5 - 1428/1

# SÉNAT DE BELGIQUE

**SESSION DE 2011-2012**

7 MARS 2012

## Informatique et libertés

## RAPPORT

FAIT AU NOM DE LA COMMISSION
DE LA JUSTICE
PAR
M. **MAHOUX**

## I. INTRODUCTION

Conformément à l'article 26 du règlement du Sénat, la commission de la Justice a décidé lors de sa réunion du 14 décembre 2010 de constituer un groupe de travail « Informatique et libertés ».

M. Philippe Mahoux a été désigné président dudit groupe de travail.

Le groupe de travail « Informatique et libertés » a entamé ses travaux le 22 mars 2011 et a procédé à plusieurs auditions en vue de prendre connaissance d'une part des avancées techniques en matière d'internet et, d'autre part, des évolutions comportementales

# BELGISCHE SENAAT

**ZITTING 2011-2012**

7 MAART 2012

## Informatica en vrijheden

## VERSLAG

NAMENS DE COMMISSIE VOOR
DE JUSTITIE
UITGEBRACHT DOOR
DE HEER **MAHOUX**

## I. INLEIDING

Overeenkomstig artikel 26 van het Reglement van de Senaat, heeft de commissie voor de Justitie op haar vergadering van 14 december 2010 beslist een werkgroep « Informatica en vrijheden » op te richten.

De heer Philippe Mahoux werd als voorzitter van die werkgroep aangewezen.

De werkgroep « Informatica en vrijheden » vatte zijn werkzaamheden aan op 22 maart 2011 en hield verscheidene hoorzittingen om kennis te nemen van de technische vooruitgang inzake internet en van de ontwikkelingen in het gedrag van de internauten, en

des internautes et d'envisager une révision du cadre juridique existant.

Le groupe de travail a consacré cinq réunions à ces auditions, qui ont eu lieu les 6 et 26 avril, 11 et 24 mai et 15 juin 2011. Ont été entendus (par ordre chronologique) :

— M. Stéphane Verschueren, vice-président de la Commission pour la protection de la vie privée (CPVP);

— M. Rogier Klimbie, représentant de Google;

— Mme Isabelle De Vinck, MM. Geert Somers et Bruno Schroder, représentants de l'Asbl « ISPA » (*Internet Service Provider Association*);

— M. Luc Beirens, Directeur de la *Federal Computer Crime Unit* (FCCU);

— M. Philippe van Linthout, juge d'instruction;

— Mme de Terwangne et M. Van Gysehem, représentants du CRIDS (centre de recherche informatique, droit et société);

— Mme Marie-Hélène Boulanger, chef d'unité « protection de données », DG Justice, Commission européenne.

## II. EXPOSÉ INTRODUCTIF DE M. MAHOUX

### Enjeux

M. Mahoux rappelle les enjeux de la problématique.

La sphère internet permet l'accès à des milliards d'informations, et leur partage. Parmi ces informations, des données personnelles, intimes et privées peuvent être enregistrées sur le net par les traces laissées par des navigations, à l'insu des navigants, ou révélées volontairement sur des réseaux sociaux, des blogs et des forums.

Cette accumulation de données personnelles pose le problème de l'application du droit de la personne, en premier lieu le droit au respect de la vie privée, sur les différentes applications proposées sur le web.

Le premier enjeu est sans doute celui de l'information : chacun est-il véritablement informé de l'exploitation de son intimité à des fins commerciales ou autres ? Et des conséquences potentielles de la mise en ligne, même volontaire, d'informations personnelles,

om een herziening van het juridische kader te overwegen.

De werkgroep besteedde vijf vergaderingen aan die hoorzittingen, die plaatsvonden op 6 en 26 april, 11 en 24 mei en 15 juni 2011. Volgende personen werden gehoord (in chronologische volgorde) :

— De heer Stéphane Verschueren, ondervoorzitter van de Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL);

— De heer Rogier Klimbie, vertegenwoordiger van Google;

— Mevrouw Isabelle De Vinck, de heren Geert Somers en Bruno Schroder, vertegenwoordigers van de VZW « ISPA » (*Internet Service Provider Association*);

— De heer Luc Beirens, Directeur van de *Federal Computer Crime Unit* (FCCU);

— De heer Philippe van Linthout, onderzoeksrechter;

— Mevrouw de Terwangne en de heer Van Gysehem, vertegenwoordigers van het CRIDS (*centre de recherche informatique, droit et société*);

— Mevrouw Marie-Hélène Boulanger, hoofd Eenheid Gegevensbescherming », DG Justitie, Europese Commissie.

## II. INLEIDENDE UITEENZETTING VAN DE HEER MAHOUX

### Uitdagingen

De heer Mahoux herinnert aan de uitdagingen rond deze problematiek.

De wereld van internet biedt toegang tot miljarden gegevens en biedt tevens de mogelijkheid gegevens te delen. Onder die gegevens bevinden zich persoonlijke, intieme en private gegevens die op het web kunnen worden geregistreerd, zonder dat de surfers dat weten, door de sporen van het surfen of die vrijwillig worden bekendgemaakt op sociale netwerken, blogs en forums.

Die accumulatie van persoonlijke data doet het probleem rijzen van de toepassing van het recht van de persoon, in de eerste plaats het recht op privacy op de diverse toepassingen die op internet worden aangeboden.

De eerste uitdaging is ongetwijfeld die van de informatie : wordt iedereen werkelijk op de hoogte gebracht van de exploitatie van zijn intimiteit voor handelsdoeleinden of andere doeleinden ? En van de mogelijke gevolgen van het, zelfs vrijwillig, *on line*

photos etc.. sur la toile mondiale ? Comment former et informer les utilisateurs, particulièrement les jeunes, sur ces risques et sur les bonnes pratiques à adopter pour maîtriser son image et son identité sur Internet ?

Le second enjeu est celui de la protection du droit des personnes sur Internet. Droit à la vie privée, droit à l'image : les normes légales sont-elles adaptées à la pratique d'internet ? Sont-elles adaptables pour faciliter concrètement leur application ? De quelles protections légales l'utilisateur dispose-t-il concrètement ?

Une nouvelle question se pose également en ce qui concerne l'application de ces normes de droit à internet : le « droit à l'oubli numérique ». Est-il possible de faire table rase de son passé numérique ? L'oubli numérique est un droit de plus en plus invoqué, mais qui reste aujourd'hui encore confus voire abstrait. De la limitation légale de durée de conservation des données personnelles au droit d'accès, de suppression et d'opposition, son périmètre ne cesse d'augmenter à la mesure de l'évolution des usages et technologies d'Internet. En pratique, la disparité des solutions développées par chaque service web contribue à rendre ces droits peu lisibles et difficiles à exercer.

Le troisième enjeu concerne la protection des données. Certaines données ne devraient-elles pas être particulièrement protégées ? Par exemple, la transmission de données génétiques ne devrait-elle pas être spécifiquement encadrée, et réservée à la recherche scientifique pure ?

