données implique que l'information à lui donner devra être claire, adaptée à son âge et à son degré de compréhension. En grandissant, il pourra être progressivement associé à ses parents pour la prise de décision relative à des traitements de données qui le concernent et pour exercer les droits que la réglementation en matière de protection des données lui accorde vis-à-vis de ses données. Dès lors que les enfants évoluent sans cesse, les données qui les concernent se révéleront rapidement dépassées, sans pertinence avec l'objectif pour lequel elles ont été initialement rassemblées ; elles ne devraient dans ce cas pas être conservées. La seconde partie du document de travail est plus particulièrement consacrée aux données des élèves, collectées, traitées, conservées à l'école. Elle ambitionne de donner aux enseignants, éducateurs et directions des écoles des orientations sur la meilleure manière de veiller au respect des données de leurs élèves. L'école est, avec la famille, un lieu capital pour les enfants et les adolescents. Ils y déploient quotidiennement leurs activités et s'y épanouissent. C'est aussi à l'école que nombre de leurs activités laissent des traces sous la forme de données les concernant : contenu des dossiers scolaires, mention d'une mesure disciplinaire,

résultats scolaires, photographies prises lors du spectacle de fin d'année postées sur le site internet de l'école, images capturées par l'éventuelle caméra surveillant l'accès au bâtiment, recours aux données biométriques à des fins d'autorisation d'accès aux bâtiments scolaires etc.

Avis 3/2008 sur le projet de norme internationale de protection de la vie privée du Code mondial antidopage

A la demande de la Commission européenne, le Groupe 29 s'est prononcé sur le projet de Standard de protection de la vie privée et des données personnelles préparé par l'Agence mondiale antidopage (AMA - <http://www.wada-ama.org>). Ce standard fixe un certain nombre de principes de base en matière de protection de la vie privée. Ces principes s'adressent aux associations sportives et aux organisations antidopage et doivent être respectés lors du traitement de données de sportifs dans le cadre de contrôles antidopage. En conclusion de son analyse de compatibilité de ce Standard avec les exigences de la directive 95/46/CE, le Groupe 29 indique que nonobstant certaines critiques essentielles, il n'en soutient pas moins l'initiative de l'AMA. Le Groupe 29 considère en effet que la portée géographique de cette norme - laquelle a pour vocation de s'appliquer dans le monde entier - peut lui permettre de jouer un rôle significatif à l'égard des traitements de données qui ne sont pas soumis à la législation de l'Union ni à une législation ayant été jugée adéquate. Dans tous les États, qu'ils aient ou non établi une protection adéquate pour le traitement des données personnelles, cette norme pourrait contribuer à sensibiliser les organisations antidopage à cette question.

Binding Corporate Rules (BCR) ou Règles d'entreprise contraignantes

- Document de travail établissant un cadre pour la structure des Règles d'entreprise contraignantes (BCR) ;
- Document de travail établissant un tableau présentant

les éléments et principes des Règles d'entreprise contraignantes (BCR) ;

- Document de travail relatif aux questions fréquemment posées (FAQ) concernant les Règles d'entreprise contraignantes (BCR).

Par le passé, le Groupe de travail avait déjà établi que les transferts internationaux de données à caractère personnel à partir de l'Union européenne effectués entre filiales d'un même groupe peuvent avoir lieu sur la base de Règles d'entreprise contraignantes (BCR). Au cours de l'année 2008, le Groupe 29 s'est penché de manière intensive sur ce mécanisme. Pour tenter de répondre aux critiques formulées à l'encontre de celui-ci (lenteur et lourdeur de la procédure, insécurité juridique consécutive à des interprétations divergentes quant au contenu obligatoire de ces règles), le Groupe s'est attaché à améliorer la procédure de coordination d'approbation de ces règles et à fournir aux entreprises des orientations destinées à les guider dans leur élaboration. Dans cette optique, une proposition quant au contenu obligatoire et quant à la façon dont les règles pourraient être structurées - accompagnée de commentaires explicatifs - a par exemple été préparée.

8.2.2 Technology Subgroup

- fait partie du Groupe 29 ;
- activités dans le domaine des TIC.

Le *Technology Subgroup* (précédemment *internet Task Force*) existe depuis plusieurs années et a pour mission de formuler des recommandations/avis du Groupe 29 sur les nouveaux projets/technologies/systèmes qui ont un impact sur la protection de la vie privée : http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm).

En 2008, ce groupe de travail s'est penché sur plusieurs projets /systèmes, notamment :

- *social networking online* : le groupe de travail a planché sur un avis sur ce thème qui sera soumis pour approbation au

Groupe 29 ;

- avis relatif à la révision prévue de la directive *e-privacy*.

Un rapport sur ces différentes études a systématiquement été présenté à la session plénière du Groupe 29.

Le *Technology Subgroup* a en outre émis les avis suivants :

Avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche

Les moteurs de recherche font désormais partie intégrante de la vie quotidienne des personnes utilisant internet et les technologies de recherche d'informations. Dans son avis, le Groupe de travail s'est penché sur la définition des moteurs de recherche, les types de données traitées dans le cadre des services de recherche, les finalités d'un traitement légitime, les responsabilités qui incombent aux fournisseurs de moteurs de recherche en qualité de responsable de traitement de données des utilisateurs - dont l'obligation d'informer les personnes concernées - et plus généralement les droits de ces dernières.

Le principal objectif poursuivi par l'avis est de parvenir à un équilibre entre les besoins légitimes des fournisseurs de moteurs de recherche dans l'exercice de leur activité et la protection des données personnelles des internautes. L'avis conclut notamment que les fournisseurs de moteurs de recherche ont l'obligation de supprimer ou de rendre les données totalement anonymes dès qu'elles ne servent plus les finalités déterminées et légitimes pour lesquelles elles ont été collectées. Ils doivent également, à tout moment, être en mesure d'en justifier le stockage. Le consentement de l'utilisateur est requis pour tout projet de recoupement entre données relatives à l'utilisateur et d'enrichissement du profil de ce dernier. Les moteurs de recherche doivent également respecter les demandes d'exclusion d'indexation formulées par les éditeurs de sites internet et répondre immédiatement aux demandes des utilisateurs concernant l'actualisation des mémoires caches. Le Groupe de travail rappelle également que les moteurs de recherche sont tenus d'informer clairement et préalablement les utilisateurs de toutes les utilisations

prévues de leurs données et de respecter leur droit de consulter et de corriger aisément ces données conformément à la Directive 95/46/CE. Cette dernière s'applique même lorsque le siège des moteurs de recherche se trouve en – dehors de l'Espace économique européen (EEE). Par contre, la Directive 2006/24/CE relative à la conservation des données ne s'applique pas aux fournisseurs de moteurs de recherche.

Avis 2/2008 sur la révision de la directive 2002/58/CE concernant la protection de la vie privée dans le secteur des communications électroniques

La Directive 2002/58/CE "Vie privée et communications électroniques" est actuellement en cours de révision. Une des modifications majeures envisagées est l'introduction d'un système de notification des violations de sécurité ("breach notification"), laquelle reçoit le plein soutien du Groupe de travail. Celui-ci souligne également l'importance d'informer toutes les personnes concernées lorsque leurs données sont compromises ou risquent de l'être. Entre autres suggestions dans le contexte de cette révision, le Groupe 29 préconise l'application du principe de minimisation des données et la prise en compte du respect de la vie privée dès la conception de la technologie ("Privacy by design").

8.3 Comité consultatif de la Convention 108

- groupe de travail Conseil de l'Europe ;
- protection des personnes dans le cadre des traitements automatisés de données.

Qu'est-ce que le Comité consultatif de la Convention 108 ?

Comme le Groupe 29 a été institué en application de la Directive européenne 95/46/CE, le Comité consultatif de la Convention n° 108 a, pour sa part, été créé en application de

la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 (communément appelée Convention 108). Ce comité est composé à la fois - au choix de chaque État - de représentants du gouvernement ou de l'autorité de protection des données des 41 États membres du Conseil de l'Europe signataires de cette convention. Il est chargé de faire des propositions en vue de faciliter ou d'améliorer l'application de la Convention ainsi que de formuler et de réagir à toute proposition d'amendement à celle-ci. A la demande d'un État partie prenante à la Convention, il peut également formuler un avis sur toute question relative à l'application de la Convention.

En 2008, le Comité consultatif s'est attelé à la rédaction d'un projet de recommandation sur la protection des données à caractère personnel dans le cadre du "profilage". Le Comité poursuivra ses travaux sur ce thème important et d'actualité en 2009. A terme, une nouvelle recommandation pourrait ainsi venir compléter celles consacrées aux traitements des données médicales, aux traitements de données à caractère personnel à des fins de marketing, de police ou encore aux traitements de données intervenant dans le cadre des relations de travail.

Les lecteurs intéressés trouveront plus d'informations sur les activités du Conseil de l'Europe en matière de protection des données à l'adresse : http://www.coe.int/T/E/Affaires_juridiques/Coop%Egration_juridique/Protection_des_donn%Eges/

8.4 IWGDPT

- Groupe de Berlin ;
- protection des données à caractère personnel dans les télécommunications.

Comme chaque année, le Secrétariat de la Commission a participé aux réunions semestrielles de l'IWGDPT (*International Working Group on Data Protection in Telecommunication*) aussi appelé "Groupe de Berlin", un groupe de travail international

sur la protection des données personnelles dans le domaine des télécommunications et des nouvelles technologies.

Ces deux réunions ont principalement permis de finaliser les working papers suivants :

- *Recommendation on the Implementation and Application of the Council of Europe Convention No. 185 on Cybercrime (a.k.a. "Budapest Convention")* (Rome, 3./4.03.2008) ;
- *Report and Guidance on Privacy in Social Network Services – "Rome Memorandum"* – (Rome, 3./4.03.2008).

Ces documents sont disponibles sur le site de l'IWGDPT :

<http://www.datenschutz-berlin.de/content/Europa+%252F+International/International+Working+Group+on+Data+Protection+in+Telecommunications+%28IWGDPT%29/Working+Papers+and+Common+Positions+adopted+by+the+Working+Group%3A>

8.5 WPPJ

- groupe de travail des autorités européennes sur la protection des données ;
- initiatives du troisième pilier.

Depuis quelques années, les initiatives relevant du troisième pilier (police et justice) demandent une attention croissante des commissaires européens à la protection des données. La Conférence européenne des autorités de protection des données a dès lors décidé de mandater un groupe de travail spécifique - le WPPJ - chargé de surveiller les développements dans le domaine de la police et de la justice pour permettre de relever défi croissant que représente la protection des individus dans le cadre du traitement de leurs données personnelles. Monsieur Bart De Schutter, membre de la Commission, est Vice-président du WPPJ.

Le 17 avril 2008, le WPPJ a adopté, conjointement avec le Groupe Article 29, une déclaration dans laquelle ils émettent de sérieuses réserves sur la nécessité et la proportionnalité des propositions européennes relatives à la gestion des frontiè-

res (création d'Eurosur, un système européen de surveillance des frontières et de Frontex, un organisme indépendant de collaboration entre les États membres de l'UE en matière de sécurité des frontières). Ils ont tout d'abord relevé l'absence d'évaluation des mesures légales existantes. Cette évaluation aurait permis de déterminer si les mesures actuelles étaient inefficaces, une condition indispensable pour justifier la nécessité de mettre en place de nouveaux systèmes. Ces nouveaux systèmes tendent vers un plan de surveillance générale qui génère des risques inacceptables en termes de liberté individuelle. Le traitement des données biométriques augmente encore ces risques. Le WPPJ et le Groupe Article 29 ont souligné avec force que tout ce qui est techniquement possible n'est pas nécessairement acceptable d'un point de vue éthique ou d'un point de vue légal. Cette déclaration a été adressée à la Commission européenne, au Parlement européen, au Conseil européen, au Comité économique et social européen et au Comité des Régions.

8.6 Organes de contrôle communs

- Schengen ;
- Europol.

8.6.1 Schengen

- échange d'informations via le SIS ;
- exécution de la Convention d'application de Schengen.

La Convention Schengen, signée en 1990 et en vigueur depuis 1995 ("Convention"), a mis en place un Système d'Information Schengen (SIS). Le SIS permet aux autorités compétentes des États membres d'échanger des informations aux fins du contrôle des personnes et des objets aux frontières extérieures ou à l'intérieur du territoire et de la délivrance de visas et de permis de séjour. La Convention Schengen crée également une Autorité de Contrôle Commune (ACC) composée de représentants des autorités nationales de contrôle, parmi lesquelles la Commission

(<http://www.schengen-isa.dataprotection.org>). Cette ACC est chargée notamment de la bonne exécution des dispositions de la Convention Schengen ainsi que de l'analyse des difficultés d'application ou d'interprétation potentielle dans le cadre de l'exploitation du SIS.

Avis sur les principes directeurs de coopération entre les autorités nationales de contrôle basés sur la Convention (juin 2008)

Compte tenu de l'échange croissant d'informations policières au sein de l'Union européenne, les données relatives à une personne peuvent être traitées dans différents États membres et/ou organisations européennes. Il est dès lors de plus en plus difficile pour la personne concernée d'exercer ses droits. Dans le cadre de l'exercice de ces droits, l'application de différentes réglementations nationales ainsi que les difficultés linguistiques constituent en outre des obstacles supplémentaires pour la personne concernée.

En vertu de la Convention Schengen, les autorités de protection des données ont l'obligation d'agir en étroite coordination. Dans son avis, l'ACC a examiné plusieurs questions pratiques telles que la langue utilisée dans les contacts avec la personne concernée, les délais de traitement des demandes ou encore la désignation des personnes de contact.

Avis sur le Système d'Information Schengen et les auteurs de troubles violents (juillet 2008)

L'ACC a pris connaissance des discussions au sein du Working Party SIS/SIRENE concernant l'insertion dans le SIS - sur la base de l'article 99 de la Convention Schengen - des données relatives aux auteurs de troubles violents aux fins de les tenir à l'écart de certains événements tels que les sommets européens, des événements internationaux culturels ou sportifs et autres rassemblements de masse.

Tant la Convention Schengen que la nouvelle base légale pour

le SIS II (décision du Conseil) limitent clairement l'utilisation des signalements sur la base de l'article 99 de la Convention à des catégories spécifiques de personnes et de crimes. Seules les personnes qui ont commis, commettent ou risquent de commettre des faits punissables extrêmement graves (Convention Schengen) ou des faits punissables graves (décision du Conseil) peuvent être signalées. Une référence claire est faite à l'article 2 de la décision cadre sur le mandat d'arrêt européen. Les seuls faits punissables mentionnés dans cette décision cadre en relation avec la violence lors d'événements pour lesquels une personne devrait être tenue à l'écart sont le meurtre et les blessures corporelles graves.

Il n'existe en outre aucune définition claire de ce qu'est un fauteur de trouble. L'ACC ne voit dès lors pas de relation réelle entre le fauteur de troubles violents et les crimes auxquels il est fait référence dans la Convention Schengen et la décision du Conseil.

En outre, en vertu de la Convention Schengen, l'objectif d'un signalement sur la base de l'article 99 est la surveillance discrète ou le contrôle spécifique. L'utilisation de l'article 99 afin de tenir à l'écart de certains événements (par le biais, par exemple, d'une arrestation ou d'une détention) des auteurs de troubles violents n'est dès lors pas compatible avec les objectifs de la Convention Schengen.

L'ACC conclut dans son avis que l'utilisation de l'article 99 de la Convention Schengen en vue d'empêcher des auteurs de troubles violents d'assister à certains événements est en infraction avec la Convention Schengen et la décision du Conseil et est, par conséquent, illégale.

Avis 102 A (7 octobre 2008)

L'Autorité de Contrôle Commune a rendu un avis à propos de l'accès par certaines autorités aux données relatives aux véhicules enregistrés dans le système d'information Schengen. Dans son avis, l'Autorité de Contrôle Commune souligne

l'absence d'enregistrement de la transmission de ces données, ce qui est contraire aux exigences de l'article 103 de la Convention Schengen.

8.6.2 Europol

- stockage, traitement et utilisation correcte des données Europol ;
- légalité de la transmission des données par Europol.

Une Autorité de Contrôle Commune (ACC) composée de représentants des autorités de contrôle nationales (dont la Commission) est chargée de surveiller l'activité d'Europol afin de s'assurer que le stockage, le traitement et l'utilisation des données dont dispose Europol ne portent pas atteinte aux droits des personnes (<http://www.europol.europa.eu/>). Elle contrôle en outre la licéité de la transmission des données provenant d'Europol.

Inspection de mars 2008

Le 17 décembre 2007, l'ACC a mandaté une équipe d'inspection avec la mission suivante :

- contrôler le contenu et la qualité des données personnelles traitées par Europol dans les fichiers de travail et dans le système d'information Europol ;
- contrôler le fonctionnement du système d'information Europol ;
- contrôler l'infrastructure technique et le suivi des recommandations des inspections précédentes.

L'inspection a également porté sur les procédures appliquées par Europol lors des demandes d'accès ainsi que sur le contenu et le fonctionnement des nouveaux projets.

Le Secrétariat de la Commission a participé à l'inspection Europol d'une semaine qui s'est déroulée en mars 2008.

On note parmi les points relevés :

- la nécessité d'une révision annuelle de la prolongation de

- la conservation des données dans les fichiers de travail ;
- la mise en œuvre des précédentes recommandations de l'ACC concernant les durées de conservation des documents sources ;
- la qualité des empreintes digitales ;
- l'obligation pour Europol d'informer l'ACC en cas d'ouverture ou de fermeture de groupes cibles au sein des fichiers de travail.

Avis sur Oasis

Le système OASIS est un nouveau projet au sein d'Europol qui implique le traitement de données personnelles. En ce qui concerne ce système, l'Autorité de Contrôle Commune a rappelé dans un avis du 8 octobre 2008 que les données ne peuvent être conservées au-delà des délais de conservation prévus au motif que l'information qui a été supprimée pourrait être très utile à un stade ultérieur.

Agreements with Third States

En ce qui concerne la conclusion d'accords entre Europol et des États tiers, l'avis de l'ACC est requis à deux étapes : avant que des négociations ne soient entamées par Europol avec le pays tiers et ensuite sur le projet d'accord avec cet État tiers. L'ACC a considéré que le projet d'accord entre Europol et l'Australie ne présentait aucun obstacle du point de vue de la protection des données. A propos d'éventuelles futures négociations entre Europol et la Russie, l'ACC a indiqué que des informations supplémentaires étaient nécessaires. Quant à de futures négociations avec Israël, l'ACC a relevé les points essentiels qui devraient être pris en considération durant les négociations.

8.7 L'affaire SWIFT

- examen des faits par la Commission ;
- arrêt de la procédure de recommandation à l'égard de SWIFT.

Le 9 décembre 2008, la Commission a décidé d'arrêter la procédure de recommandation relative à SWIFT qui avait été entamée en 2007. Cette décision a également entraîné la clôture du dossier de contrôle ouvert en 2006 sur SWIFT. La fin de cette procédure a été dictée par la constatation que SWIFT avait consenti à tous les efforts nécessaires pour mener une politique de protection de la vie privée conforme aux exigences de la législation belge en la matière.

Un examen précis des faits par la Commission, effectué avec la collaboration loyale de SWIFT, a mené à la détermination précise des responsabilités qui incombent aux différents acteurs dans le cadre des transactions financières internationales. SWIFT a réservé un accueil favorable à la décision de la Commission qui délimitait ses responsabilités et conformément à cette décision SWIFT déclare les traitements de données à caractère personnel dans le registre public.

Un examen approfondi des faits a permis de réfuter les infractions à la loi alléguées et de montrer, e.a. que SWIFT a fait preuve de prudence et que de ce fait, les informations qui se trouvaient chez SWIFT/USA et qui avaient été saisies par les autorités américaines avaient, au contraire, été effectivement protégées (contrairement aux données à caractère personnel collectées massivement dans le cadre de certains autres programmes de surveillance et utilisées systématiquement).

La Commission a aussi pu constater que SWIFT ne s'est pas seulement limitée au strict respect des obligations légales. En réaction aux soupçons et accusations, SWIFT a également pris une série de mesures pour mieux se protéger contre certains risques et augmenter la protection des données à caractère personnel qu'elle traite :

- nouvelle architecture de son réseau international, implantation d'un nouveau centre de traitement en Suisse pour la gestion des messages intra-européens (qui ne sont plus envoyés aux É-U) ;
- engagement dans la société d'un "Privacy Officer" à temps plein pour certaines missions déterminées ;
- formalisation des procédures d'encadrement, d'orientation et de suivi des demandes des personnes dont les données sont traitées ;
- création d'un groupe de travail permanent "data protection", chargé de l'évaluation et de l'adaptation des mesures de protection existantes, du développement d'une politique de l'information accessible ;
- ...

Des leçons peuvent être tirées de cette affaire qui seront utiles dans d'autres situations similaires. Les entreprises privées isolées ne sont pas armées pour lutter contre les risques liés aux injonctions et à l'utilisation problématique des données à caractère personnel conservées légitimement par certains États. Elles ne sont pas non plus en mesure d'en supporter toutes les conséquences. Dans un monde dans lequel l'information circule librement, il est plus que jamais nécessaire de mettre en place des mécanismes de régulation et de contrôle pour continuer à garantir les droits fondamentaux.

La Commission a décidé de publier les éléments et les analyses de l'enquête, et ceci plus précisément en publiant sa décision motivée détaillée intégralement sur son site web : <http://www.privacycommission.be/nl/static/pdf/cbpl-documents/swift-nl-final-og.pdf>

9 Les activités de la Commission en chiffres

La Commission vie privée :

- émet des avis sur la réglementation et la normalisation ;
- mène une politique de respect des dispositions légales ;
- fournit des informations et apporte un soutien en matière d'information ;
- assiste les personnes concernées dans l'exercice de leurs droits et obligations ;
- traite les plaintes qui lui sont soumises concernant le traitement des données et intervient en qualité de médiateur le cas échéant

pour contribuer au juste respect de la protection des droits fondamentaux de chacun en matière de protection de la vie privée dans le cadre du traitement des données à caractère personnel.

9.1 Réglementation et normalisation

Les avis et recommandations s'adressent principalement aux autorités et instances compétentes et ont pour objectif de leur proposer un cadre pour le traitement et la communication de données à caractère personnel. Ces avis et recommandations sont élaborés par la Commission ou par des comités sectoriels spécifiques institués au sein de la Commission. Les recommandations relatives aux traitements ultérieurs sont par contre destinées aux responsables des traitements.

Cette tâche d'avis repose principalement sur les demandes d'avis. En 2008, la Commission a ainsi reçu au total 49 demandes de ce type. La Commission peut toutefois également émettre des avis ou des recommandations d'initiative. En 2008, elle a ainsi émis 3 avis et 2 recommandations d'initiative. Une recommandation est aussi émise dans le cadre des déclarations de traitement ultérieur de données à caractère personnel lorsque le responsable du traitement est dans l'impossibilité de satisfaire aux exigences de la Loi vie privée. Dans ce cas, cette recommandation fixe les conditions à res-

pecter dans le cadre du traitement des données concernées. En 2008, la Commission a émis 11 recommandations concernant des traitements ultérieurs.

9.2 Politique de respect des dispositions légales

Les activités déployées dans ce domaine s'adressent non seulement aux autorités publiques compétentes mais aussi à tous les responsables de traitements de données à caractère personnel.

Quand la Commission vie privée accorde une autorisation, cela veut dire qu'elle autorise une instance active dans un secteur déterminé à traiter ou à communiquer des données à caractère personnel. Si un comité sectoriel a été institué pour le secteur concerné, cette mission est assurée par ce comité sectoriel. Le droit d'évocation permet cependant toujours aux comités sectoriels de soumettre une demande d'autorisation pour avis à la Commission.

Le Comité de surveillance statistique créé en 2007 n'a pas encore été composé ce qui explique que les demandes d'autorisations sont actuellement traitées par la Commission. Ce Comité surveille la communication de données d'étude codées à des tiers par la Direction générale Statistique et Information Économique et l'utilisation de ces données par ces tiers. En 2008, 40 demandes d'autorisation ont été reçues et 4 dossiers de 2007 étaient encore en suspens. Ces demandes ont débouché sur 36 autorisations, 2 dossiers ont été classés sans suite et 6 dossiers sont encore en cours de traitement.

La Commission est également investie de tâches de contrôle et d'inspection à l'égard des responsables des traitements qu'elle exerce en élaborant des recommandations et en évaluant les mesures de sécurité prises.

Tâches de contrôle

En 2008, la Commission vie privée a effectué des contrôles à deux niveaux. Le premier niveau est celui des traitements effectués dans le cadre d'une part des systèmes d'information Schengen, Eurodac et Douane et d'autre part des activités d'Europol. Le deuxième niveau concerne les contrôles effectués d'initiative. Ces contrôles sont toujours des contrôles individuels concernant un responsable de traitement précis. Il ne s'agit pas de contrôles à caractère sectoriel. En 2008, 13 dossiers de contrôle de ce type ont été ouverts.

9.3 Information

Dans sa mission d'information, la Commission s'adresse aussi bien aux instances publiques qu'aux responsables des traitements ou encore aux personnes concernées par ces traitements. Ses principales tâches d'information sont de tenir le registre public et d'informer le public. Cette mission d'information peut avoir un caractère aussi bien individuel (réponses orientées client) que collectif (conférence) ou public (site web et registre public).

Support du front office en matière d'information

On note une tendance à la baisse du nombre des appels téléphoniques : en 2008, on en a enregistré 1.512, soit 126 appels par mois en moyenne.

Comme en 2007, la majorité des questions posées au front desk concernaient l'obligation de déclaration (34%) avec en tête, celles relatives à la déclaration thématique d'une surveillance par caméra. Outre les questions sur les caméras, celles relatives au crédit à la consommation (10%) et celles relatives à des questions générales sur la protection de la vie privée (12%) ont également été nombreuses.

Soutien du back office en matière d'information

En 2008, la Commission vie privée a répondu à 2.096 demandes d'information. Ces questions provenaient principalement de trois grandes catégories de demandeurs : de personnes concernées par un traitement de données (60%), de sous-traitants actuels ou futurs (20%) et de services publics (20%).

Les 5 principaux thèmes concernés ont été : le traitement des images avec un intérêt massif pour la "surveillance par caméra" (14%), les questions concernant e.a. les applications marketing par les acteurs financiers et commerciaux (12%), les "autorités publiques et vie privée" (12%), l'utilisation des données à caractère personnel dans le cadre des relations professionnelles (11%) et enfin les questions sur les dossiers crédit (9%).

La Commission vie privée dispose presque toujours des connaissances nécessaires pour répondre aux questions qui lui sont posées et dans 90% des cas, le délai de traitement moyen des demandes d'information est de maximum trois mois.

Sept pour cent des questions reçues par la Commission vie privée ne la concernaient pas. Dans ce cas, la Commission s'efforce, dans la mesure du possible, d'orienter le demandeur vers l'instance ou l'organisme qui pourra l'aider. Dans 90% des cas, les informations demandées ont pu être communiquées.

Déclarations enregistrées dans le registre public

Avant qu'un responsable de traitement puisse effectuer un traitement entièrement ou partiellement automatisé, il doit le déclarer à la Commission.

En 2008, 3.681 nouveaux traitements de données ont été déclarés sur la base des formulaires de déclaration suivants :

- déclaration ordinaire (26,5%) ;
- déclaration VIA/DPR (17%) ;
- déclaration de codage de données à caractère personnel à

- des fins historiques, statistiques et scientifiques (0,3%) ;
- déclaration de traitement ultérieur de données à caractère personnel codées à des fins historiques, statistiques ou scientifiques (0,5%) ;
- déclaration de traitement ultérieur de données à caractère personnel non-codées à des fins historiques, statistiques ou scientifiques (0,4%) ;
- déclaration thématique pour l'installation et l'utilisation d'une caméra de surveillance dans un lieu ouvert (0,6%) ;
- déclaration thématique pour l'installation et l'utilisation d'une caméra de surveillance dans un lieu fermé (50%) ;
- déclaration thématique pour l'installation et l'utilisation d'une caméra de surveillance des travailleurs sur un lieu de travail surveillé (4,9%).

Les modifications et la fin des traitements de données doivent également être déclarées. En 2008, il y a eu 291 déclarations de modifications à des traitements de données existants et 161 déclarations de fin de traitement.

Les principales finalités visées par les traitements de données déclarés ont été : 1.858 fois "surveillance et contrôle" et 181 fois "surveillance et contrôle des personnes qui travaillent sur un lieu de travail surveillé", 468 fois "les banques, organismes de crédit et assurances", 444 fois "finalités générales", 150 fois "soins de santé" et 134 fois "commerce".

Publication d'informations sur le site web

En 2008, le site web de la Commission vie privée a été consulté 183.120 fois. Au total, 3.178.393 de pages ont été consultées et le nombre moyen de pages consultées par visite a été de 17,35 pages. La rubrique "En pratique" est très prisée et les thèmes les plus consultés ont été : les caméras de surveillance (18.847 consultations), les principes de base de la vie privée (12.626 consultations) et les déclarations (12.411 consultations). Les pages consacrées à la législation et aux décisions de la Commission et de ses comités sectoriels sont également très fréquemment consultées.

Les questions les plus consultées sont :

- puis-je installer une caméra de surveillance comme bon me semble ? : 544 consultations ;
- existe-t-il, pour la déclaration de caméras de surveillance, un formulaire papier et un formulaire électronique ? : 358 consultations ;
- ma caméra de surveillance filme également un lieu de travail. Puis-je filmer cet endroit sans problème ? : 341 consultations.

Dans le lexique, les définitions les plus consultées sont celles des mots suivants :

- responsable du traitement (922) ;
- caméra (loi) (547) ;
- traitement de données à caractère personnel (487).

9.4 Assistance

La Commission vie privée aide aussi bien les instances publiques que les responsables de traitement en répondant aux demandes de concertation informelle préalable qui permettent de tenir compte des exigences en matière de protection de la vie privée dès la phase de conception des projets. La Commission vie privée aide également les personnes sur lesquelles des données sont rassemblées à exercer leurs droits.

En 2008, la Commission a traité 363 dossiers d'aide. Toute médiation est systématiquement précédée d'une analyse de recevabilité qui mène à une déclaration d'irrecevabilité pour 13% des demandes. Les principales causes d'irrecevabilité sont : la non-communication d'informations (74%) et une procédure judiciaire en cours (18%).

Dans 44% des cas, les demandes de médiation concernent des contrats de crédit et l'enregistrement qui y est lié à la Centrale des crédits aux particuliers. En 2008, la Commission a procédé à de nombreuses vérifications auprès de la Banque Nationale et a établi de nombreux contacts avec les prêteurs. Dans les dossiers clôturés, cette vérification et la

prise de contact ont mené aux résultats suivants: dans 54% des cas, les données ont été supprimées, dans 7% des cas, une correction a été effectuée et dans 31% des cas il s'est avéré que l'enregistrement était justifié et correct. Dans 8% des cas, malgré une demande, cette vérification n'a pas pu être effectuée en raison de données insuffisantes.

En plus de recevoir des demandes de médiation dans le cadre de litiges liés à des contrats de crédit, la Commission vie privée est également régulièrement saisie par les secteurs suivants : le secteur financier et commercial (12%) et le secteur télécom (9%). Dans 61% des dossiers, le rôle de médiateur de la Commission a débouché sur une solution, dans 27% des cas, la demande de médiation s'est avérée non fondée.

En 2008, le délai moyen de traitement des demandes d'assistance a été d'environ 4,5 mois.

9.5 Traitement des plaintes

Ce dernier domaine d'activités concerne plus particulièrement les personnes sur lesquelles sont rassemblées des données. Ces activités comprennent le traitement des plaintes et la médiation qui y est liée le cas échéant. Lorsque les droits des personnes sur lesquelles sont rassemblées des données ne sont pas respectés par le responsable du traitement, la Commission intervient à la demande de l'intéressé afin de lui garantir le respect de ses droits.

Dossiers relatifs à l'accès indirect (dossiers 13)

Dans les dossiers relatifs à l'accès indirect, la Commission exerce le droit spécifique de consultation et de rectification des données à caractère personnel pour des tiers dont les données sont reprises dans une base de données des services de police. En 2008, la Commission a été saisie 159 fois. Ce chiffre représente une forte augmentation par rapport à 2007.

Le délai de traitement de ces dossiers reste épineux et il faut encore souvent six mois entre le moment de la réception de la demande de vérification et l'envoi de la confirmation que la vérification a été effectuée.

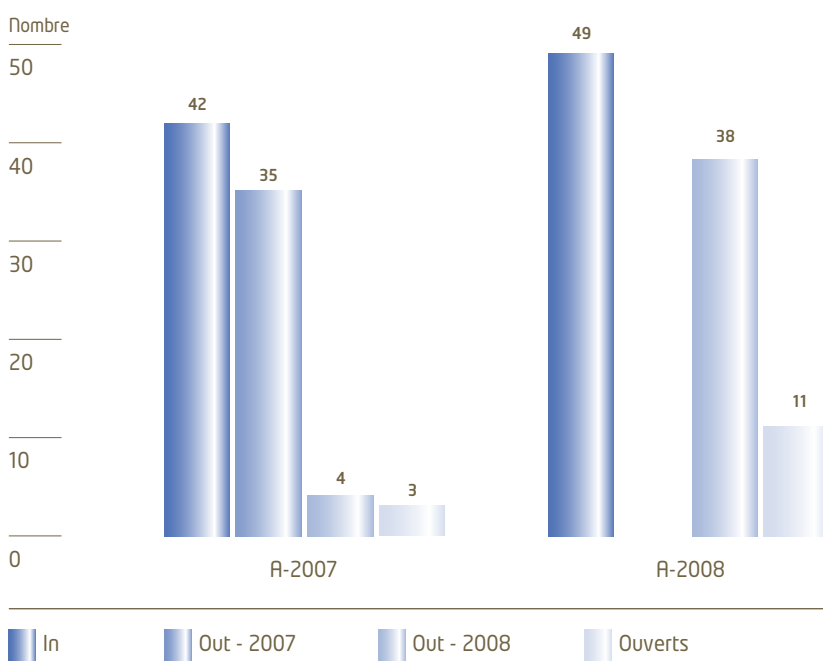
En 2008, 58 vérifications seulement ont pu être clôturées. Dans 57% des cas cette vérification a entraîné la suppression totale des données du fichier et dans 17% des cas, leur suppression partielle. Dans 17% des cas, l'enregistrement était pertinent et les données ont été conservées et 9% des demandes concernaient des demandeurs qui n'avaient pas été enregistrés.