Internet étant un réseau mondial, les règles minimales d'encadrement de l'usage et du traitement des informations devraient être adoptées à l'échelon mondial. Actuellement, les seuls principes établis internationalement relèvent de la « *soft law* » : il s'agit notamment des résolutions des conférences des Commissions de protection de la vie privée et du traitement de données (dont la Résolution de Madrid, qui établit des Standards minimums que les différentes Commissions nationales s'engagent à faire respecter dans leurs États).

Mais les États ont bien entendu un rôle à jouer, tant pour œuvrer à l'élaboration de textes internationaux contraignants que pour anticiper, ou compléter et préciser ces normes.

Les parlements et exécutifs de plusieurs pays membres de l'Union européenne mènent d'ailleurs actuellement des réflexions sur ces enjeux dans le but de renforcer et compléter les lois sur la protection de la vie privée et le traitement des données.

Enfin, M.Mahoux rappelle qu'il conviendra de prendre en compte les législations suivantes :

brengen van persoonlijke informatie, foto's, enz. op het *world wide web* ? Hoe kan men de gebruikers, vooral de jongeren, vormen en informeren over die risico's en de goede praktijken die men zich eigen moet maken om zijn imago en identiteit op internet onder controle te houden ?

De tweede uitdaging is die van de bescherming van het recht van de personen op het internet. Recht op leven, recht op het imago : zijn de wettelijke normen aangepast aan het internet ? Zijn ze aanpasbaar, om de toepassing ervan concreet mogelijk te maken ? Welke wettelijke bescherming geniet de gebruiker concreet ?

Er rijst ook een nieuw probleem betreffende de toepassing van die rechtsnormen op internet : het « recht op digitale vergetelheid ». Kan men tabula rasa maken van zijn digitale verleden ? Men heeft het steeds vaker over het recht op digitale vergetelheid, maar het blijft vandaag nog een verward of zelfs abstract begrip. Van de wettelijke beperking van de bewaartijd van de persoonlijke gegevens tot het recht op inzage, schrappen en verzet : de perimeter ervan blijft groeien met de ontwikkeling van de gebruiken en technologieën van internet. In de praktijk draagt de verscheidenheid van de door elke internetdienst ontwikkelde oplossingen ertoe bij dat die rechten weinig leesbaar en moeilijk uit te oefenen zijn.

De derde uitdaging behelst de bescherming van de data. Moeten bepaalde data niet speciaal worden beschermd ? Moet er bijvoorbeeld geen specifieke regeling komen voor de overdracht van genetische data, die voorbehouden blijft voor zuiver wetenschappelijk onderzoek ?

Internet is een wereldwijd netwerk en de minimale regels voor het gebruik en de verwerking van de gegevens moeten op wereldschaal worden aangenomen. Momenteel behoren de internationaal vastgelegde beginselen tot de « *soft law* » : het gaat onder andere om de resoluties van de conferenties van de Commissies voor de bescherming van de persoonlijke levenssfeer en van de dataverwerking (waaronder de Resolutie van Madrid, die minimumstandaarden vaststelt die de diverse nationale commissies in hun respectieve staten moeten doen naleven).

De Staten hebben echter vanzelfsprekend een rol te spelen, zowel om zich in te zetten voor de totstandkoming van bindende internationale teksten, als om op die normen te anticiperen, ze aan te vullen en ze nader te bepalen.

De parlementen en executieven van verscheidene lidstaten van de Europese Unie reflecteren overigens momenteel over die uitdagingen, om de wetten ter bescherming van de privacy en de dataverwerking te versterken en aan te vullen.

Tot slot herinnert de heer Mahoux eraan dat met de volgende wetten rekening moet worden gehouden :

— La Convention européenne des Droits de l'homme et son article 8,

— La Directive 2002/58/CE sur la protection de la vie privée et les communications électroniques

— La loi du 8 décembre 1992 relative à la protection de la vie à l'égard du traitement de données à caractère personnel.

Mais aussi la résolution de Madrid relative aux « *International Standards on the protection of personal data and privacy* » qui est à considérer comme de la « *soft law* ».

— het Europees Verdrag van de rechten van de mens en zijn artikel 8,

— richtlijn 2002/58/EG betreffende privacy en elektronische communicatie

— de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

Maar ook met de resolutie van Madrid betreffende de « *International Standards on the protection of personal data and privacy* », die als « *soft law* » moet worden beschouwd.

## III. AUDITIONS

### A. Audition du 6 avril 2011

*1. Exposé de M. Stéphane Verschueren, vice-président de la Commission pour la protection de la vie privée (CPVP)*

M. Verschueren précise qu'il est accompagné de M. Marc Lognoul, et Mme Corten, responsables de la section « Études, recherches et enquêtes » ainsi que de M. Vansensen, responsable du « Frontdesk », qui constitue le point de contact avec l'ensemble des plaignants et des personnes qui saisissent la Commission d'une simple demande de renseignements.

L'orateur propose de rappeler brièvement ce qu'est la Commission, quel est son rôle et comment elle fonctionne, et de faire ensuite un exposé sur l'état de certains dossiers qui paraissent emblématiques.

#### Rôle et fonctionnement de la CPVP

La CPVP est un organe collatéral de la Chambre des représentants, comme le sont la Cour constitutionnelle, la Cour des Comptes, le médiateur fédéral, le Comité P, et le Comité R.

Ce statut lui a été donné pour garantir son indépendance, parce que celle-ci est requise par une la directive européenne 95/46 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, qui impose à tous les pays de l'Union européenne de disposer d'un contrôle sur le traitement des données à caractère personnel. L'organe de contrôle le plus connu et le plus ancien est sans doute la CNIL française (Commission Nationale Informatique et Libertés).

La CPVP fonctionne comme une juridiction. Elle est composée de huit membres effectifs et de huit membres suppléants, et siège généralement en assemblée plénière, qui réunit les effectifs et les suppléants.

## III. HOORZITTINGEN

### A. Hoorzitting van 6 april 2011

*1. Uiteenzetting van de heer Stéphane Verschueren, ondervoorzitter van de Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL)*

De heer Verschueren preciseert dat hij vergezeld wordt door de heer Marc Lognoul, en mevrouw Corten, afdelingshoofden « Studie en onderzoek », alsook door de heer Vansensen, hoofd van de « Frontdesk », het contactpunt voor alle klagers en personen die een eenvoudige vraag om informatie aan de Commissie stellen.

Spreker stelt voor kort te herhalen wat de Commissie is, wat haar rol is en hoe ze werkt en vervolgens een uiteenzetting te houden over de stand van zaken van een aantal emblematische dossiers.

#### Rol en werking van de CBPL

De CBPL is een collateraal orgaan van de Kamer van volksvertegenwoordigers, zoals het Grondwettelijke Hof, het Rekenhof, de federale ombudsman, het Comité P en het Comité I.