9.6 Tableaux et graphiques

9.6.1 Autorisations et avis

9.6.1.1 Évolution des dossiers A : 2007-2008

Dossiers A		Nombre	%
A-2007	in	42	
	out - 2007	35	83,33
	out - 2008	4	9,52
	ouverts	3	7,14
A-2008	in	49	
	out	38	77,55
	ouverts	11	22,45



9.6.1.2 Nature des dossiers d'avis (2008)

	Nombre	%
Demande d'avis	43	87,76
Avis d'initiative	6	12,24

9.6.1.3 Nombre de dossiers clôturés : comparaison 2007 - 2008

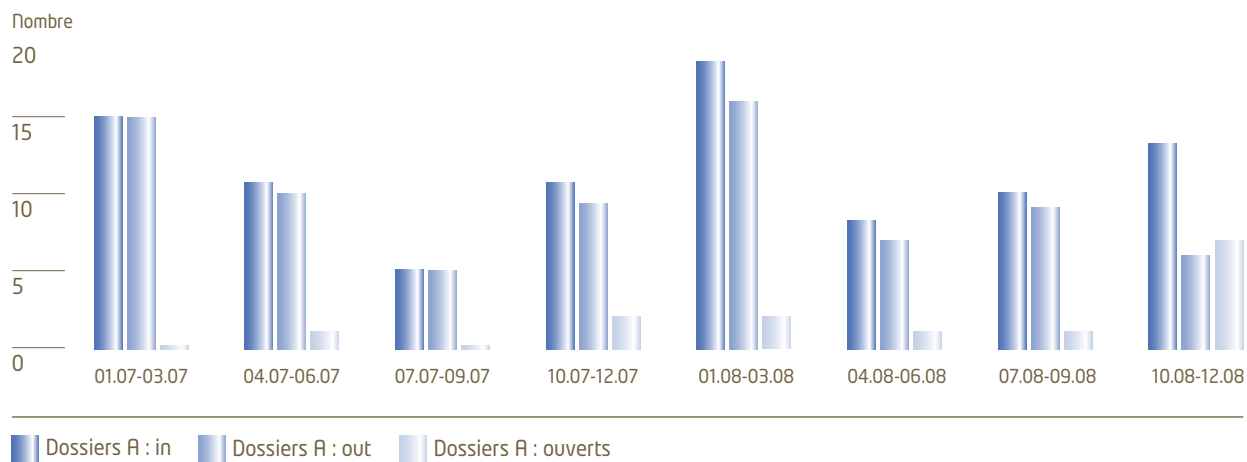
	Type	Nombre	%
Activités 2007	A-2006	6	14,29
	A-2007	36	85,71
		42	
Activités 2008	A-2007	4	9,52
	A-2008	38	90,48
		42	

9.6.1.4 Dossiers A : évolution trimestrielle

Dossiers A	Trimestre	Dossiers A in	Dossiers A out	% clôturés	Dossiers A ouverts
Activités 2007	01.07 - 03.07	15	15	100,00	0
	04.07 - 06.07	11	10	90,91	1
	07.07 - 09.07	5	5	100,00	0
	10.07 - 12.07	11	9	81,82	2
		42	39	92,86	3
Activités 2008	01.08 - 03.08	18	16	88,89	2
	04.08 - 06.08	8	7	87,50	1
	07.08 - 09.08	10	9	90,00	1
	10.08 - 12.08	13	6	46,15	7
		49	38	77,55	11

9.6.1.5 Comité de surveillance statistique : évolution des dossiers d'autorisation (dossiers STAT-MA) : 2007-2008

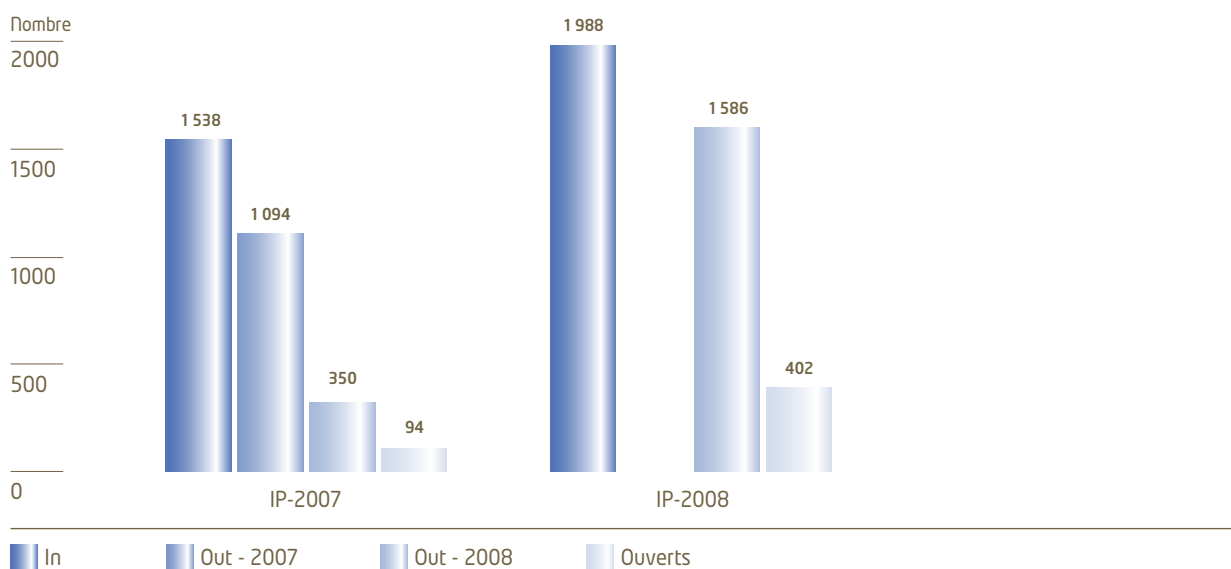
Dossiers STAT-MA		Nombre	%
STAT-MA-2007	in	5	
	out - 2007	1	20,00
	out - 2008	4	80,00
	ouverts	0	0,00
STAT-MA-2008	in	40	
	out	34	85,00
	ouverts	6	15,00



9.6.2 Plaintes et information : les dossiers IP en chiffres

9.6.2.1 Évolution des dossiers IP : 2007-2008

Dossiers IP		Nombre	%
IP-2007	in	1.538	
	out - 2007	1.094	71,13
	out - 2008	350	22,76
	ouverts	94	6,11
IP-2008	in	1.988	
	out	1.586	79,78
	ouverts	402	20,22

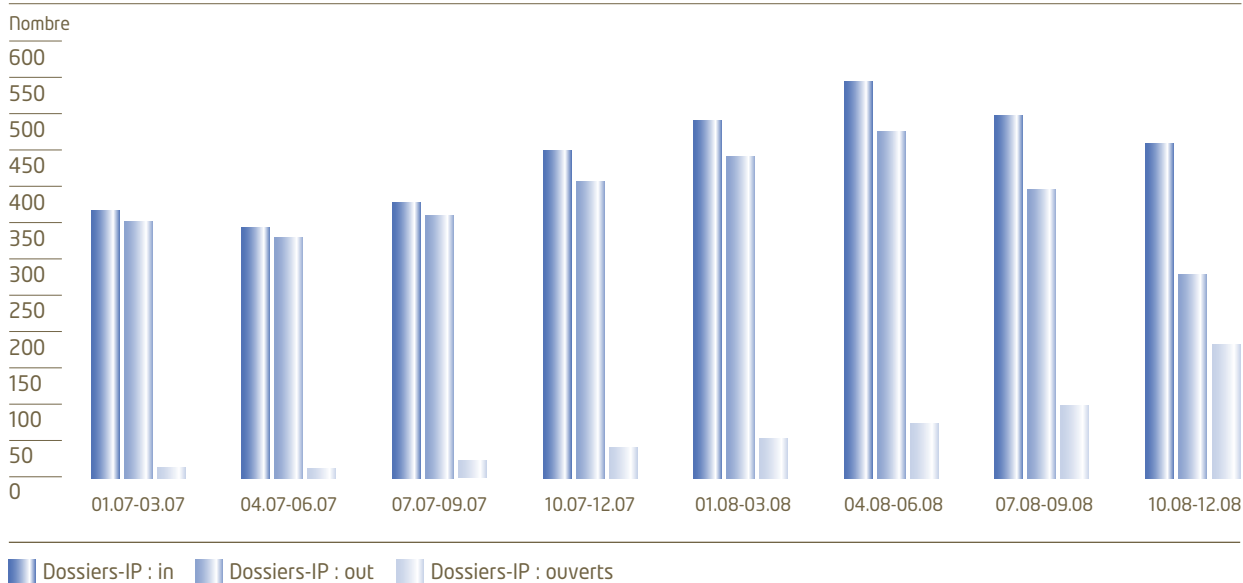


9.6.2.2 Nombre de dossiers clôturés : comparaison 2007 - 2008

	Type	Nombre	%
Activités 2007	IP-2006	256	18,96
	IP-2007	1.094	81,04
		1.350	
Activités 2008	IP-2007	350	18,08
	IP-2008	1.586	81,92
		1.936	

9.6.2.3 Dossiers IP : évolution trimestrielle

Dossiers IP	Trimestre	Dossiers IP in	Dossiers IP out	% clôturés	Dossiers IP ouverts
IP-2007	01.07 - 03.07	365	349	95,62	16
	04.07 - 06.07	347	332	95,68	15
	07.07 - 09.07	377	356	94,43	21
	10.07 - 12.07	449	407	90,65	42
		1.538	1.444	93,89	94
IP-2008	01.08 - 03.08	489	438	89,57	51
	04.08 - 06.08	546	473	86,63	73
	07.08 - 09.08	497	397	79,88	100
	10.08 - 12.08	456	278	60,96	178
		1.988	1.586	79,78	402



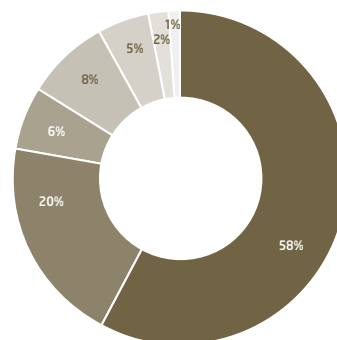
Suite donnée aux dossiers clôturés (IP-2007 et IP-2008)

	Nombre	%
Réponse à une demande d'informations	1.553	80,22
Médiation réussie	136	7,02
Commission incompétente (Loi vie privée pas applicable)	138	7,13
- notification de non-compétence	87	4,49
- renvoi à l'institution/l'autorité compétente	51	2,63
Plainte non fondée (pas d'inraction à la Loi vie privée)	13	0,67
Plainte irrecevable	34	1,76
- le plaignant n'a pas fourni les informations requises	1	0,05
- le plaignant n'a pas exercé ses droits	3	0,15
- le plaignant n'a pas fourni les informations requises	22	1,14
- procédure juridique	8	0,41
Autre	62	3,20

9.6.2.5 Analyse des dossiers IP clôturés en 2008 (IP-2007 et IP-2008)

	Nombre	Pourcentage
Langue		
néerlandais	1.164	60,12
français	707	36,52
anglais	65	3,36
Type de dossier		
médiation	202	10,43
information	1.734	89,57
Activité		
interne	1.758	90,81
externe	178	9,19
Nombre moyen de pièces entrantes et sortantes par dossier		
	4	
Délai d'accusé de réception		
≤ 3 jours	1.209	62,64
> 3 jours	721	37,36
Délai moyen de traitement		
jours calendrier	57	
jours de travail	34	
Rapport entre le nombre de pièces et le délai de traitement		
jours calendrier	14	
jours de travail		
Délai de traitement		
≤ 3 mois	1.624	83,88
≤ 30 jours	1.125	58,11
31 - 60 jours	380	19,63
61 - 90 jours	119	6,15
> 3 mois	312	16,12
91 - 180 jours	154	7,95
181 - 270 jours	93	4,80
271 - 365 jours	37	1,91
> 1 an	28	1,45
Secteur du demandeur		
avocat	27	1,39
société	312	16,12
administration	392	20,25
personne physique	1.205	62,24

Délai de traitement des dossiers IP

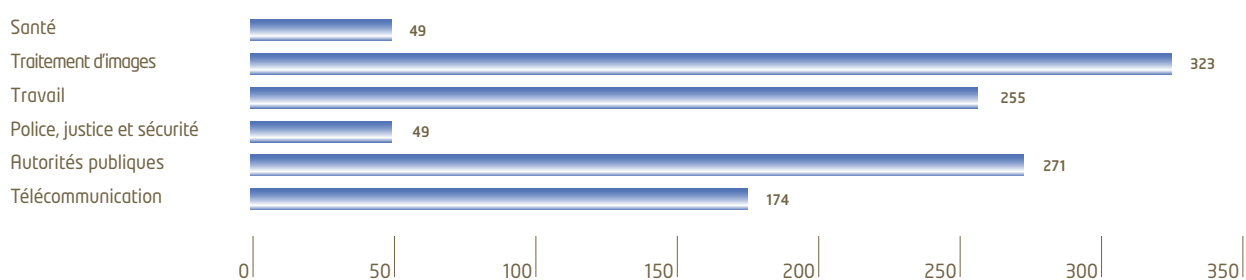


9.6.2.6 Thèmes des dossiers traités (IP-2007 et IP-2008)

	Nombre	%
Télécommunication	174	8,99
divers	35	
internet	117	
nouvelles technologies	21	
droit d'auteur	1	
Autorités publiques	271	14,00
divers	45	
Registre national	75	
registre public	1	
registre de la population	27	
contrôle du stationnement et de la circulation	81	
communes	42	
Police, justice et sécurité	49	2,53
divers	7	
tribunaux, parquet, police	13	
casier judiciaire/bonne vie et mœurs	3	
renseignements	21	
Schengen, Europol, Eurodac, Eurojust	2	
criminalité informatique	1	
ADN/biométrie	2	
Travail	255	13,17
divers	23	
syndicats	3	
données relatives aux travailleurs	119	
"whistleblowers"	6	
badges	13	
courriel	33	
télécommunication	35	
vidéosurveillance	23	
Sécurité sociale	8	0,41
Crédit	7	0,36
Listes négatives	30	1,55

	Nombre	%
Traitement d'images	323	16,68
E-gouvernement	36	1,86
divers	2	
carte d'identité électronique	27	
moyens d'identification (biométrie)	7	
Santé	49	2,53
divers	36	
dossier médical informatisé	11	
assurances	2	
Finances / consommateurs	299	15,44
divers	20	
banques / assurances	35	
marketing	182	
pourriels/hameçonnage (phishing)	42	
listes d'adresses	16	
cartes de fidélité	4	
Presse et médias	18	0,93
Flux transfrontières de données	36	1,86
Pouvoirs d'investigation du fisc	7	0,36
Copropriété / syndic	24	1,24
Élections	17	0,88
Vie privée en général	154	7,95
Autre	179	9,25
divers	39	
recherche scientifique	21	
généalogie	13	
biométrie	28	
droit d'opposition	25	
utilisation du numéro de Registre national	31	
enseignement	20	
statistiques	2	

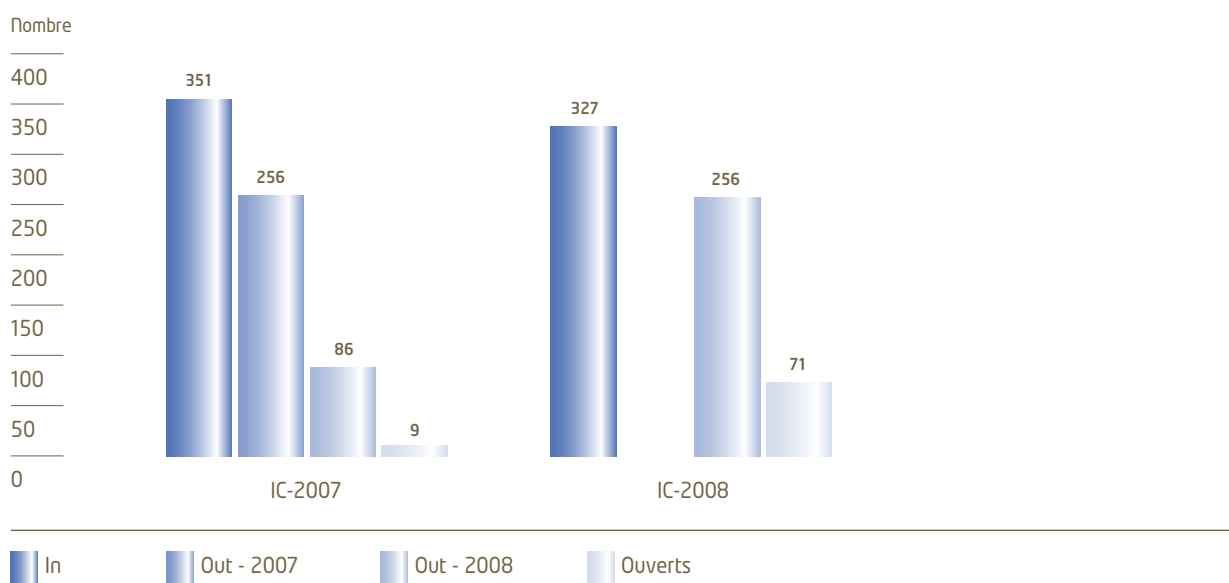
Thèmes les plus fréquemment abordés



9.6.3 Crédit à la consommation : les dossiers IC en chiffres

9.6.3.1 Évolution des dossiers IC : 2007-2008

Dossiers IC		Nombre	%
IC-2007	in	351	
	out - 2007	256	72,93
	out - 2008	86	24,50
	open	9	2,56
IC-2008	in	327	
	out	256	78,29
	open	71	21,71