Ze heeft die status gekregen om haar onafhankelijkheid te waarborgen, omdat die geëist wordt door de Europese richtlijn 95/46 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, die alle landen van de Europese Unie ertoe verplicht de verwerking van persoonsgegevens te controleren. Het best gekende en oudste orgaan is ongetwijfeld de Franse CNIL (*Commission Nationale Informatique et Libertés*).

De CBPL werkt als een rechtscollege. Ze bestaat uit 8 leden en 8 plaatsvervangers en houdt meestal in plenaire vergadering zitting, met de leden en de plaatsvervangers. De beslissingen worden bij consen-

Les décisions sont prises par consensus et sont le résultat de discussions parfois longues.

Les membres sont assistés d'un secrétariat, qui comprend environ soixante personnes, dont les sections « Études, recherches et enquêtes » et « *Front-desk* » mentionnées ci-avant.

La CPVP rend des avis au gouvernement qui-c'est un impératif européen- doit la saisir lorsqu'un projet de loi ou de réglementation quelconque met en jeu un traitement de données à caractère personnel. Tel est le cas par exemple des traitements de données en matière sociale (Banque-carrefour de la sécurité sociale), en matière de soins de santé, de données policières, de données judiciaires, etc.

La CPVP, comme le Conseil d'État, est également un organe de conseil des parlements, qui peuvent la saisir d'une demande d'avis.

Elle rend en outre des avis d'initiative sur des problèmes qu'elle identifie ou des sollicitations qui lui sont faites par des demandeurs autres que des institutions.

La CPVP a aussi un pouvoir de recommandation, plus spécifique que son pouvoir d'avis, et qui consiste à recommander, sans force contraignante, à certains responsables de traitements de données à caractère personnel, d'adopter des attitudes plus conformes à la loi et plus respectueuses des droits et des intérêts des personnes concernées.

Ainsi, l'une des dernières recommandations de la Commission a été adressée, en matière de télébillétique, à la STIB et aux autres sociétés de transport, pour leur demander de conformer leur système d'achat et de paiement de titres de transport à des normes de protection suffisantes pour éviter par exemple que ceux qui utilisent des cartes de type « Mobib » ne puissent être pistés dans tous leurs déplacements.

À côté de ces pouvoirs d'avis et de recommandation, la CPVP a également une mission légale parajuridictionnelle, qui consiste à traiter les plaintes dont elle est saisie en matière de traitements de données à caractère personnel. La CPVP intervient d'abord dans une perspective de médiation. Si celle-ci n'aboutit pas, elle se prononce sur le caractère fondé de la plainte. Elle ne tranche donc pas le litige en octroyant une réparation du dommage identifié. Celui qui bénéficie d'une telle décision dispose, par rapport à son adversaire, d'une « longueur d'avance » devant les tribunaux quand il s'agit d'une demande en réparation d'un dommage.

Enfin, les membres de la CPVP disposent d'un pouvoir d'enquête assez approfondi, puisqu'ils sont tous, dans leur mission, officiers de police judiciaire auxiliaires du procureur du Roi. Ils bénéficient, de par l'effet de la loi, d'un pouvoir de perquisition étendu

sus genomen en zijn het resultaat van soms lange debatten.

De leden worden bijgestaan door een secretariaat, dat uit ongeveer 60 personen bestaat, waaronder de reeds vermelde afdelingen « Studie en onderzoek » en « *Frontdesk* ».

De CBPL geeft adviezen aan de regering, die — dat is een Europese verplichting — dat advies moet vragen wanneer bij een wetsontwerp of enig ontwerp van regelgeving verwerking van persoonsgegevens betrokken is. Dat geldt bijvoorbeeld voor de verwerking van gegevens op sociaal gebied (Kruispuntbank van de sociale zekerheid), inzake gezondheidszorg, politiegegevens, gerechtelijke gegevens, enz.

De CBPL is, zoals de Raad van State, tevens een raadgevend orgaan voor de parlementen, die haar om een advies kunnen vragen.

Tevens geeft ze op eigen initiatief adviezen over problemen die ze waarneemt, of op verzoek van verzoekers die geen instellingen zijn.

De CBPL heeft tevens een bevoegdheid van aanbeveling, die specifieker is dan haar adviserende bevoegdheid en die erin bestaat zonder bindende kracht bepaalde leidinggevenden inzake de verwerking van persoonsgegevens aan te bevelen zich beter te schikken naar de wet en de rechten en belangen van de betrokkenen meer te eerbiedigen.

Een van de laatste aanbevelingen van de Commissie werd aan de MIVB en aan de andere vervoersmaatschappijen gericht en ging over teleticketing, om hun te vragen hun systeem voor de aankoop en de betaling van vervoerbewijzen te doen beantwoorden aan toereikende beschermingsnormen, om te voorkomen dat wie kaarten van het « Mobib »-type gebruikt bij al zijn verplaatsingen kan worden gevolgd.

Naast die bevoegdheden inzake adviezen en aanbevelingen, heeft de CBPL tevens een wettelijke parajurisdictionele opdracht, die erin bestaat de klachten te behandelen inzake de verwerking van persoonsgegevens die bij haar aanhangig worden gemaakt. De CBPL treedt eerst op met het vooruitzicht te bemiddelen. Indien dat niet lukt, spreekt ze zich uit over de gegrondheid van de klacht. Ze beslecht het geschil dus niet door het herstel van de geïdentificeerde schade op te leggen. Wie een dergelijke beslissing in zijn voordeel heeft, heeft voor de rechtbanken « een lengte voorsprong » op zijn tegenstrever wanneer het om een vordering tot schadevergoeding gaat.

Tot slot beschikken de leden van de CBPL over een vrije diepgaande onderzoeksbevoegdheid, aangezien ze in hun opdracht officieren van gerechtelijke politie zijn, die de procureur des Konings bijstaan. Op grond van de wet hebben ze een uitgebreide huiszoekings-

dans tous les lieux où des données à caractère personnel sont traitées, principalement sous forme de fichiers via des outils informatiques.

Des comités sectoriels sont associés à la CPVP et sont chargés de délivrer des autorisations pour tous les flux de données émanant des services publics fédéraux, comme par exemple le comité sectoriel « sécurité sociale » pour les flux de données émanant de toutes les instances de la sécurité sociale. Il existe également un comité sectoriel pour le registre national et un comité sectoriel « autorités fédérales » (supplétif pour les cas où il n'existe pas de comité sectoriel spécialisé). Un comité « Statistiques » dont les fonctions sont actuellement exercées par la Commission, sera aussi installé sous peu. Il donnera toutes les autorisations pour les flux de données émanant de la direction générale « Statistiques » (ex-INS), et pour toutes les données de celle-ci exploitées par des tiers.