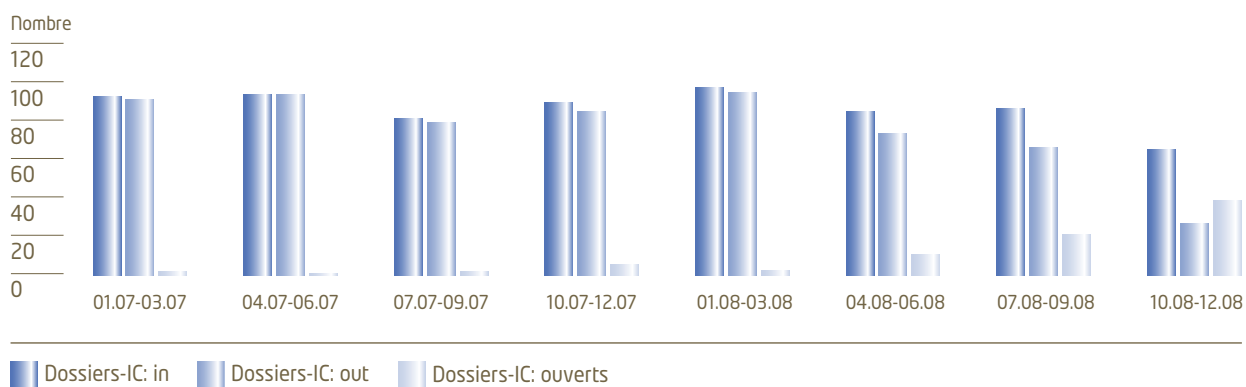


9.6.3.2 Nombre de dossiers clôturés : comparaison 2007 - 2008

	Type	Nombre	%
Activités 2007	IC-2006	61	19,24
	IC-2007	256	80,76
		317	
Activités 2008	IC-2007	86	25,15
	IC-2008	256	74,85
		342	

9.6.3.3 Dossiers IC : évolution trimestrielle

Dossiers IC	Trimestre	Dossiers IC in	Dossiers IC out	% clôturés	Dossiers IC ouverts
Activités 2007	01.07 - 03.07	91	89	97,80	2
	04.07 - 06.07	92	92	100,00	0
	07.07 - 09.07	80	78	97,50	2
	10.07 - 12.07	88	83	94,32	5
		351	342	97,44	9
Activités 2008	01.08 - 03.08	97	95	97,94	2
	04.08 - 06.08	83	73	87,95	10
	07.08 - 09.08	84	64	76,19	20
	10.08 - 12.08	63	24	38,10	39
		327	256	78,29	71



9.6.3.4 Suite donnée aux dossiers clôturés en 2008 (IC-2007 et IC-2008)

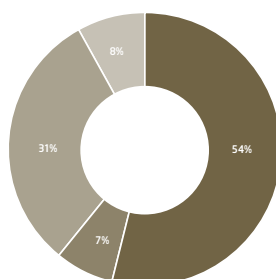
	Nombre	%
Réponse à une demande d'informations	176	51,46
Suppression de l'enregistrement	83	24,27
Rectification de l'enregistrement	11	3,22
Plainte non fondée (maintien de l'enregistrement)	48	14,04
Commission incompétente (Loi vie privée pas applicable)	12	3,51
- notification de non-compétence	9	2,63
- renvoi à l'institution / l'autorité compétente	3	0,88
Plainte irrecevable		
- le plaignant n'a pas fourni les informations requises	12	3,51

9.6.3.5 Analyse des dossiers IC clôturés en 2008 (IC-2007 et IC-2008)

	Nombre	Pourcentage
Langue		
néerlandais	141	41,23
français	200	58,48
anglais	1	0,29
Type de dossier		
médiation	154	45,03
information	188	54,97
Activité		
interne	200	58,48
externe (partie adverse)	142	41,52
Nombre moyen de pièces entrantes et sortantes par dossier		
	4,81	
Délai d'accusé de réception		
≤ 3 jours	192	56,14
> 3 jours	150	43,86
Délai de traitement moyen		
jours calendrier	63,03	
jours de travail	37,99	
Rapport nombre de pièces / délai de traitement		
jours calendrier	13,10	
jours de travail	7,90	
Délai de traitement		
≤ 3 mois	272	83,95
≤ 30 jours	164	50,62
31 - 60 jours	66	20,37
61 - 90 jours	42	12,96
> 3 mois	70	21,60
91 - 180 jours	44	13,58
181 - 270 jours	12	3,70
271 - 365 jours	7	2,16
> 1 an	7	2,16

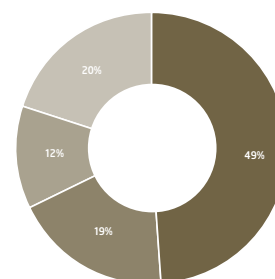
Dossiers IC - analyse des dossiers de médiation

- Suppression de l'enregistrement
- Rectification de l'enregistrement
- Plainte non fondée (maintien de l'enregistrement)
- Plainte irrecevable



Dossiers IC - délai de traitement

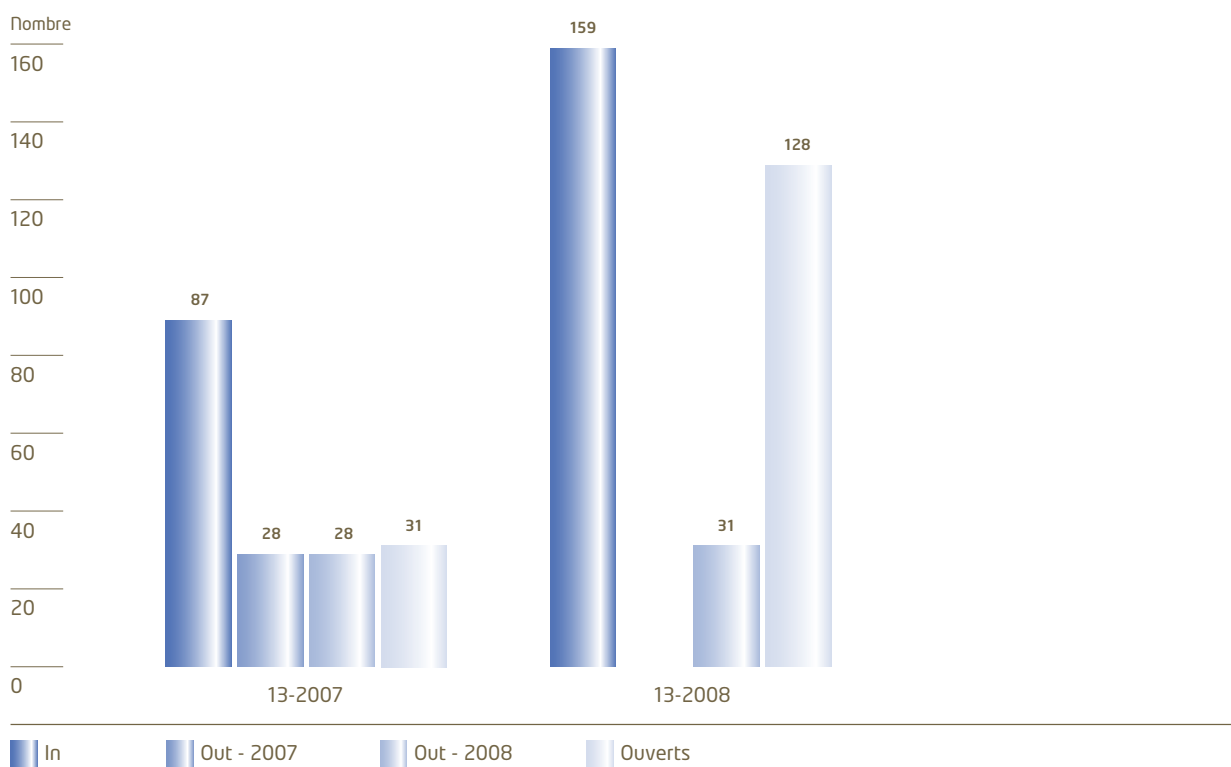
- ≤ 30 jours
- 31-60 jours
- 61-90 jours
- > 3 mois



9.6.4 Accès indirect : les dossiers 13 en chiffres

9.6.4.1 Évolution des dossiers 13 : 2007-2008

Dossiers 13		Nombre	%
13-2007	in	87	
	out - 2007	28	32,18
	out - 2008	28	32,18
	ouverts	31	35,63
13-2008	in	159	
	out	31	19,50
	ouverts	128	80,50

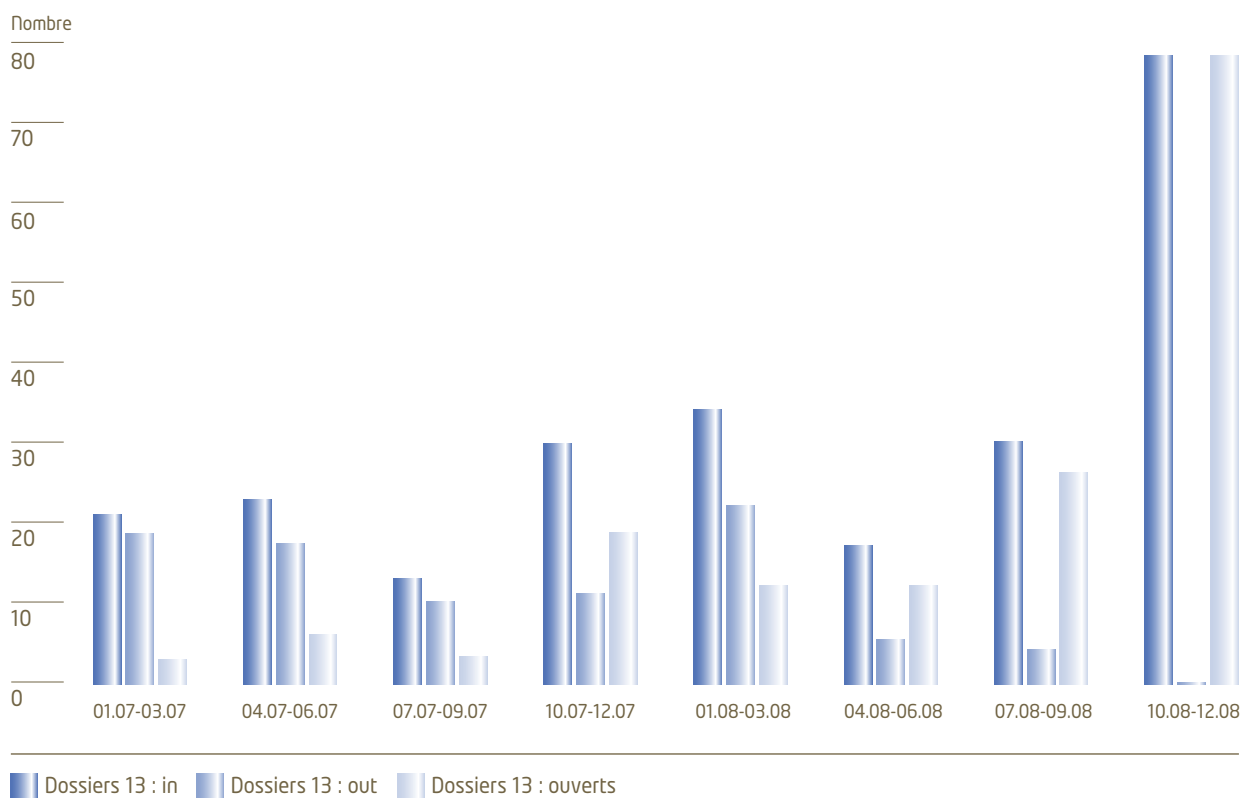


9.6.4.2 Nombre de dossiers clôturés : comparaison 2007 - 2008

	Type	Nombre	%
Activités 2007	13-2006	57	67,06
	13-2007	28	32,94
		85	
Activités 2008	13-2007	28	47,46
	13-2008	31	52,54
		59	

9.6.4.3 Dossiers 13 : évolution trimestrielle

Dossiers 13	Trimestre	Dossiers 13 in	Dossiers 13 out	% clôturés	Dossiers 13 ouverts
Activités 2007	01.07 - 03.07	21	18	85,71	3
	04.07 - 06.07	23	17	73,91	6
	07.07 - 09.07	13	10	76,92	3
	10.07 - 12.07	30	11	36,67	19
		87	56	64,37	31
Activités 2008	01.08 - 03.08	34	22	64,71	12
	04.08 - 06.08	17	5	29,41	12
	07.08 - 09.08	30	4	13,33	26
	10.08 - 12.08	78	0	0,00	78
		159	31	19,50	128



9.6.4.4 Suite donnée aux dossiers clôturés en 2008 (13-2007 et 13-2008)

	Nombre	%
Vérification effectuée	58	98,31
Commission incompétente	1	1,69

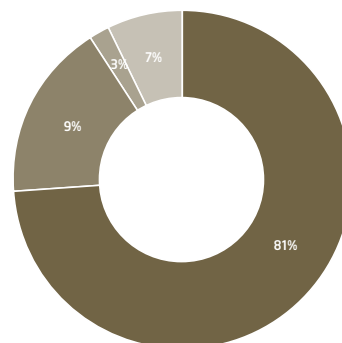
9.6.4.5 Analyse des dossiers 13 clôturés en 2008 (13-2007 et 13-2008)

	Nombre	Pourcentage
Langue		
néerlandais	20	33,90
français	38	64,41
anglais	1	1,69
Suite donnée		
Suppression complète	33	56,90
Suppression partielle	10	17,24
Conservation des données	10	17,24
Pas enregistré	5	8,62
Nombre moyen de pièces entrantes et sortantes par dossier	7,34	
Délai d'accusé de réception		
≤ 3 jours	18	30,51
> 3 jours	41	69,49
Demande de vérification	67	77,91
Délai moyen d'introduction de la demande (jours calendrier)		
≤ 3 mois	54	93,10
≤ 30 jours	43	74,14
31 - 60 jours	10	17,24
61 - 90 jours	1	1,72
> 3 mois	2	3,45
91 - 180 jours		0,00
181 - 270 jours	1	1,72
271 - 365 jours	1	1,72
Réception du résultat de la vérification		
délai moyen de réponse (jours calendrier)	132,48	
≤ 3 mois	25	43,10
≤ 30 jours	9	15,52
31 - 60 jours	6	10,34
61 - 90 jours	10	17,24
> 3 mois	33	56,90
91 - 180 jours	16	27,59
181 - 270 jours	11	18,97
271 - 365 jours	3	5,17
> 1 an	3	5,17
Délai moyen de traitement		
jours calendrier	185,93	
jours de travail	112,07	

	Nombre	Pourcentage
Rapport nombre de pièces / délai de traitement		
jours calendrier	25,33	
jours de travail	15,27	
Délai de traitement		
≤ 3 mois	17	28,81
≤ 30 jours	4	6,78
31 - 60 jours	6	10,17
61 - 90 jours	7	11,86
> 3 mois	42	71,19
91 - 180 jours	17	28,81
181 - 270 jours	12	20,34
271 - 365 jours	6	10,17
> 1 an	7	11,86

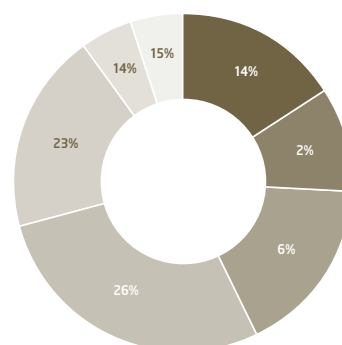
Demande de vérification - délai d'introduction

- ≤ 30 jours
- 31-60 jours
- 61-90 jours
- > 3 mois



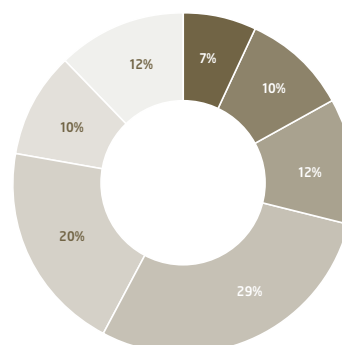
Réception du résultat de la vérification

- ≤ 30 jours
- 31-60 jours
- 61-90 jours
- 91-180 jours
- 181-270 jours
- 271-365 jours
- > 1 an



Dossiers 13 - délai de traitement

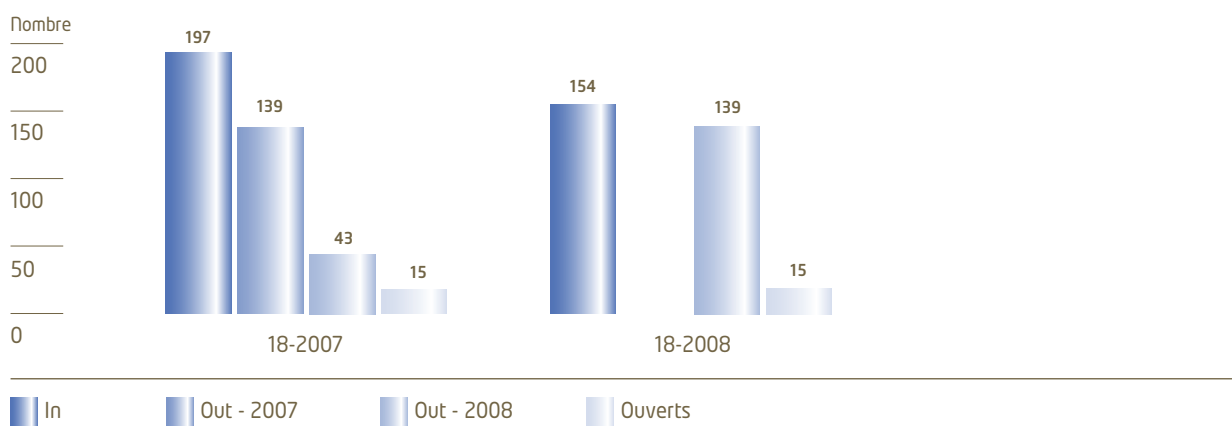
- ≤ 30 jours
- 31-60 jours
- 61-90 jours
- 91-180 jours
- 181-270 jours
- 271-365 jours
- > 1 an



9.6.5 Déclarations et registre public : les dossiers 18 en chiffres

9.6.5.1 Évolution des dossiers 18 : 2007-2008

Dossiers 18		Nombre	%
18-2007	in	197	
	out - 2007	139	70,56
	out - 2008	43	21,83
	ouverts	15	7,61
18-2008	in	154	
	out	139	90,26
	ouverts	15	9,74

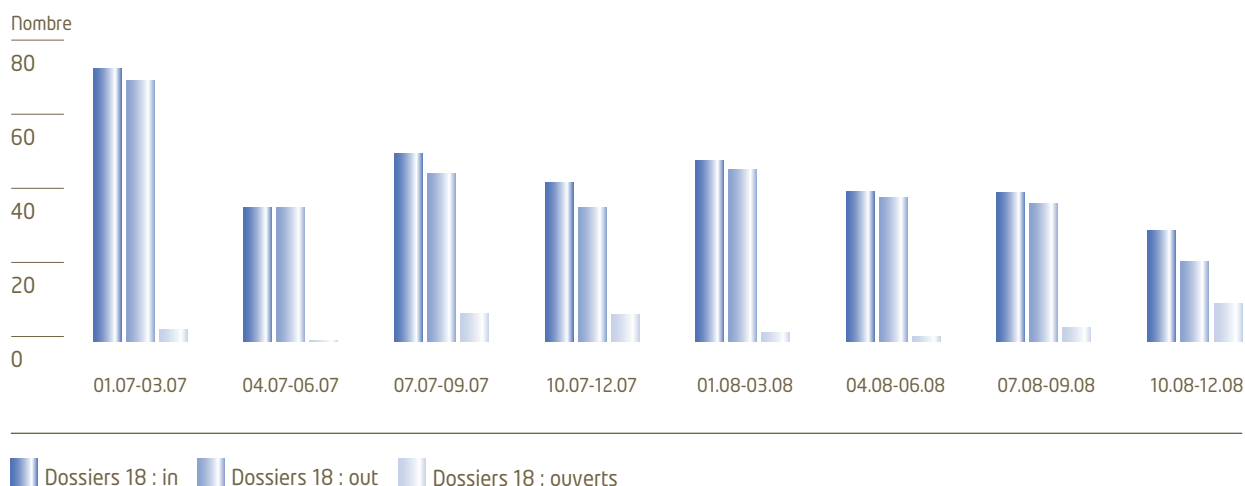


9.6.5.2 Nombre de dossiers clôturés: comparaison 2007 - 2008

	Type	Nombre	%
Activités 2007	18-2006	59	29,80
	18-2007	139	70,20
		198	
Activités 2008	18-2007	43	23,63
	18-2008	139	76,37
		182	

9.6.5.3 Dossiers 18 : évolution trimestrielle

Dossiers 18	Trimestre	Dossiers 18 in	Dossiers 18 out	% clôturés	Dossiers 18 ouverts
Activités 2007	01.07 - 03.07	72	69	95,83	3
	04.07 - 06.07	35	35	100,00	0
	07.07 - 09.07	49	43	87,76	6
	10.07 - 12.07	41	35	85,37	6
		197	182	92,39	15
Activités 2008	01.08 - 03.08	47	45	95,74	2
	04.08 - 06.08	39	38	97,44	1
	07.08 - 09.08	39	36	92,31	3
	10.08 - 12.08	29	20	68,97	9
		154	139	90,26	15



9.6.5.4 Suite donnée aux dossiers clôturés en 2008 (18-2007 et 18-2008)

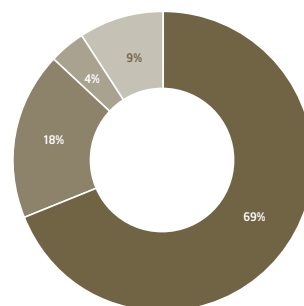
	Nombre	%
Dispense d'informations	159	87,36
Délivrance d'un extrait du registre public	1	0,55
Envoi d'un formulaire de déclaration vierge	2	1,10
Réception d'un formulaire de déclaration	20	10,99
- enregistrement de la déclaration	12	6,59
- impossibilité d'enregistrer la déclaration	7	3,85
- exemption de déclaration	1	0,55

9.6.5.5 Analyse des dossiers r8 clôturés en 2008 (r8-2007 et r8-2008)

	Nombre	Pourcentage
Langue		
néerlandais	65	35,71
français	115	63,19
anglais	2	1,10
Type de dossier		
registre public	7	3,85
obligation de déclaration	175	96,15
Nombre moyen de pièces entrantes et sortantes par dossier		
	3,09	
Délai d'accusé de réception		
≤ 3 jours	80	43,96
> 3 jours	102	56,04
Délai moyen de traitement		
jours calendrier	36,34	
jours de travail	21,90	
Rapport nombre de pièces - délai de traitement		
jours calendrier	11,76	
jours de travail	7,09	
Délai de traitement		
≤ 3 mois	134	73,63
≤ 30 jours	126	69,23
31 - 60 jours		0,00
61 - 90 jours	8	4,40
> 3 mois	16	8,79
91 - 180 jours	13	7,14
181 - 270 jours	1	0,55
271 - 365 jours	0	0,00
> 1 an	2	1,10
Secteur du demandeur		
avocat	1	0,55
société	103	56,59
administration	51	28,02
personne physique	27	14,84

Dossiers r8 - délai de traitement

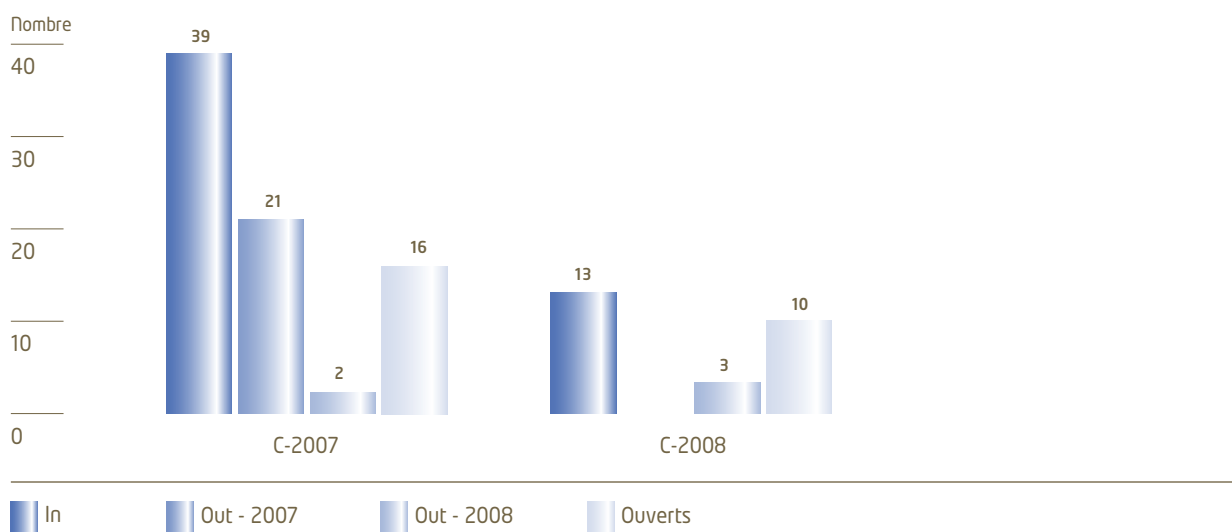
- ≤ 30 jours
- 31-60 jours
- 61-90 jours
- > 3 mois



9.6.6 Contrôle : les dossiers C en chiffres

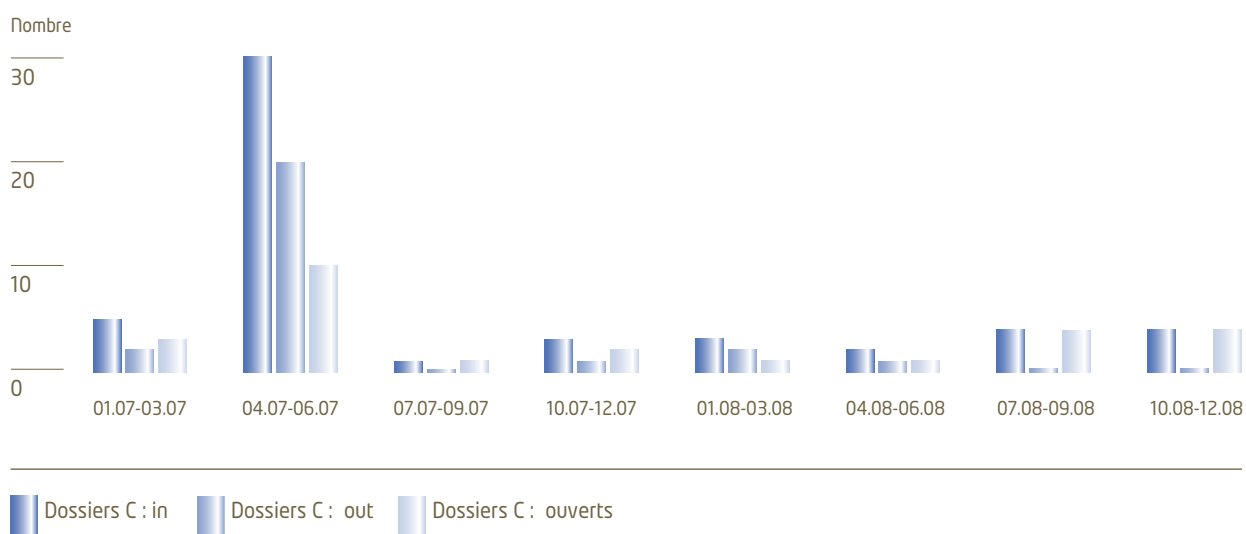
9.6.6.1 Évolution des dossiers C : 2007-2008

Dossiers C		Nombre	%
C-2007	in	39	
	out - 2007	21	53,85
	out - 2008	2	5,13
	ouverts	16	41,03
C-2008	in	13	
	out	3	23,08
	ouverts	10	76,92



9.6.6.2 Dossiers C : évolution trimestrielle

Dossiers C	Trimestre	Dossiers C in	Dossiers C out	% clôturés	Dossiers C ouverts
Activités 2007	01.07 - 03.07	5	2	40,00	3
	04.07 - 06.07	30	20	66,67	10
	07.07 - 09.07	1	0	0,00	1
	10.07 - 12.07	3	1	33,33	2
		39	23	58,97	16
Activités 2008	01.08 - 03.08	3	2	66,67	1
	04.08 - 06.08	2	1	50,00	1
	07.08 - 09.08	4	0	0,00	4
	10.08 - 12.08	4	0	0,00	4
		13	3	23,08	10

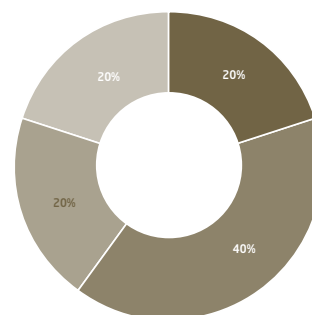


9.6.6.3 Nombre de dossiers clôturés : comparaison 2007 - 2008

	Nombre	Pourcentage
Nombre moyen de pièces entrantes et sortantes par dossier	21,4	
Délai moyen de traitement		
jours calendrier	252,20	
jours de travail	152,01	
Délai de traitement (temps écoulé entre le début et la fin du contrôle)		
≤ 3 mois	3	60,00
≤ 30 jours	1	20,00
61 - 90 jours	2	40,00
> 3 mois	2	0,00
271 - 365 jours	1	20,00
> 365 jours	1	20,00

Temps écoulé entre le début et la fin du contrôle

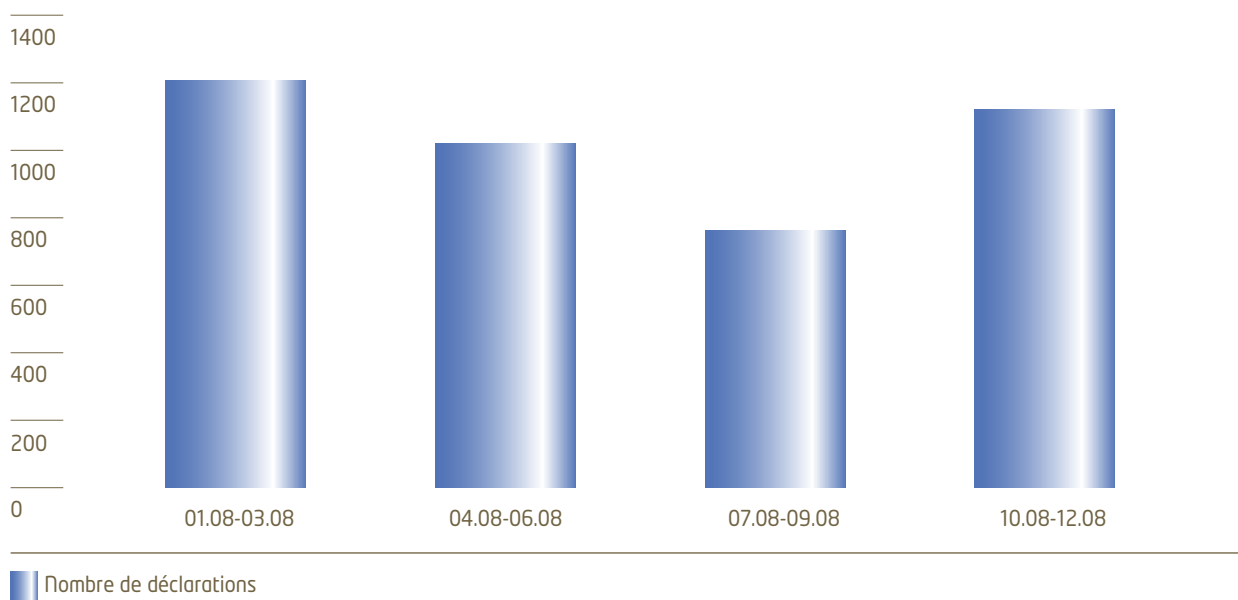
- ≤ 30 jours
- 61-90 jours
- 271-365 jours
- > 365 jours



9.6.7 Les déclarations en chiffres

9.6.7.1 Analyse globale des déclarations et des traitements

Trimestre	Nombre de déclarations	Nouveaux traitements	Modification du traitement	Correction du traitement	Fin du traitement
01.08 - 03.08	1.201	1.082	62	23	34
04.08 - 06.08	1.037	928	41	10	58
07.08 - 09.08	758	644	63	18	33
10.08 - 12.08	1.137	1.027	63	11	36
	4.133	3.681	229	62	161

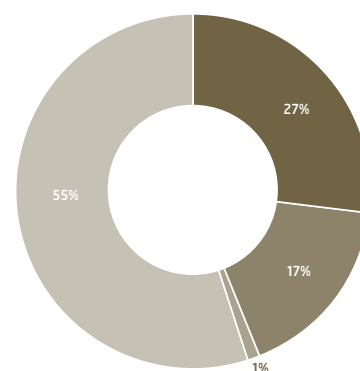


9.6.7.2 Déclarations de nouveaux traitements de données

Trimestre	Nouveaux traitements	Déclaration ordinaire	Déclaration VIA/DPR	Déclaration de traitement ultérieur	Déclaration thématique
01.08 - 03.08	1.082	309	378	12	383
04.08 - 06.08	928	200	103	8	617
07.08 - 09.08	644	210	70	11	353
10.08 - 12.08	1.027	257	73	12	685
	3.681	976	624	43	2.038

Nouveaux traitements des données par type de déclaration

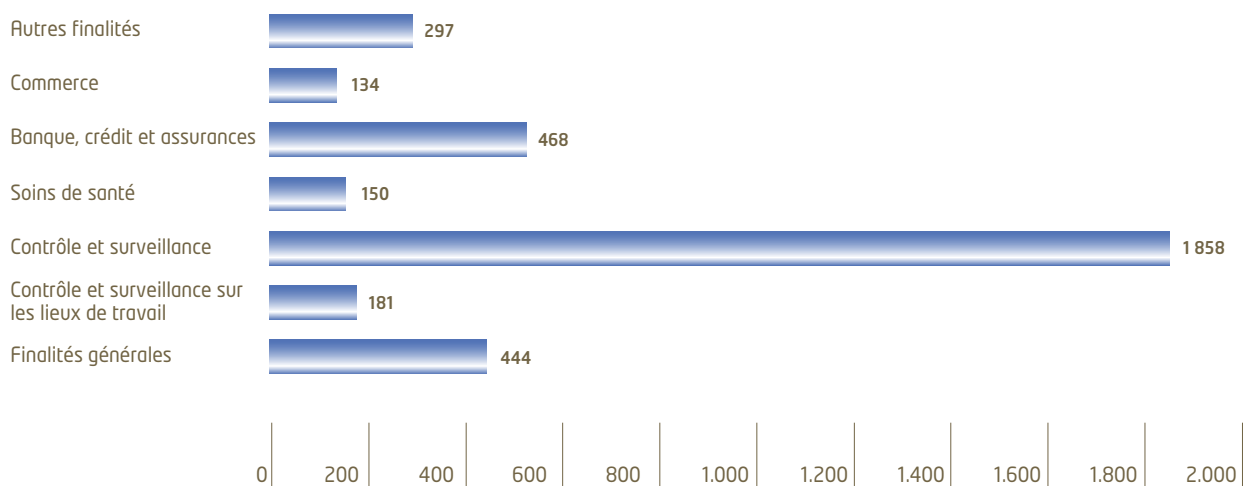
- Déclaration ordinaire
- Déclaration VIA/DPR
- Déclaration traitement ultérieur
- Déclaration thématique



9.6.7.3 Traitements par finalité

Finalité	Nombre de déclarations
Finalités générales	444
Finalités des autorités publiques	26
Contrôle et surveillance sur les lieux de travail	181
Justice et police	19
Contrôle et surveillance	1.858
Enseignement	10
Culture et bien-être	7
Sécurité sociale	1
Soins de santé	150
Recherche scientifique - primaire ou secondaire	90
Banque, crédit et assurances	468
Commerce	134
Traitement ultérieur	44
Autres finalités	297