Au-delà de son activité d'avis et de recommandation, la CPVP exerce donc aussi une activité de contrôle et d'autorisation, pour tous les flux de données émanant des services publics.

M. Verschueren indique également que la Communauté et la Région flamande ont créé ensemble un « Toezichtscomité », similaire aux comités sectoriels fédéraux susmentionnés, et qui contrôlera désormais tous les flux de données partant de et arrivant vers les administrations contrôlées par la Région et la Communauté flamande. Ce type de contrôle n'existe ni en Région wallonne, ni en Communauté française, ni en Région bruxelloise. C'est là un type de contrôle que la Commission appelle de ses vœux, car l'efficacité d'une telle régulation au niveau fédéral a été constatée.

La CPVP agit au niveau national, mais aussi au niveau international. Elle est, comme tous ses homologues européens, membre du « Groupe de l'article 29 », créé par l'article 29 de la directive 95/46 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Ce groupe se réunit tous les mois. Il se constitue aussi en sous-groupes qui traitent de matières spécialisées, afin de coordonner les politiques dans tous les États membres. Ainsi, un sous-groupe se consacre au problème du contrôle des données aux frontières, un autre aux données en matière financière, un autre encore aux moteurs de recherche ou au direct marketing. La CPVP s'efforce de prendre des décisions qui soient les plus similaires possibles, dans l'application des lois et des principes de la directive, pour éviter ce que l'on a connu voici quelques années, à savoir une sorte de forum shopping de la part de grandes sociétés qui délocalisent parfois leur siège social ou leur lieu de traitement de bases de données, afin de bénéficier d'une législation plus favorable.

bevoegdheid op alle plaatsen waar persoonsgegevens worden verwerkt, hoofdzakelijk in de vorm van bestanden en met informaticatools.

De CBPL beschikt over sectorale comités, die belast zijn met het afgeven van machtigingen voor alle datastromen afkomstig van de federale overheidsdiensten, zoals het sectoraal comité « sociale zekerheid » voor de datastromen afkomstig van alle instanties van de sociale zekerheid. Er bestaat ook een sectoraal comité van het rijksregister en een sectoraal comité « federale overheid » (dat aanvullend is voor het geval waarin er geen gespecialiseerd sectoraal comité bestaat). Binnenkort wordt een comité « Statistiek » geïnstalleerd, waarvan de functies nu door de Commissie worden uitgeoefend. Het zal de machtigingen afgeven voor de datastromen afkomstig van de algemene directie « Statistiek »(ex-NIS), en voor al haar data die door derden worden gebruikt.

Naast haar activiteit inzake adviezen en aanbevelingen, oefent de CBPL dus ook een controle- en machtigingsactiviteit uit voor alle datastromen afkomstig van de overheidsdiensten.

De heer Verschueren verklaart ook dat de Vlaamse Gemeenschap en het Vlaamse Gewest samen een « Toezichtscomité » hebben opgericht, dat vergelijkbaar is met de reeds vermelde sectorale comités en dat voortaan alle datastromen van en naar de door het Vlaamse Gewest en de Vlaamse Gemeenschap gecontroleerde administraties controleert. Dergelijke controle bestaat noch in de Franse Gemeenschap, noch in het Brusselse Gewest. Het is een vorm van controle die zeer gewenst is door de Commissie, want de efficiëntie ervan werd op het federale niveau vastgesteld.

De CBPL handelt op nationaal niveau, maar ook op internationaal niveau. Ze is, zoals al haar Europese soortgenoten, lid van de « Groep artikel 29 », opgericht bij artikel 29 van richtlijn 95/46 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens. Die groep vergadert elke maand. Hij bevat ook subgroepen die gespecialiseerde thema's behandelen, om het beleid in alle lidstaten te coördineren. Zo wijdt een subgroep zich aan het probleem van de datacontrole aan de grenzen, een andere aan de financiële data, nog een andere aan zoekmachines of aan direct marketing. De CBPL spant zich in om beslissingen te nemen die zoveel mogelijk vergelijkbaar zijn, met toepassing van de wetten en de beginselen van de richtlijn, om te voorkomen wat men enkele jaren geleden heeft meegemaakt, te weten een soort forumshopping voor grote ondernemingen, die hun maatschappelijke zetel of de plaats van hun databases verplaatsen, om onder de gunstigste wetgeving te vallen.

Cette instance internationale est doublée d'autres instances. Ainsi, il y a, pour les DPA (*data protection authorities*), la *Spring Conference*, conférence européenne qui associe, au-delà des membres de l'Union européenne, tous les États de la zone Europe (Islande, Turquie, Norvège, Pays baltes non membres de l'Union européenne, certains pays du Proche Orient ...). Le principe est, ici aussi, celui de la coordination des politiques et des dossiers. En effet, certains dossiers, comme des dossiers liés à la société Google, sont traités idéalement de manière similaire dans différents États.

Enfin, il existe depuis 30 ans, au niveau international, une instance importante, appelée la « Conférence internationale des autorités de protection des données ». En effet, des instances comme la CPVP n'existent pas seulement en Europe, mais aussi dans beaucoup d'autres pays du monde : au Canada, aux États-Unis (uniquement pour les données gérées par les administrations publiques), dans tous les pays du Sud-Est asiatique, en Australie, etc.

Une fois par an, une réunion est organisée entre tous les membres de cette conférence internationale; les relations étant suivies en cours d'année par celui qui la préside.

Ces concertations internationales font dire à la commission belge, mais aussi à ses homologues du monde entier, qu'il est aujourd'hui plus que jamais nécessaire de tenter de mettre sur pied un instrument juridique international pour réguler et encadrer le traitement des données à caractère personnel.

Il existe un instrument juridique au niveau européen, mais il s'agit d'une directive qui doit être mise en œuvre dans chaque État membre. Il se fait par ailleurs que le contrôle de la mise en œuvre de cette directive relève encore d'autorités nationales, alors que certains dossiers sont internationaux.

La coopération que la commission belge a avec ses homologues se limite à ses compétences. Il n'existe pas encore de réelle compétence judiciaire ou policière permettant d'encadrer le traitement de données.

Au-delà des régulations régionales comme celle opérée par la directive européenne 95/46, il y a très certainement la nécessité d'une régulation internationale à plus grande échelle, qui permette d'appréhender de manière beaucoup plus sereine et saine des dossiers relatifs à des traitements de données réalisés simultanément à plusieurs endroits du monde et sous le régime de législations très différentes. Ainsi, Google stocke ses données en Californie. Ses privacy policies, qui sont sur Internet, prévoient que les tribunaux d'élection sont ceux du Maine. Les ponctions de données se font en Belgique. Elles sont envoyées dans le sud-est asiatique, où elles sont agrégées avec

Naast die internationale instantie zijn er nog andere. Wat de DPA (*data protection authorities*) betreft is er nog de Spring Conference, een Europese conferentie met naast de lidstaten van de Europese Unie alle staten van de Europese zone (IJsland, Turkije, Noorwegen, Baltische staten die geen lid zijn van de Europese Unie, bepaalde landen van het Nabije Oosten ...). Ook hier geldt het beginsel van de coördinatie van het beleid en van de dossiers. Bepaalde dossiers, zoals die in verband met de onderneming Google, worden idealiter immers op vergelijkbare wijze in de diverse staten behandeld.

Tot slot bestaat er op internationaal niveau al 30 jaar een belangrijke instantie, « Internationale Conferentie van de commissarissen voor de bescherming van gegevens en de privacy ». Instanties zoals de CBPL bestaan immers niet alleen in Europa, maar ook in tal van andere landen in de wereld : in Canada, in de Verenigde Staten (alleen voor de data die door de overheidsadministraties worden beheerd), in alle landen van Zuidoost-Azië, in Australië, enz.

Eenmaal per jaar wordt er een vergadering van alle leden van die internationale conferentie georganiseerd, waarbij de betrekkingen in de loop van het jaar worden verzekerd door het lid dat het voorzitterschap bekleedt.

Uit dat internationaal overleg leidt de Belgische commissie, maar ook haar tegenhangers in de hele wereld, af dat het vandaag meer dan ooit noodzakelijk is dat er gepoogd wordt een internationaal juridisch instrument tot stand te brengen om de verwerking van persoonsgegevens te regelen.

Er bestaat een juridisch instrument op Europees niveau, maar het gaat om een richtlijn die in elke lidstaat ten uitvoer moet worden gelegd. Daarbij komt nog dat de controle op de tenuitvoerlegging van die richtlijn nog de bevoegdheid is van nationale autoriteiten, terwijl sommige dossiers internationaal zijn.

De samenwerking van de Belgische commissie met haar tegenhangers beperkt zich tot haar bevoegdheden. Er bestaat nog geen echte juridische of politionele bevoegdheid waardoor de dataverwerking geregeld kan worden.

Naast de regionale regelingen zoals die van de Europese richtlijn 95/46, is er zeker de noodzaak van een internationale regeling op grotere schaal, waardoor dossiers in verband met dataverwerking die simultaan op verscheidene plaatsen op de wereld gebeurt onder zeer verschillende wetgevingen, veel serener en gezonder kunnen worden aangepakt. Google bijvoorbeeld slaat zijn data in Californië op. Zijn privacy policies, die op internet staan, bepalen dat de gekozen rechtbanken die van Maine zijn. De data worden in België opgenomen. Ze worden naar Zuidoost-Azië verzonden, waar ze worden samengevoegd met andere data, waarna ze naar een andere plaats

d'autres données, après quoi elles sont envoyées ailleurs. Les flux de données sont donc considérables, et voyagent très rapidement. Le cadre juridique qui leur est applicable varie donc de seconde en seconde.

Avec ses homologues internationaux, la Commission a adopté, lors de la réunion de Madrid, des standards internationaux (« *soft law* »). Il s'agit de la manière commune dont ceux-ci entendent encadrer les traitements de données. C'est un « *gentlemen agreement* », un accord de coopération à bas niveau entre les autorités de protection de données, qui ne lie pas les États dans lesquels les données se traitent, mais qui constitue, aux yeux de l'orateur, un bon exemple de ce que pourrait être demain une convention internationale sur la protection des données. Les principes qui y sont repris sont calqués sur ceux de la directive européenne.

Au cours d'une assez longue négociation, on a pu faire admettre aux Américains et aux Canadiens que les principes de la directive européenne ne devaient pas susciter leur méfiance et pouvaient être partagés.

En vue de l'adoption d'un tel instrument international, chacun s'est donné pour mission de sensibiliser son gouvernement et ses autorités nationales à l'importance de prendre une initiative en la matière et d'engager un processus de négociation susceptible de conduire à l'adoption de cet instrument.

L'orateur communique également aux membres un codex à la rédaction duquel la Commission a participé, et qui est un recueil de l'ensemble de la législation belge et européenne relative à la protection des données à caractère personnel. On y trouve la loi de base du 8 décembre 1992 sur le traitement des données à caractère personnel, mais aussi toute la législation existante en matière sociale à partir du développement de la Banque-Carrefour, en matière de santé à partir du développement de la plate-forme e-health, en matière de sécurité (*cf.* lois sur la fonction de police et sur les services de police et loi sur les caméras).

Ces dispositifs sont nombreux, et forment un ensemble assez complet, qui permet aujourd'hui au niveau national, sous réserve de l'évolution des techniques, de maîtriser les enjeux qui se développent sur notre territoire.

**Dossiers spécifiques**

L'orateur souhaite ensuite évoquer une série de dossiers qui préoccupent la CPVP, et sur lesquels l'intervention du législateur serait à son avis opportune, pour l'adoption, sinon d'une norme, à tout le moins d'une résolution, et pour évaluer de manière

worden gezonden. De datastromen zijn dus aanzienlijk en ze verplaatsen zich zeer snel. Het juridisch kader waaronder ze vallen verandert dus van seconde tot seconde.

De Commissie heeft op de vergadering van Madrid met haar internationale tegenhangers internationale standaarden (« *soft law* ») goedgekeurd. Het gaat om de gemeenschappelijke wijze waarop zij de dataverwerking willen omkaderen. Het is een « *gentlemen's agreement* », een samenwerkingsakkoord op laag niveau tussen de autoriteiten voor databescherming, die de staten waarin de data worden verwerkt niet bindt, maar die volgens spreker een goed voorbeeld zijn van wat morgen een internationaal verdrag betreffende databescherming kan zijn. De beginselen die erin zijn opgenomen zijn een doorslag van die van de Europese richtlijn.

In vrij lange onderhandelingen heeft men de Amerikanen en de Canadezen ervan kunnen overtuigen dat ze de beginselen van de Europese richtlijn niet moesten wantrouwen en dat ze die konden delen.

Met het oog op de goedkeuring van een dergelijk internationaal instrument heeft iedereen zich ertoe verbonden zijn regering en zijn nationale autoriteiten ervan bewust te maken dat het belangrijk is een initiatief terzake te nemen en een onderhandelingsproces aan te vatten dat tot het goedkeuren van dat instrument kan leiden.

Spreker overhandigt de leden ook een codex waaraan de Commissie heeft meegewerkt. Het is een overzicht van alle Belgische en Europese wetten in verband met de bescherming van persoonsgegevens. Men vindt er de basiswet van 8 december 1992 ten opzichte van de verwerking van persoonsgegevens, maar ook de hele bestaande wetgeving op sociaal gebied rond de ontwikkeling van de Kruispuntbank, op gezondheidsgebied rond de ontwikkeling van het *e-health platform*, op veiligheidsgebied (*cf.* wetten op het politieambt en op de politiediensten en camerawet).