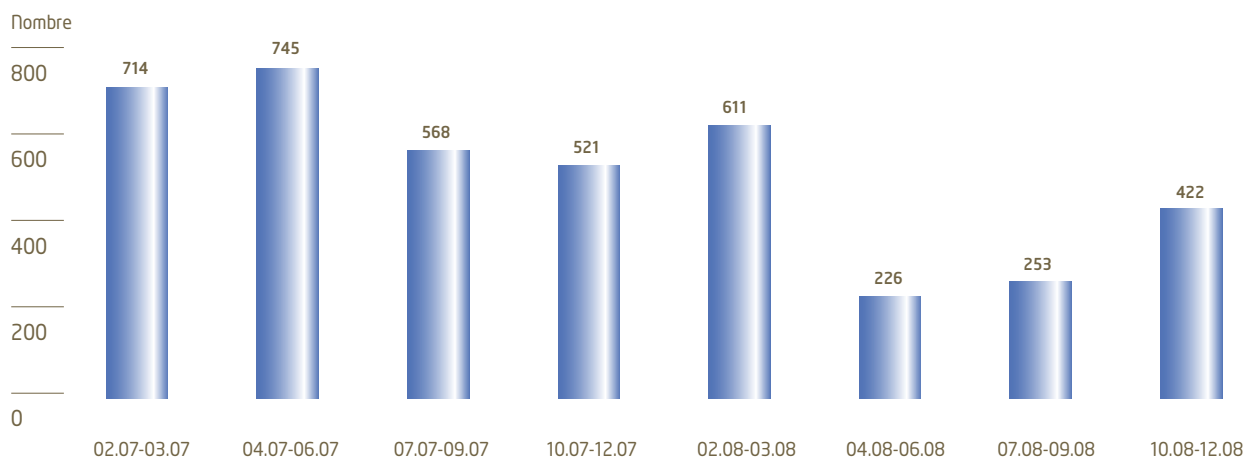
Principales finalités des traitements de données



9.6.8 Appels téléphoniques traités par le front office

9.6.8.1 Analyse globale des dossiers téléphoniques

Appels FO	Trimestre	Appels entrants FO
Activités 2007	02.07 - 03.07	714
	04.07 - 06.07	745
	07.07 - 09.07	568
	10.07 - 12.07	521
		2.548
Activités 2008	02.08 - 03.08	611
	04.08 - 06.08	226
	07.08 - 09.08	253
	10.08 - 12.08	422
		1.512

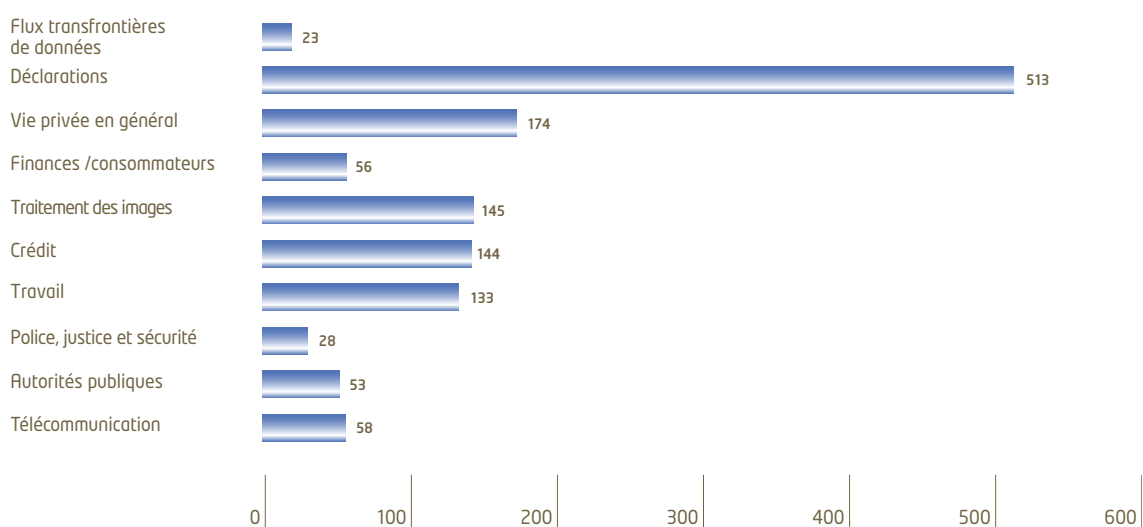


■ Appels entrants FO

9.6.8.2 Analyse des dossiers téléphoniques 2008

	01.08 - 03.08	04.08 - 06.08	07.08 - 09.08	10.08 - 12.08	Nombre	%
Télécommunication	14	13	18	13	58	3,84
Autorités publiques	16	13	8	16	53	3,51
Police, justice et sécurité	14	4	4	6	28	1,85
Travail	36	27	29	41	133	8,80
Sécurité sociale	0	0	1	0	1	0,07
Crédit	54	8	35	47	144	9,52
Listes négatives	3	1	1	0	5	0,33
Traitement des images	52	24	30	39	145	9,59
E-gouvernement	4	0	3	3	10	0,66
Santé	5	0	1	3	9	0,60
Finances / consommateurs	25	9	10	12	56	3,70
Presse et médias	0	0	1	0	1	0,07
Flux transfrontières de données	9	5	3	6	23	1,52
Copropriété / syndic	0	1	1	2	4	0,26
Élections	0	0	0	1	1	0,07
Vie privée en général	86	25	19	44	174	11,51
Déclarations	232	63	68	150	513	33,93
Divers	61	33	21	39	154	10,19
Global	611	226	253	422	1.512	100,00

Les 10 thèmes les plus populaires du front office



9.6.9 Analyse comparative : 2007 - 2008

9.6.9.1 Ouverture des dossiers

	2007	2008	▲ in - chiffres absolus	▼ in - pourcentage
IP	1.538	1.988	450	29,26
IC	351	327	-24	-6,84
I3	87	159	72	82,76
I8	197	154	-43	-21,83
C	39	13	-26	-66,67
SS	90	66	-24	-26,67
AF-MA	11	11	0	0,00
STAT-MA	5	40	35	700,00
RN -MA	61	73	12	19,67
A	42	49	7	16,67
Dossiers de déclaration RPR	5.111	4.133	-978	-19,14
Appels téléphoniques FO	2.548	1.512	-1036	-40,66

9.6.9.2 Clôture des dossiers

	2007	2008	▲ in - chiffres absolus	▼ in - pourcentage
IP	1.094	1.586	492	44,97
IC	256	256	0	0,00
I3	28	31	3	10,71
I8	139	139	0	0,00
C	21	3	-18	-85,71

IP	Informations - plaintes d'ordre général
IC	Crédit à la consommation
I3	Accès indirect
I8	Déclaration et registre public
C	Dossier de contrôle
SZ	Problématique des autorisations "Sécurité sociale"
AF-MA	Autorisation "Autorité fédérale"
STAT-MA	Autorisation "Comité de surveillance statistique"
RN-MA	Autorisation "Registre national"
A	Demandes d'avis (article 29 de la Loi vie privée)
RPR	Registre public
FO	Front office - aide de première ligne

Deuxième partie : les comités sectoriels

1 La composition des comités sectoriels

La Commission compte actuellement six comités sectoriels.

Ces comités sont compétents pour les traitements de données effectués dans des secteurs spécifiques.

Ils sont généralement composés pour une moitié des membres de la Commission et pour l'autre moitié d'experts du secteur.

Des comités sectoriels institués au sein de la Commission veillent à ce que les traitements de données à caractère personnel effectués dans divers secteurs spécifiques ne portent pas atteinte à la vie privée. Ces comités rassemblent des membres de la Commission et des experts choisis pour leur connaissance pratique du secteur concerné. Pour l'heure, six comités sectoriels ont été créés.

Les comités sectoriels ont été institués au sein de la Commission, soit par la Loi du 8 décembre 1992, soit par une loi relative au secteur spécifique du comité sectoriel.

A quelques exceptions près, les comités sectoriels sont composés à parts égales de membres de la Commission et d'experts du secteur concerné.

La Commission désigne elle-même ses représentants au sein du comité sectoriel, alors que les autres membres de ce dernier sont nommés par la Chambre des Représentants. Quoi qu'il en soit, tous sont désignés pour un mandat renouvelable de six ans et peuvent d'une manière ou d'une autre se prévaloir d'une expertise en matière de protection de la vie privée et de gestion des données à caractère personnel.

La présidence des comités sectoriels est en principe assurée par le président de la Commission.

Le président de chaque comité sectoriel doit en tout cas veiller à ce que les décisions prises n'aillent pas à l'encontre des positions défendues par la Commission. Dans ce cadre, il est ainsi autorisé à interrompre le traitement d'un dossier pour le soumettre à l'appréciation de la Commission.

Les comités sectoriels ont pour mission de veiller à ce que tous les traitements de données à caractère personnel effectués dans le secteur dont ils sont responsables respectent la vie privée des personnes concernées. Leurs compétences ne sont pas nécessairement identiques.

Sauf si d'autres arrangements sont prévus, les comités sectoriels sont assistés par le Secrétariat de la Commission.

1.1 Comité sectoriel du Registre national

Protège les données contenues dans le Registre national.

Contrôle l'utilisation du numéro d'identification.

Veille au respect des lois concernant les cartes d'identité et les registres de la population.

Ce Comité sectoriel a été créé au sein de la Commission par la Loi du 8 août 1983. Il est chargé de veiller à la sécurité et à la protection des données enregistrées dans le Registre national, ainsi que de contrôler l'utilisation du numéro d'identification dudit registre.

Compétences

Les compétences du Comité sectoriel du Registre national sont définies à l'article 16 de la Loi du 8 août 1983 *organisant un Registre national des personnes physiques*.

Elles peuvent être résumées comme suit :

- accorder des autorisations permettant :
 - o d'avoir accès aux informations enregistrées dans le

- o Registre national,
- o d'utiliser le numéro de Registre national ;
- veiller à l'application et au respect des lois concernant :
 - o le Registre national,
 - o les registres de la population,
 - o les cartes d'identité ;
- traiter des éventuelles plaintes ;
- aider à résoudre les litiges ;
- effectuer certaines enquêtes.

1.2 Comité sectoriel de la Sécurité Sociale et de la Santé

Autorise la communication de données relatives à la sécurité sociale et à la santé.

Facilite l'échange d'informations dans le secteur de la sécurité sociale.

Collabore avec les services publics du secteur de la santé.

Le Comité sectoriel de la Sécurité Sociale et de la Santé a été institué au sein de la Commission par la Loi du 15 janvier 1990. Il est chargé de veiller à ce que les traitements de données à caractère personnel effectués via le réseau de la sécurité sociale ne mettent pas en péril la vie privée des assurés sociaux. Il remplit par ailleurs également une mission de contrôle portant plus particulièrement sur la communication des données relatives à la santé.

Compétences

Les compétences du Comité sectoriel de la Sécurité Sociale et de la Santé sont définies à l'article 46 de la Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la Sécurité Sociale.

En plus d'une compétence d'avis, le Comité a notamment le

pouvoir d'autoriser la transmission électronique de données à caractère personnel au sein du réseau spécialement créé en vue de faciliter l'échange d'informations dans le secteur de la sécurité sociale. Il est également habilité à autoriser la communication de données à caractère personnel relatives à la santé. Il veille à l'application et au respect de la législation en vigueur dans ces matières. Il peut aussi, le cas échéant, traiter les plaintes, contribuer à la résolution des litiges et effectuer certaines enquêtes.

1.3 Comité sectoriel pour l'Autorité Fédérale

Surveille la communication électronique de

données personnelles par les autorités fédérales.

Autorise la communication de données par le SPF ou par un organisme public relevant de l'Autorité fédérale.

Le Comité sectoriel pour l'Autorité Fédérale a été institué au sein de la Commission en vertu de la Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Il est chargé de surveiller la communication électronique des données à caractère personnel par l'administration fédérale.

Compétences

Les compétences du Comité sectoriel pour l'Autorité Fédérale sont définies à l'article 36bis de la Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

Le Comité autorise la communication électronique de données à caractère personnel par un SPF ou par un organisme public doté de la personnalité juridique relevant de l'Autorité fédérale.

1.4 Comité sectoriel de la Banque-Carrefour des Entreprises

Autorise l'accès aux informations détenues par la Banque-Carrefour des Entreprises et leur communication.

Ce Comité sectoriel a été créé au sein de la Commission par la Loi du 16 janvier 2003 pour veiller à la sécurité des traitements de données effectués au sein de la Banque-Carrefour des Entreprises.

Compétences

Les compétences du Comité sectoriel de la Banque-Carrefour des Entreprises sont définies aux articles 18 et 27 de la Loi du 16 janvier 2003 portant création d'une Banque-Carrefour des Entreprises.

Ce comité est habilité à délivrer des autorisations permettant :

- d'avoir accès aux informations détenues par la Banque-Carrefour des Entreprises ;
- de communiquer ces informations.

Il veille à l'application et au respect de la législation en vigueur dans cette matière.

1.5 Comité de surveillance sectoriel Phenix

Veiller à la sécurité et à la confidentialité des échanges de données nécessaires au bon fonctionnement de l'appareil judiciaire belge.

Le Comité de surveillance sectoriel Phenix a été institué au sein de la Commission en vertu de la Loi du 10 août 2005 instituant le système d'information Phenix, en vue de veiller à la sécurité et à la confidentialité des traitements de données effectués par l'appareil judiciaire belge.

Compétences

Les compétences du Comité de surveillance sectoriel Phenix sont définies à l'article 24 de la Loi du 10 août 2005 instituant le système d'information Phenix.

Le Comité de surveillance est compétent pour tout ce qui a trait aux échanges de données nécessaires au bon fonctionnement de la Justice belge (avis et contrôle). Il est également habilité à traiter des plaintes et à contribuer à la résolution des litiges.

1.6 Comité de surveillance statistique

Contrôler la communication des données d'étude codées de la statistique publique et leur utilisation par des tiers.

Le Comité de surveillance statistique a été institué au sein de la Commission par la Loi du 4 juillet 1962. Il est chargé de contrôler la communication de données d'étude codées à des tiers par la Direction générale Statistique et Information économique et l'utilisation de ces données par ces tiers.

Compétences

Les compétences du Comité de surveillance statistique sont principalement définies aux articles 15, 15bis, 24septies et 24octies de la Loi du 4 juillet 1962 relative à la statistique publique.

Le Comité de surveillance statistique est compétent pour :

- autoriser la communication, par la Direction générale Statistique et Information économique, de données d'étude codées à des tiers ;
- approuver le contrat de confidentialité en vertu duquel ces données sont transmises par la Direction générale Statistique et Information économique et peuvent être utilisées

- par le tiers bénéficiaire ;
- formuler des recommandations ;
 - émettre des avis concernant des projets de nouveaux arrêtés ;
 - procéder à certaines enquêtes.

Toute communication doit faire l'objet d'une demande motivée.

2 Les principales activités des comités sectoriels

Voici les principaux documents publiés par ces différents comités sectoriels en 2008, classés par comité.

2.1 Comité sectoriel de la Banque-Carrefour des Entreprises

Avis BCE n° 01/2008 du 11 juin 2008:

- modification de l'accès à la Banque-Carrefour des Entreprises (BCE) ;
- introduction de sanctions et d'une protection préventive.

Le projet d'arrêté royal examiné dans cet avis avait pour principal objectif de préciser l'interdiction de principe de l'accès massif par internet aux données par nature accessibles gratuitement en prévoyant des poursuites pénales pour certains faits. Sur la base des considérants du projet, le blocage technique de l'accès massif serait impossible pour des raisons de coût.

Le Comité a estimé que le contrôle *a posteriori* des infractions représente un coût financier non négligeable pour l'État, un coût par ailleurs vraisemblablement supérieur à celui de mesures préventives de sécurité. Le Comité a donc estimé qu'il fallait mettre en place un processus de blocage technique minimum – dont le coût ne semble pas inabordable – si nécessaire de manière échelonnée dans le temps. Le Comité a également suggéré que le "public search" fasse mention de cette interdiction et que les réponses se réfèrent à l'usage limité des données obtenues, notamment à l'interdiction de les commercialiser.

2.2 Commission loco le Comité de surveillance statistique

Délibérations STAT n° 34/2008 et 36/2008 :

- Direction générale Statistique et Information économique (DGSIE) ;
- communication de données d'étude codées.

Dans son avis juridique et technique, l'institution de gestion DGSIE s'est posé la question de savoir si cette demande, vu son contenu (les données individuelles du Registre national), ne devrait pas être évaluée par le Comité sectoriel du Registre national plutôt que par le Comité de surveillance statistique, ou éventuellement par les deux. La DGSIE s'est également demandé s'il ne relevait pas de sa tâche d'intervenir en tant que boîte aux lettres/guichet des données provenant directement du Registre national ? Il lui semblait en effet plus logique et plus sûr au niveau de la diffusion des données, que les données soient directement fournies via le Registre national.