Die teksten zijn talrijk en vormen een vrij volledig geheel, waardoor men vandaag de uitdagingen die op ons grondgebied ontstaan op nationaal niveau kan bevatten, onder voorbehoud van de verandering van de technieken.

**Specifieke dossiers**

Spreker wenst vervolgens een reeks dossiers aan te halen die de CBPL zorgen baren en waarvoor de tussenkomst van de wetgever volgens hem opportuun zou zijn teneinde een norm of een resolutie goed te keuren en teneinde de evolutie van het dossier en de

approfondie l'évolution du dossier et la possibilité de préciser des normes d'encadrement.

M. Verschueren a d'ailleurs relevé, dans la note d'intentions qui a présidé à la création du présent groupe de travail, des similitudes dans les préoccupations exprimées.

*— Droit à l'oubli et effacement d'informations*

Préalablement, l'orateur souhaite forumer quelques remarques sur le développement des médias, de la presse, et des enjeux que cela pose en matière de traitement de données à caractère personnel.

Aujourd'hui, les médias ne sont plus seulement diffusés sur support papier ni sur support audiovisuel classique (télévision, radio). Ils se développent fortement sur les réseaux internet. Tous les journaux ont d'ailleurs un site en ligne et sont consultés sur Internet. Il en va de même pour les radios et les télévisions. Par ailleurs, tout ce qui constitue les archives de la presse ne se trouve plus aujourd'hui stocké sous forme d'exemplaires reliés dans des caves, mais est numérisé et informatisé, et accessible en ligne très rapidement. Contrairement à l'exemplaire papier disponible en librairie, la consultation de la version électronique des journaux sur Internet est « gratuite ». Or, la gratuité totale n'existe pas. Les journalistes travaillent et doivent être payés. Il en va de même des informaticiens qui créent les supports informatiques, des auteurs et des photographes.

Dès lors, la gratuité de l'accès aux médias en ligne ne doit pas manquer d'étonner, et de soulever la question de savoir qui paie le travail effectué, et comment.

Quels sont les problèmes auxquels la CPVP est le plus souvent confrontée, au travers des plaintes qui lui sont adressées ?

Il arrive par exemple qu'une personne se plaigne de ce qu'un fait la concernant a été relaté dans la presse quelques années ou quelques mois auparavant, et qu'une recherche sur son nom, effectuée aujourd'hui sur Internet au travers d'un moteur de recherche, fait apparaître en premier lieu les articles qui relataient ce fait. Ceci s'explique par le fait que ces articles ont peut-être été diffusés dans la presse écrite ou dans un reportage télévisé, mais quasiment toujours à travers le site informatique du journal ou du support média. En outre, même l'article publié sur support papier a été archivé dans les archives de ce support média et est consultable en ligne. Plus un article est consulté, plus il figure parmi les premiers résultats d'une recherche.

Les personnes se plaignent également de ce que les faits sont rappelés comme s'ils se sont déroulés la

mogelijkheid om begeleidingsnormen uit te werken, grondig te evalueren.

De heer Verschueren heeft er trouwens in de intentienota die aan de oprichting van deze werkgroep ten grondslag ligt, op gewezen dat er sprake is van gelijklopende bezorgdheden.

*— Recht op het vergeten en wissen van informatie*

Spreker wil vooraf enkele opmerkingen maken rond de ontwikkeling van de media, de pers en de uitdagingen hiervan met betrekking tot persoonsgegevens.

Tegenwoordig worden de media niet enkel verspreid op papier of op een klassieke audiovisuele drager (televisie, radio). Ze ontwikkelen zich sterk via het internet. Alle kranten hebben trouwens een website en worden op het internet geraadpleegd. Hetzelfde geldt voor radio en televisie. Bovendien worden de persarchieven niet langer bewaard als gebonden exemplaren in kelders, maar worden ze gedigitaliseerd en geïnformatiseerd en zijn ze snel online toegankelijk. In tegenstelling tot het exemplaar in de krantenwinkel is de elektronische versie van de kranten op het internet « gratis ». Volledige kosteloosheid bestaat echter niet. De journalisten doen hun werk en moeten worden betaald. Hetzelfde geldt voor de informatici die de informaticamiddelen creëren, de auteurs en de fotografen.

De kosteloosheid van de toegang tot de onlinemedia is dan ook verbazingwekkend en roept vragen op over wie het geleverde werk betaalt en hoe.

Met wat voor problemen wordt de CBPL het vaakst geconfronteerd via de klachten die aan haar worden gericht ?

Het gebeurt bijvoorbeeld dat iemand erover klaagt dat een feit dat hem of haar betreft enkele jaren of maanden daarvoor in de pers is vermeld en dat een opzoeking van zijn of haar naam via een zoekmachine op het internet op dit moment in de eerste plaats de artikelen weergeeft die over dat bewuste feit gaan. Dit valt te verklaren door het feit dat deze artikelen misschien zijn verspreid via de geschreven pers of in een televisiereportage, maar quasi altijd via de website van de krant of de media. Bovendien is het artikel op papier opgeslagen in het archief van deze media en is het online raadpleegbaar. Hoe vaker een artikel wordt geraadpleegd, hoe meer het bovenaan in de lijst van zoekresultaten belandt.

De personen in kwestie klagen er tevens over dat de feiten in herinnering worden gebracht alsof ze de dag

veille, ce qui nuit à leur carrière professionnelle et leur vie privée.

L'orateur cite les exemples suivants.

Il y a quelques années, le responsable d'une grande société européenne de parfums a été arrêté à Tokyo pour des faits délictueux de consommation de drogue. Ces faits sont relatés dans les journaux européens. Cette personne veut aujourd'hui reprendre une carrière internationale et défendre une certaine notoriété, mais dès que l'on fait une recherche à son sujet sur Internet, on aboutit aux articles relatant ses anciens déboires. La personne en question demande donc aux journaux, à travers la CPVP, et en exerçant des droits que la loi prévoit (droit d'opposition aux données personnelles), que cette information soit effacée, au nom de ce qu'elle estime être un droit à l'oubli. Les faits étant archivés, la personne estime qu'ils ne doivent plus être accessibles avec la même vigueur ou facilité que par le passé.

Un autre exemple est celui de l'affaire Riga, qui s'est déroulée dans le Brabant wallon. M. Riga avait tué à coups de carabine deux jeunes qui s'étaient introduits dans sa propriété privée. Après trois jours de détention préventive, il avait été relâché. Cela avait causé un certain émoi dans la presse, parce qu'il s'agissait d'un notable, et qu'il aurait ainsi bénéficié d'un traitement privilégié. Ce fait divers avait été fort médiatisé. Aujourd'hui, l'ex-femme de M. Riga, qui exerce une profession tout à fait honorable, demande que, lorsque l'on introduit son nom dans un moteur de recherche, toutes les informations qui la lient à son ancien mari, et qui apparaissent massivement et par priorité, soient effacées.