La Commission, agissant en lieu et place du Comité de surveillance statistique, a estimé que cette autorisation était suffisante et ceci pour les raisons suivantes :

- l'obligation de faire effectuer le codage des données à caractère personnel par la source authentique de données (ici le Registre national) pourrait constituer un bon point de départ mais pour en préserver le caractère protecteur, il est indispensable que ce codage soit effectué en connaissance de cause. Convertir des données à caractère personnel non codées en données à caractère personnel codées est loin d'être évident et doit se faire dans le respect des règles de l'art. Dans cette optique, la DGSIE est plus au fait que le Registre national du processus de codage des données à caractère personnel qui fait partie de ses principales missions légales ;

- les données demandées sont disponibles dans les banques de données de la DGSIE et la communication sous forme codée des données d'étude individuelles en sa possession à des fins de recherche scientifique, même s'il s'agit de données du Registre national, relève typiquement de la compétence du Comité de surveillance statistique telle qu'elle a été fixée dans la Loi statistique publique. Il faut pour le moins admettre que la demande a été introduite auprès du comité sectoriel de la Commission le "plus" compétent ;
- en outre, le Comité de surveillance statistique a autorisé la DGSIE à ne communiquer les données d'étude codées que dans le cadre d'un contrat de confidentialité. Ce contrat de confidentialité garantit que les données fournies par la DGSIE ne peuvent en aucun cas être utilisées à des fins autres que celles stipulées dans la demande ;
- en dépit des objections de la DGSIE, l'avis de l'institution de gestion concernant la communication demandée reste en fin de compte positive pour le chercheur, à condition toutefois que ce dernier tienne compte d'un certain nombre d'autres conditions, auxquelles la Commission se rallie ;
- la suggestion de l'institution de gestion de soumettre éventuellement cette demande à deux délibérations (une de la Commission, en lieu et place du Comité de surveillance statistique, et une du Comité sectoriel du Registre national) n'apporte finalement que peu de plus-value en termes de protection de la vie privée.

Sans préjudice de ce qui précède, la Commission exige bel et bien qu'afin d'exclure raisonnablement toute possibilité de reconnaissance par les responsables de l'étude, la DGSIE utilise les techniques de codage appropriées pour coder les données du Registre national très détaillées demandées.

2.3 Comité sectoriel du Registre national

Recommandation RN n° 02/2008 du 16 avril 2008 :

- carte d'identité électronique (eID) ;
- utilisation comme carte de bibliothèque.

Le Comité a reçu une série de questions sur l'utilisation de la carte d'identité électronique (eID - <http://eid.belgium.be/>) dans les bibliothèques. Dans la recommandation du Comité à ce sujet, ce dernier attire avant tout l'attention sur le fait que l'Arrêté royal relatif au contrôle automatisé de la carte d'identité par des procédés de lecture optiques ou autres prescrit à l'article 6, § 4 de la Loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes d'étranger et aux documents de séjour et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques n'a toujours pas été élaboré.

Le Comité a aussi fait remarquer à ce propos que l'inscription en tant que membre d'une bibliothèque constitue sans équivoque une situation dans laquelle il est logique d'exiger de l'intéressé qu'il prouve son identité. Puisque sur l'eID l'adresse ne figure que sous forme électronique et qu'elle constitue une donnée pertinente pour la bibliothèque, le fait qu'à l'occasion de ce contrôle l'eID soit non seulement présentée mais aussi lue au moyen d'un lecteur de carte est acceptable. Le fait que les données d'identité pertinentes de l'intéressé soient aussi copiées de l'eID dans le fichier des membres au moment de cette inscription ne semble pas non plus excessif. Cette façon de procéder permet d'éviter les éventuelles erreurs de retranscription des données.

L'eID représente l'instrument d'identification idéal et l'Arrêté royal du 25 mars 2003 relatif aux cartes d'identité précise quand elle doit être présentée. Ces conditions de présentation excluent l'utilisation obligatoire de l'eID en tant que carte de bibliothèque. S'il le désire, le citoyen reste bien sûr libre d'utiliser et de présenter sa carte d'identité comme il l'en-

tend. Cela signifie qu'il peut de lui-même choisir d'utiliser sa carte eID comme carte de bibliothèque, mais ce choix ne peut pas lui être imposé. Cela veut aussi dire qu'aucun avantage dont ne pourrait pas bénéficier le titulaire d'une carte de bibliothèque distincte ne peut être lié à l'utilisation de l'eID en tant que carte de bibliothèque.

Recommandation RN n° 04/2008 du 7 mai 2008 :

- données codées du Registre national ;
- utilisation par les antennes provinciales de planning social.

Un dossier concernant une demande introduite par une antenne provinciale de planning social traité par les services de la Commission a soulevé toute une série de questions qui ont nécessité de demander le point de vue du Comité.

La première de ces questions concernait l'allégation selon laquelle une antenne provinciale de planning social ne devait disposer d'aucune autorisation spécifique pour avoir accès aux données du Registre national du fait qu'après l'intervention de l'organe intermédiaire, elle ne reçoit finalement que des données codées.

Le Comité a constaté que ce n'est pas parce que le destinataire des données du Registre national ne les reçoit finalement que sous forme codée qu'il ne doit pas disposer d'une autorisation. Cette constatation repose sur le fait qu'avant que ces données ne soient codées, elles impliquent la consultation et la collecte des données à caractère personnel non codées dans le Registre national au profit de leur destinataire. La Loi du 8 août 1983 *organisant un Registre national des personnes physiques* exige une autorisation pour toute consultation ou collecte de données du Registre national, sans opérer aucune distinction en fonction de la forme sous laquelle ces données sont finalement remises à l'instance habilitée à les recevoir.

Une deuxième question concernait la portée de l'Arrêté royal du 27 février 1985 *autorisant l'accès des gouverneurs de province*

et des députations permanentes des conseils provinciaux au Registre national des personnes physiques. L'article 1^{er} de cet arrêté d'autorisation octroie aux gouverneurs des provinces et aux députations permanentes des conseils provinciaux un accès aux données mentionnées à l'article 3, premier alinéa, 1^o à 9^o, et deuxième alinéa de la LRN pour l'accomplissement des tâches qui relèvent de leur compétence.

La question à laquelle il fallait répondre à cet égard était celle de savoir si la finalité pour laquelle l'antenne provinciale de planning social – qui fait partie de l'administration provinciale – souhaitait obtenir des données du Registre national faisait ou non partie de ces tâches.

De l'avis du Comité, rassembler du matériel chiffré sur des aspects du domaine politique "Bien-être et Santé" pour permettre aux autorités tant provinciales que locales de se faire une idée des besoins dans le domaine des soins aux personnes âgées et des soins à domicile, de la lutte contre la pauvreté ou des soins de santé, par exemple, relève effectivement des tâches confiées à la province.

En ce qui concerne ses activités, l'antenne de planning social peut donc invoquer l'arrêté d'autorisation.

Délibérations RN n° 17/2008, 19/2008 et 50/2008 :

- accès du VDAB à l'information "nationalité" ;
- utilisation du numéro du Registre national par Fedict dans le cadre des applications informatiques ;
- accès d'un hôpital au Registre national via la plateforme eHealth.

Dans sa **délibération RN n° 17/2008 du 16 avril 2008**, le Comité a refusé de donner suite à la demande d'extension de son arrêté d'autorisation en vue de la réalisation d'un monitoring socioéconomique par le VDAB (<http://vdab.be/>) pour lui permettre de consulter la nationalité (y compris son historique) des parents des demandeurs d'emploi. Le Comité a motivé ce refus en se référant, d'une part à l'avis n° 05/ 2008

du 27 février 2008 de la Commission relatif au monitoring des groupes à potentiel et, d'autre part à l'Arrêté du Gouvernement flamand du 30 janvier 2004 portant exécution du décret du 8 mai 2002 relatif à la participation proportionnelle sur le marché de l'emploi en ce qui concerne l'orientation professionnelle, la formation professionnelle, l'accompagnement de carrière et le placement dont il ressort que la nationalité des parents n'est pas pertinente dans ce contexte.

La **délibération RN n° 19/2008 du 7 mai 2008** a autorisé le SPF de la Technologie de l'Information et de la Communication (Fedict – <http://www.fedict.belgium.be>) à accéder aux informations du Registre national et à utiliser le numéro d'identification de ce registre en vue de tester et entretenir des applications informatiques. Dans cette délibération, le Comité a estimé que les applications de Fedict ne doivent être authentifiées vis-à-vis du Registre national que sur la base d'un certificat d'application et que l'identité de l'utilisateur final ne doit donc pas être communiquée au Registre national. En cas de nécessité, par exemple quand une personne souhaite savoir qui a consulté ses données ou quand on a constaté un comportement de consultation divergent, le système des "cercles de confiance" élaboré par le demandeur permet d'identifier l'utilisateur final par les accords conclus entre les différents maillons du flux des informations. Ce système permet donc d'éviter de devoir développer, au sein du Registre national, une banque de données regroupant des données à caractère personnel dont le Registre national n'a pas besoin pour l'exécution de ses missions.

La **délibération RN n° 50/2008 du 12 novembre 2008** a autorisé un hôpital à avoir accès aux données du Registre national. Dans le cadre de cette autorisation, le Comité a cependant prévu des conditions d'accès spécifiques liées à la nouvelle loi relative à l'institution et à l'organisation de la plateforme eHealth récemment approuvée. Le Comité a ainsi considéré que l'accès au Registre national doit s'effectuer soit via la plateforme eHealth, soit via une autre plateforme qui offre des garanties comparables en matière de sécurité

de l'information, notamment sur le plan de la journalisation et du contrôle préventif des accès, également soumise à un contrôle spécifique par le Comité sectoriel de la Sécurité Sociale et de la Santé institué au sein de la Commission de la protection de la vie privée.

2.4 Comité sectoriel pour l'Autorité Fédérale

Délibérations AF n° 03/2008, 04/2008, 05/2008 et 06/2008 du 03 juillet 2008 :

- flux de données électroniques ONEm-SPF Finances ;
- contrôle de la déclaration de revenus des chômeurs en vue de différentes finalités.

Lors de sa séance du 3 juillet 2008, le Comité sectoriel pour l'Autorité Fédérale a autorisé, sous conditions, l'ONEm à mettre en place des communications électroniques de données, entre lui et le SPF Finances.

Dans le cadre de cette demande, le Secrétariat de la Commission a apporté à l'ONEm un soutien continu afin de lui permettre de rédiger sa demande d'autorisation de manière telle que le Comité soit en mesure d'apprécier la demande au regard de la Loi vie privée.

Les traitements de données concernés poursuivent quatre finalités distinctes qui sont :

- la mise en place d'un flux de communications électroniques de données à caractère personnel, entre le SPF Finances et les fonctionnaires de l'ONEm chargés de la gestion administrative des dossiers des chômeurs, relatives aux montants de divers types de revenus déclarés et perçus par les chômeurs en vue de déterminer et d'actualiser la mesure dans laquelle les allocations de chômage doivent être réduites dans le cadre du cumul de la perception d'allocations et de l'exercice autorisé d'une activité lucrative non salariée ;
- la mise en place d'un flux de communications électro-

niques de données à caractère personnel, entre le SPF Finances et les fonctionnaires de l'ONEm en charge de la gestion administrative des dossiers des chômeurs, relatives aux montants de divers types de revenus déclarés et perçus par les chômeurs, pour vérifier le caractère accessoire d'une activité complémentaire exercée par un chômeur qui perçoit des allocations de chômage ;

- la mise en place d'un flux de communications électroniques de données à caractère personnel, entre le SPF Finances et les inspecteurs sociaux de l'ONEm, relatives aux montants de divers types de revenus déclarés et perçus par les chômeurs, pour contrôler l'exactitude et le caractère complet des déclarations sur l'honneur des demandeurs d'allocations de chômage relatives à leurs revenus influençant leur droit aux allocations de chômage ;
- la mise en place d'un flux de communications électroniques de données à caractère personnel, entre le SPF Finances et les inspecteurs sociaux de l'ONEm, relatives aux montants de divers types de revenus déclarés et perçus par les personnes avec lesquelles le chômeur cohabite pour contrôler l'exactitude et le caractère complet des déclarations sur l'honneur des personnes avec lesquelles le demandeur des allocations de chômage cohabite relatives à leurs revenus professionnels et/ou de remplacement.

Révision de la demande d'autorisation du Comité sectoriel pour l'Autorité Fédérale :

- demande d'autorisation de traitement automatisé de données ;
- demande distincte par finalité.

Au vu des problèmes rencontrés sur le terrain par les personnes requérant l'autorisation du Comité sectoriel pour l'Autorité Fédérale de mettre en place des traitements automatisés de données, le Secrétariat de la Commission a entamé un travail de refonte du questionnaire de demande d'autorisation mis à la disposition des demandeurs afin de leur permettre de justifier en quoi le traitement automatisé de

données qu'ils projettent est compatible avec les dispositions de la Loi vie privée.

Des précisions ont été apportées au formulaire afin d'attirer l'attention des demandeurs sur l'importance de préciser le traitement de données qu'ils soumettent à la compétence d'autorisation du Comité et ce, sous divers angles : description exhaustive et précise de la finalité du traitement de données (pourquoi envisage-t-on de mettre en place le traitement automatisé de données ?, quels types d'opérations précises de traitement de données cette (ces) collecte(s) automatisée(s) de données va ou vont-elle(s) servir ?, liste précise des données strictement nécessaires qu'il est envisagé de collecter pour la réalisation de la finalité précise poursuivie, justification du caractère légitime de la finalité poursuivie, description de la mission de service public à la mise en œuvre de laquelle les données collectées vont servir (le cas échéant, description du traitement initial de collecte des données auprès des personnes concernées, des finalités du responsable du traitement ainsi que du caractère légitime de la communication ultérieure des données pour d'éventuelles finalités distinctes), description de l'impact du traitement de données envisagé sur les traitements actuels éventuellement non automatisés réalisés par le demandeur ...

Il est ainsi demandé aux demandeurs d'adresser une demande d'autorisation par finalité distincte poursuivie dans la mesure où les types de données nécessaires devant être collectées, les services en ayant fonctionnellement besoin ou les destinataires, les durées de conservation, ... varient en fonction de la finalité poursuivie. Cette façon de procéder permet au Comité sectoriel d'apprécier la demande d'autorisation au regard des principes de la Loi vie privée.

Dans ce cadre, il a également été rappelé qu'il appartient à l'auteur d'une demande d'autorisation de rédiger cette dernière de manière concertée avec toutes les parties concernées par le flux électronique de données demandé.

Le nouveau formulaire de demande d'autorisation a été approuvé par le Comité à la séance du 3 juillet 2008.

Délibération AF n° 10/2008 du 20 novembre 2008 :

- Agentschap Vlaamse Belastingdienst (VLABEL) (Service flamand des impôts) ;
- données de l'Administration générale de la documentation patrimoniale et du Service des Pensions du secteur public.

Afin de pouvoir percevoir le précompte immobilier en Flandre, VLABEL souhaitait disposer d'un accès à certaines données à caractère personnel se trouvant dans des banques de données de l'Administration générale de la Documentation patrimoniale et du Service des pensions du secteur public. Le Comité a autorisé ces échanges de données moyennant le respect de certaines conditions.

Délibération AF n° 09/2008 du 20 novembre 2008 :

- échange des données organismes assureurs-SPF Finances & SPF-Finances-mutualités ;
- données de revenus des assurés sociaux lors d'une demande de statut OMNIO.

À sa séance du 20 novembre 2008, le Comité sectoriel pour l'Autorité Fédérale a autorisé, sous conditions, les organismes assureurs à mettre en place des communications électroniques de données entre eux et le SPF Finances pour la finalité d'octroi du statut OMNIO et plus précisément dans ce cadre, pour vérifier si les revenus des ménages demandant le statut OMNIO se situent sous le plafond légal.

Le Comité n'a pas été en mesure d'autoriser la mise en place du flux électronique entre le SPF Finances et les 77 mutualités en raison du défaut de légitimité dans le chef de ces dernières à exercer elles-mêmes le contrôle sur les revenus des personnes qui demandent à bénéficier du statut OMNIO. L'Arrêté royal du 1^{er} avril 2007 fixant les conditions d'octroi de l'intervention majorée de l'assurance visée à l'article 37, §§ 1^{er} et 19 de la loi relative

à l'assurance obligatoire soins de santé et indemnités, coordonnée le 14 juillet 1994, et instaurant le statut OMNIO a en effet confié le pouvoir de contrôle des revenus dans ce cadre aux organismes assureurs et non pas aux 77 mutualités.

Au vu de l'article 3 de la Loi du 6 août 1990 relative aux mutualités et aux unions nationales et au vu du fait que les mutualités peuvent être amenées à participer à la gestion de l'assurance obligatoire, dont fait partie le statut OMNIO, moyennant autorisation de l'union nationale, le Comité a tout de même considéré qu'à défaut d'un accès direct à la base de données TAXI-AS, les mutualités étaient autorisées à recevoir de l'organisme assureur concerné le résultat du contrôle des revenus par ce dernier auprès du SPF Finances ou en d'autres termes être informées si oui ou non le statut OMNIO peut être octroyé à un ménage déterminé.

Au vu de l'article 4, § 1^{er}, 3° de la Loi vie privée, le Comité a également précisé qu'en lieu et place d'un accès libre à la base de données TAXI-AS, le SPF Finances devait communiquer aux organismes assureurs si les ménages demandant le droit au statut OMNIO disposent ou non de revenus se situant en dessous du plafond légal fixé à l'article 38 de l'Arrêté royal précité du 1^{er} avril 2007 pour pouvoir bénéficier du statut OMNIO. Le Comité a toutefois précisé à ce sujet qu'il ne s'opposait pas à ce que les organismes assureurs disposent des revenus détaillés lorsque cela s'avère nécessaire pour la gestion d'un dossier particulier dans le cadre d'une demande de contrôle d'une décision d'octroi ou de refus du bénéfice du statut OMNIO.

2.5 Comité sectoriel de la Sécurité Sociale et de la Santé

Avis n° 09/2008 du 27 février 2008 :

- projet d'arrêté royal portant instructions pour les pharmaciens ;
- dossier pharmaceutique.

C'est à l'intervention du Conseil d'État que ce projet d'arrêté royal a été soumis à l'avis de la Commission de la protection de la vie privée. Le Conseil d'État a, en effet, estimé qu'en application de l'article 7, § 3, de la Loi vie privée, tout projet d'arrêté royal portant sur un traitement de données de santé doit être délibéré en Conseil des ministres et soumis à l'avis de la Commission de la protection de la vie privée.

Le projet d'arrêté royal impose aux pharmaciens une série d'obligations en matière de tenue d'un "dossier pharmaceutique" pour chaque patient, ainsi que d'un "dossier du suivi des soins pharmaceutiques", pour les patients qui y ont consenti par écrit. Ces dossiers contiennent des données administratives, de nombreuses données relatives à la santé et parfois des données judiciaires.

La Commission de la protection de la vie privée a estimé le projet d'arrêté compatible avec la Loi vie privée, moyennant quelques adaptations et clarifications. Elle a donc émis un avis favorable sous certaines conditions.

Avis n° 14/2008 du 02 avril 2008 :

- projet de loi sur la création d'une plateforme *eHealth* ;
- échange électronique sécurisé de données relatives à la santé.

Le projet de loi soumis à l'avis de la Commission concerne la création, au sein de la Banque Carrefour de la sécurité sociale (www.ksz-bcss.fgov.be), d'une nouvelle institution publique dotée de la personnalité juridique : la plateforme *eHealth*. Cette plateforme est destinée, essentiellement, à offrir une infrastructure et des services de base pour l'échange sécurisé de données de santé entre les différents acteurs du secteur de la santé, et à servir d'organisation intermédiaire chargée de la collecte et du codage de données destinées à la recherche historique, statistique ou scientifique. Le numéro de Registre national et le numéro d'identification de la sécurité sociale serviront d'identifiants au sein de la plateforme *eHealth*. Celle-ci conservera par ailleurs un répertoire des références

repreuant, pour les patients qui y consentent, chez quels acteurs de la santé quels types de données à caractère personnel sont repris les concernant. Ce répertoire servira à canaliser les demandes de données vers l'endroit où ces dernières sont disponibles et à assurer un contrôle d'accès préventif.

La Commission a estimé que dans ce contexte, une plateforme décentralisée de ce type qui se contente de véhiculer des données mais ne conserve aucune donnée à caractère personnel (à l'exception néanmoins de celles contenues dans le répertoire des références), va dans le sens d'un respect satisfaisant de la vie privée des patients concernés et répond ainsi aux recommandations du Groupe 29 (document de travail 131 sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques).

Le rôle d'*eHealth* en tant qu'organisation intermédiaire correspond aux vœux émis par la Commission de faire assurer le codage en vue de la recherche historique, statistique ou scientifique par un tiers indépendant et neutre respectant les principes de protection de la vie privée. La Commission a par ailleurs insisté sur la nécessité que cette organisation intermédiaire ne puisse effectuer aucune recherche elle-même.

En ce qui concerne l'utilisation du numéro de Registre national comme identifiant au sein de la plateforme *eHealth*, la Commission a rappelé sa jurisprudence générale, qui tend à favoriser l'usage d'identifiants sectoriels. Néanmoins, vu l'importance de garantir une identification fiable et dans le cas présent, la nécessité de veiller à ce que tous les acteurs de la santé utilisent le même identifiant, l'impossibilité des interconnexions vu le fait qu'aucune donnée n'est stockée dans *eHealth*, et l'usage très large qui sera fait d'un éventuel numéro sectoriel, la Commission a estimé qu'un tel identifiant sectoriel n'offrirait en l'occurrence pas de meilleure protection de la vie privée que le numéro de Registre national.

La Commission a également insisté sur le rôle important du

conseiller en sécurité et le médecin responsable d'eHealth.

Délibération n° 08/048 du 02 septembre 2008 :

- introduction de données relatives à la santé dans eCare par les orthopédistes ;
- introduction dans et accès via la plateforme eHealth.

En vertu de la Loi du 13 décembre 2006 portant dispositions diverses en matière de santé (article 42, § 2, 3°), la section Santé du Comité sectoriel de la Sécurité Sociale et de la Santé est compétente pour octroyer une autorisation de principe concernant toute communication de données à caractère personnel relatives à la santé. Toutefois, la date et les modalités d'entrée en vigueur de cette disposition légale doivent être fixées par le Roi, ce qui n'a pas encore été fait.

La section Santé du Comité a néanmoins estimé pouvoir se prononcer, en l'occurrence en application de l'article 46, § 2, de la Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque Carrefour de la sécurité sociale qui prévoit la compétence générale du Comité sectoriel de la Sécurité Sociale et de la Santé pour veiller au respect des dispositions fixées par ou en vertu de la loi et visant à la protection de la vie privée à l'égard des traitements de données à caractère personnel relatives à la santé.

Le projet eCare vise à constituer une base de données à caractère personnel concernant certaines pathologies. Dans cette base de données, les spécialistes de ces pathologies pourront enregistrer les données relatives à leurs propres patients et consulter celles relatives à ces mêmes patients enregistrées par d'autres praticiens.

L'accès des praticiens à la base de données eCare se fait grâce à une connexion sécurisée fournie par la plateforme eHealth (qui se charge de l'identification, de l'authentification et de l'accès), sur la base uniquement du numéro de sécurité sociale qui figure sur la carte d'identité électronique du prati-

cieu (pas de login ni de mot de passe). Le praticien peut aussi mandater d'autres personnes travaillant dans le même hôpital pour traiter les données à caractère personnel de ses patients. Dans ce cas, la plateforme eHealth vérifiera si la personne qui demande l'accès est bien mandatée par un praticien ayant lui-même accès à eCare. Elle ne vérifiera néanmoins pas si la personne mandatée est un professionnel des soins de santé tenu au secret médical.

La demande ayant donné lieu à cette délibération concerne l'accès des orthopédistes à la base de données eCare. La finalité de cet accès est de constituer une base de données relative aux prothèses de la hanche et du genou (identité du prestataire de soins, identité du patient, diagnostic, opération effectuée, nature de la prothèse placée, etc.).

Le consentement du patient à l'intégration de ses données à caractère personnel dans eCare n'est pas demandé. La section Santé du comité sectoriel estime néanmoins que le traitement des données de santé envisagé est légitime et légal en application de l'article 7, § 2, j de la Loi vie privée (traitement nécessaire aux fins de médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitement soit à la personne concernée, soit à un parent, ou de la gestion de services de santé agissant dans l'intérêt de la personne concernée et les données sont traitées sous la surveillance d'un professionnel des soins de santé).

La section Santé estime aussi que la consultation de la base de données n'exige pas d'autorisation de sa part, étant donné qu'il s'agit d'une communication de données entre professionnels des soins de santé tenus au secret professionnel et associés en personne à l'exécution des actes de diagnostic, de prévention ou de prestation de soins à l'égard du patient (sauf en ce qui concerne les personnes mandatées bien entendu) (application de l'article 42, § 2, 3° de la Loi du 13 décembre 2006 précitée).

Seuls les orthopédistes ayant besoin des données pour le traitement d'un patient peuvent accéder à la base de données *eCare*. Ceci ne fait néanmoins l'objet d'aucune vérification. Toute autre mise à disposition des données d'*eCare* devra faire l'objet d'une nouvelle autorisation de la section Santé du Comité sectoriel.

En conclusion, la section Santé estime que le traitement des données à caractère personnel envisagé répond aux exigences légales et réglementaires en matière de vie privée

3 Les activités des comités sectoriels en chiffres

Des comités sectoriels ont été institués au sein de la Commission. Ces comités veillent au respect de la législation relative à la vie privée dans certains secteurs. Six comités sectoriels ont été créés parmi lesquels 5 ont été constitués : le Comité sectoriel du Registre national, le Comité sectoriel de la Sécurité Sociale et de la Santé, le Comité sectoriel pour l'Autorité Fédérale, le Comité sectoriel de la Banque-Carrefour des Entreprises et le Comité de surveillance sectoriel Phenix. Le Comité de surveillance statistique n'a pas encore été constitué et c'est la Commission qui exerce ses compétences pour le moment.

3.1 Le Comité sectoriel de la Sécurité Sociale et de la Santé

Le Comité sectoriel de la Sécurité Sociale et de la Santé traite les demandes relatives à la communication électronique des données à caractère personnel au sein du réseau d'échange de données de la sécurité sociale. En 2008, 66 autorisations ont été accordées.

3.2 Le Comité sectoriel pour l'Autorité Fédérale

Le Comité sectoriel pour l'Autorité Fédérale surveille la communication électronique des données à caractère personnel au sein de l'Autorité fédérale et accorde les autorisations de communication électronique de données à caractère personnel par les SPF ou les organismes publics dotés de la personnalité juridique relevant de l'Autorité fédérale. En 2008, le nombre de demandes est resté stable avec 11 demandes comme en 2007. Sur l'ensemble de ces dossiers auxquels ont été ajoutés les 6 dossiers de 2007 encore en cours de traitement, des autorisations ont été accordées dans 8 dossiers. Huit dossiers sont encore en cours de traitement, soit parce

des renseignements complémentaires ont été demandés au demandeur, soit parce que leur délibération est en préparation. Un dossier a été classé sans suite.

3.3. Le Comité sectoriel du Registre national

L'octroi d'autorisations pour la communication de données du Registre national et l'utilisation du numéro d'identification du Registre national relève de la compétence du Comité sectoriel du Registre national. En 2008, la tendance à la hausse du nombre de ces dossiers notée en 2007 s'est maintenue et 73 demandes d'autorisations ont été introduites. Sur l'ensemble de ces dossiers auxquels il faut encore ajouter les dossiers de 2007 encore en cours de traitement, 56 autorisations ont été accordées avec ou sans conditions suspensives et 4 dossiers ont été classés sans suite. Les autres dossiers sont encore en cours de traitement.

3.4 Le Comité sectoriel de la Banque-Carrefour des Entreprises et le Comité de surveillance sectoriel Phenix

Ni le Comité sectoriel de la Banque-Carrefour des Entreprises – qui veille à la sécurité du traitement des données au sein de la Banque-Carrefour – ni le Comité de surveillance sectoriel Phenix – qui veille à la sécurité et à la confidentialité des traitements de données effectués par l'appareil judiciaire belge – n'ont reçu des demandes d'autorisation.

Le Comité sectoriel de la Banque-Carrefour des Entreprises a néanmoins émis un avis.

3.5 Tableaux et graphiques

3.5.1 Avis et autorisations du Comité sectoriel de la Sécurité Sociale et de la Santé

En 2008, 66 autorisations ont été accordées.

En 2008, 20 avis ont été émis.

3.5.2 Avis et autorisations de la Banque-Carrefour des Entreprises

En 2008, 1 avis a été émis.

3.5.3 Avis et autorisations du Comité sectoriel pour l'Autorité Fédérale

AF-MA dossier		Nombre
AF-MA 2007	in	11
	out - 2007	5
	out - 2008	4
	ouverts	2
AF-MA 2008	in	11
	out	5
	ouverts	6

Suite donnée aux dossiers traités en 2008 (AF-MA 2007 et 2008)

	Nombre
Délibération	8
Sans objet	1
Dossiers en cours de traitement	8

3.5.4 Avis et autorisations du Comité sectoriel du Registre national

3.5.4.1 Les dossiers d'avis (dossiers A) en chiffres

En 2008, 1 avis a été émis.

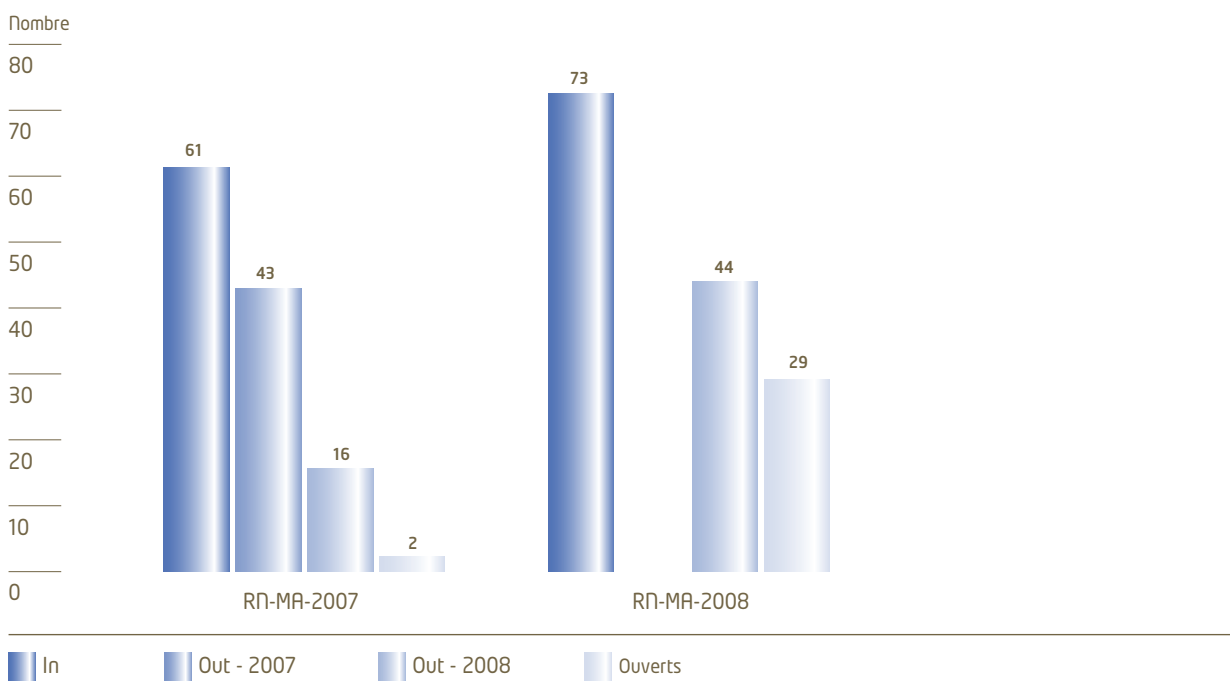
3.5.4.2 Les dossiers de recommandation (dossiers REC) en chiffres

En 2008, 4 recommandations ont été émises.

3.5.4.3 Dossiers d'autorisations (dossiers MA) en chiffres

Évolution des dossiers RN : 2007-2008

Dossiers RN-MA		Nombre	%
RN-MA 2007	in	61	
	out - 2007	43	70,49
	out - 2008	16	26,23
	ouverts	2	3,28
<hr/>			
RN-MA 2008	in	73	
	out	44	60,27
	ouverts	29	39,73

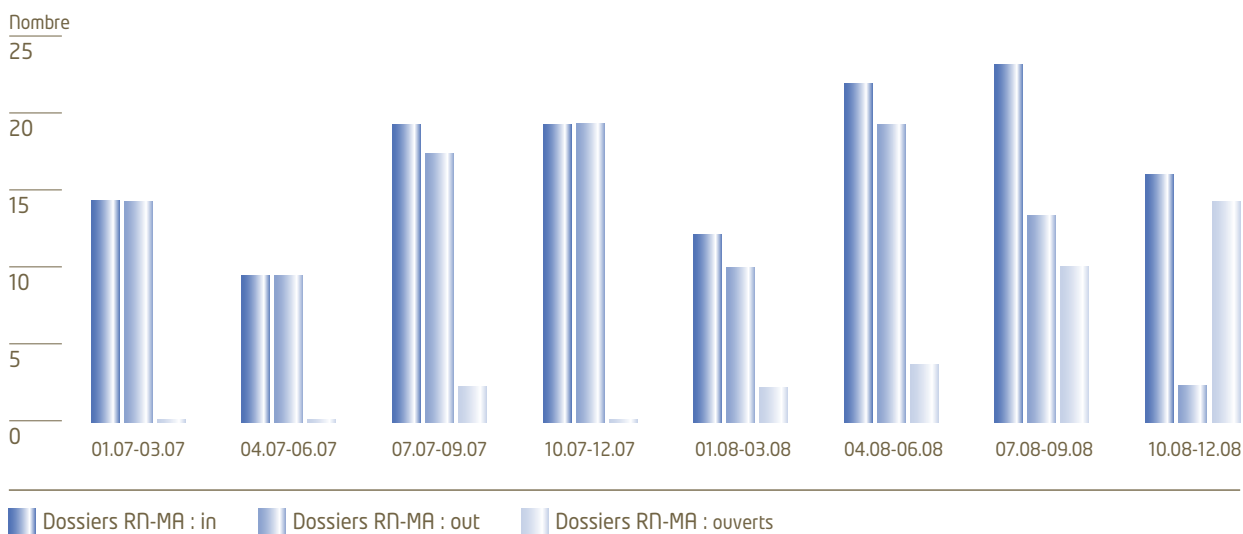


Nombre de dossiers clôturés : comparaison 2007 - 2008

	Type	Nombre	%
Activités 2007	RN-2006	3	6,52
	RN-2007	43	93,48
		46	
Activités 2008	RN-2007	16	26,67
	RN-2008	44	73,33
		60	

Dossiers RN : évolution trimestrielle

Dossiers RN-MA	Trimestre	Dossiers RN-MA in	Dossiers RN-MA out	% clôturés	Dossiers RN-MA ouverts
Activités 2007	01.07 - 03.07	14	14	100,00	0
	04.07 - 06.07	9	9	100,00	0
	07.07 - 09.07	19	17	89,47	2
	10.07 - 12.07	19	19	100,00	0
		61	59	96,72	2
Activités 2008	01.08 - 03.08	12	10	83,33	2
	04.08 - 06.08	22	19	86,36	3
	07.08 - 09.08	23	13	56,52	10
	10.08 - 12.08	16	2	12,50	14
		73	44	60,27	29



Suite donnée aux dossiers clôturés en 2008 (RN-MA 2007 et RN-MA 2008)

	Nombre	%
Délibération	56	93,33
Sans objet	4	6,67