Une autre affaire du même ordre, mais qui présente un aspect plus délicat, est celle d'un ex-militant du Front National, qui s'adresse à la Commission pour demander, de la même manière, que l'on ne puisse plus avoir accès à tous les articles publiés à son propos et qui le dénoncent comme militant de cette organisation, ayant des sympathies nazies avérées. Il justifie sa demande par le fait qu'il a aujourd'hui changé, mais se trouve dans l'impossibilité de trouver du travail ou de faire une quelconque démarche sans que ces données relatives à son passé n'apparaissent. Il s'est avéré ensuite, après une enquête approfondie de l'un des sites Internet auxquels on demandait d'effacer les données, que l'affirmation de cette personne selon laquelle elle avait quitté les milieux d'extrême-droite était fausse et qu'elle y était toujours très active.

Ces exemples montrent que la question du droit à l'oubli et à l'effacement de certaines informations n'est pas simple, et doit être traitée au cas par cas.

L'orateur cite encore l'exemple d'un responsable néerlandophone de la FGTB métallo de Liège qui,

voordien zijn gebeurd, hetgeen schade berokkent aan hun carrière en hun privéleven.

Spreker haalt de volgende voorbeelden aan.

Enkele jaren geleden werd de verantwoordelijke van een groot Europees parfumbedrijf aangehouden in Tokio wegens strafbare feiten die te maken hadden met drugsgebruik. Deze feiten hebben in de Europese kranten gestaan. De betrokkene wil nu opnieuw internationaal carrière maken en een bepaalde reputatie verdedigen, maar zodra men zijn naam op het internet opzoekt, treft men de artikelen over zijn vroegere tegenslagen aan. De persoon in kwestie vraagt bijgevolg via de CBPL aan de kranten om, op grond van de rechten waarin de wet voorziet (recht op verzet tegen persoonsgegevens), deze gegevens te wissen uit naam van wat volgens hem een recht is namelijk het recht om te worden vergeten. Aangezien de feiten gearchiveerd zijn, meent de persoon dat ze niet langer even makkelijk toegankelijk moeten zijn als in het verleden.

Een ander voorbeeld is dat van de zaak Riga die zich in Waals-Brabant heeft afgespeeld. De heer Riga had met een karabijn twee jongeren gedood die zijn privé-eigendom waren binnengegaan. Na drie dagen voorlopige hechtenis werd hij vrijgelaten. Dit zorgde voor opschudding in de pers omdat het om een notabele ging en hij daardoor een voorkeursbehandeling zou hebben genoten. Dit *fait divers* werd sterk gemediatiseerd. Vandaag vraagt de ex-vrouw van de heer Riga, die een eervol beroep uitoefent, dat van alle informatie over haar op het internet de informatie die massaal als eerste uit de zoekmachines komt en die haar in verband brengt met haar ex-man, zou worden gewist.

Een andere zaak in dezelfde zin maar dan delicater is die van een ex-militant van het Front National, die zich eveneens tot de Commissie richt om te vragen niet langer toegang te verlenen tot alle artikelen die over hem zijn gepubliceerd en waarin hij genoemd wordt als militant van deze organisatie, waarvan bewezen is dat ze nazisympathieën heeft. Hij verantwoordt zijn verzoek met het argument dat hij tegenwoordig veranderd is, maar onmogelijk werk kan vinden of om het even wat kan ondernemen zonder dat deze gegevens over zijn verleden opduiken. Vervolgens is na een grondig onderzoek van een van de websites waaraan men vroeg om de gegevens te wissen, gebleken dat de bewering dat deze persoon het extreemrechtse milieu had verlaten, onjuist was en dat die persoon daar nog steeds zeer actief was.

Deze voorbeelden tonen aan dat de kwestie van het recht op het vergeten en wissen van bepaalde informatie niet eenvoudig is, en geval per geval moet worden bekeken.

Spreker haalt nog het voorbeeld aan van een Nederlandstalige verantwoordelijke van ABVV Me-

voici plus de trente ans, était militant d'une association d'extrême-droite néerlandophone. Cette information a été révélée à partir d'une recherche sur Internet. Cette situation a posé des problèmes dans le cadre de son organisation politique, dont il a fini par être exclu, de manière « préventive » selon ceux qui ont procédé à cette exclusion. L'intéressé revendiquait pour sa part le droit à avoir des opinions et à pouvoir en changer sans devoir traîner son passé durant toute sa vie.

Enfin, l'orateur cite le cas du ministre Folien, ministre des Finances PSC avant la guerre, qui avait fait des déclarations contre les juifs dans une série de cénacles publics. Un journaliste néerlandophone a voulu faire une longue enquête pour démontrer qu'il était faux de prétendre que c'était toujours du côté néerlandophone que la collaboration avait eu lieu, et que du côté francophone, on trouvait aussi des collaborateurs et des déclarations suspectes. Une fois cet article paru, la fille de M. Folien a saisi la Commission, invoquant le droit à l'oubli.

Tous ces exemples partent de la même situation, à savoir une publication dans un journal, et la capacité qu'offre aujourd'hui l'Internet d'accéder, avec une extraordinaire facilité, à des faits et informations très anciens.

La CPVP a eu des contacts avec des organes de presse, pour examiner avec eux comment résoudre ces problèmes, partant de l'idée qu'il fallait, à un moment donné, pouvoir pondérer l'accès à certaines informations; les réalités d'hier n'étant pas celles d'aujourd'hui.

La première réponse, tout à fait légitime, des organes de presse, était qu'ils ne pouvaient pas « tricher » avec l'histoire et qu'ayant publié ces informations, ils n'allaient pas maintenant les effacer. Lorsque les informations étaient publiées sur support papier, elles étaient archivées et plus difficilement accessibles mais les journaux n'étaient pas détruits. Or, transmettre une information, c'est également transmettre un état de fait sur ce qui a été fait et dit. Les organes de presse ont donc refusé de porter atteinte aux informations en question, et ont souhaité les maintenir dans l'état où elles ont été publiées.

Par contre, au cours de cette discussion, des pistes sont apparues, qui font actuellement l'objet d'une réflexion. Ces pistes concernent tout d'abord le droit de réponse. Les législations en la matière doivent être complètement adaptées à ce que sont devenues aujourd'hui la presse et la diffusion d'informations.

Les journaux semblaient ouverts à cette possibilité, et notamment à la création d'un système de droit de réponse sur les supports informatiques, appelant

taal Luik die meer dan dertig jaar geleden militant was binnen een Nederlandstalige extreemrechtse vereniging. Deze informatie werd aan het licht gebracht op grond van een zoektocht op het internet. Deze situatie heeft tot problemen geleid in het kader van zijn politieke organisatie, waar hij uiteindelijk werd uitgesloten, zij het « preventief » volgens diegenen die tot deze uitsluiting zijn overgegaan. De betrokkene eiste van zijn kant het recht op om een mening te hebben en van mening te mogen veranderen zonder zijn verleden zijn hele leven lang met zich te moeten meeslepen.

Tot slot noemt spreker het geval van minister Pholien, PSC-minister van Financiën vóór de oorlog, die zich in het openbaar herhaaldelijk tegen de joden had uitgelaten. Een Nederlandstalige journalist heeft een langdurig onderzoek willen voeren om aan te tonen dat het verkeerd was te beweren dat er altijd aan Nederlandstalige kant werd gecollaboreerd, maar dat men ook aan Franstalige kant collaborateurs en verdachte uitlatingen vond. Zodra dit artikel is verschenen, is de dochter van de heer Pholien naar de Commissie gestapt om gebruik te maken van het recht om te worden vergeten.

Al deze voorbeelden gaan uit van dezelfde situatie, namelijk een publicatie in een krant en de mogelijkheid die het internet tegenwoordig biedt om met een buitengewoon gemak toegang te krijgen tot feiten en informatie uit een ver verleden.

De CBPL heeft contact gehad met persorganen om samen met hen na te gaan hoe deze problemen kunnen worden opgelost. Het idee waarvan men uitging was dat men op een bepaald moment de toegang tot bepaalde informatie moest kunnen wegen; de realiteit van vroeger is immers niet dezelfde als die van vandaag.

De eerste — overigens volstrekt legitieme — reactie van de persorganen is dat ze niet mochten « knoeien » met de geschiedenis. Aangezien zij deze informatie hebben gepubliceerd, gingen zij die nu niet zomaar wissen. Wanneer de informatie op papier is gepubliceerd, is ze gearchiveerd en moeilijker toegankelijk, maar de kranten zijn niet vernietigd. Informatie doorgeven is tevens een feitelijke stand meegeven van wat er gedaan en gezegd is. De persorganen hebben bijgevolg geweigerd om te raken aan de informatie in kwestie en wensen ze te behouden in de toestand waarin ze is gepubliceerd.

Tijdens deze bespreking zijn echter wel bepaalde opties geopperd waarover momenteel wordt nagedacht. Het gaat hierbij in de eerste plaats om het recht van antwoord. De wetgeving ter zake moet volledig worden aangepast aan wat de pers en de informatieverspreiding momenteel zijn geworden.

De kranten leken voor deze mogelijkheid open te staan, met name voor de invoering van een recht van antwoord met betrekking tot informaticamiddelen. Zo

directement, en même temps qu'un article, le droit de réponse, donnant ainsi aux personnes concernées (pas nécessairement de manière systématique, mais selon des règles à déterminer) la possibilité d'ajouter en ligne un commentaire à l'information qui les concerne.

Le second point concerne le fait que le problème ne se situe pas tant dans les archives des journaux, que dans la capacité qu'offrent les moteurs de recherche à accéder à ces archives.

Hier, on pouvait y accéder, et il est normal qu'on le puisse encore aujourd'hui.

Mais par le passé, il fallait une bonne raison d'accéder à une information. Il fallait un indice sur l'existence de l'information, sur le fait qu'elle se trouvait à un endroit précis, et l'on procédait par étapes successives pour arriver à ce que l'on cherchait.

Aujourd'hui, on trouve même ce que l'on ne cherche pas.

Une autre piste est donc de trouver une manière structurée qui empêche les moteurs de recherche d'indexer les archives de la presse, et qui ne permette d'accéder à ces archives que via les moteurs de recherche internes des journaux. La Commission a déjà obtenu ce résultat de la part de moteurs de recherche, principalement de Google, pour ce qui concerne les archives du Moniteur. Cela permet d'éviter certains problèmes, par exemple de discrimination à l'embauche.

Cette solution pourrait également être envisagée pour l'indexation des archives de la presse.

Le droit à l'oubli, qui a été évoqué de manière marginale dans les exemples précités, et qui est souvent invoqué, est un concept philosophique, et non juridique. On ne le trouve nulle part, sauf lorsqu'il est figé dans une norme comme, par exemple, les dispositions existant en matière de prescription. Il n'y a pas de droit général à l'oubli. Plutôt que de tenter de « théoriser » ce droit, il y a un intérêt à réfléchir à des cas particuliers, comme par exemple la situation que crée le développement numérique de la presse.

— *Le profilage*

L'orateur souhaite également aborder une question complexe, qui pourrait et devrait retenir l'attention du groupe de travail. Il s'agit du profilage. Il consiste, à partir d'une série d'informations relatives à une personne ou une catégorie de personnes, à constituer un sorte de portrait de celle-ci. Ce portrait n'est pas une photo, mais la personne y est très reconnaissable, car comportant des éléments très précis sur sa personne et

zou samen met het artikel het recht van antwoord ontstaan, waarbij de betrokken personen (niet noodzakelijk systematisch, maar volgens nader te bepalen regels) de mogelijkheid krijgen om online commentaar toe te voegen bij de informatie die op hen betrekking heeft.

Het tweede punt betreft het feit dat het probleem niet zozeer te maken heeft met de krantenarchieven, maar met de mogelijkheid van de zoekmachines om toegang te krijgen tot deze archieven.

Aangezien we er gisteren toegang toe hadden, vinden we het normaal dat we dat vandaag ook nog kunnen.

In het verleden had men echter een goede reden nodig om toegang te hebben tot informatie. Er was een aanwijzing nodig dat de informatie bestond, dat ze zich op een welbepaalde plek bevond en zo ging men stelselmatig verder tot men vond wat men zocht.

Vandaag vinden we zelfs dingen die we niet eens zochten.

Een andere optie is dus een gestructureerde manier zien te vinden om de zoekmachines te beletten om de persarchieven te indexeren, waardoor de toegang tot deze archieven enkel mogelijk is via de interne zoekmachines van de kranten. De Commissie heeft dit resultaat reeds bereikt bij de zoekmachines, voornamelijk Google, voor wat de archieven van het *Staatsblad* betreft. Hierdoor kunnen bepaalde problemen worden voorkomen, bijvoorbeeld discriminatie bij het solliciteren.

Men zou deze oplossing eveneens kunnen overwegen voor de indexering van de persarchieven.

Het recht om te worden vergeten, dat in de marge werd genoemd in de voorgaande voorbeelden en dat vaak wordt aangevoerd, is een filosofisch en niet-juridisch begrip. Een begrip dat men nergens terugvindt, behalve in een norm zoals bijvoorbeeld de bestaande bepalingen inzake verjaring. Er bestaat geen algemeen recht om te worden vergeten. In plaats van over dit recht te « theoretiseren », is het belangrijk om na te denken over specifieke gevallen, zoals bijvoorbeeld de situatie die wordt gecreëerd door de digitale ontwikkeling van de pers.

— *Profilering*

Spreker wenst ook een andere complexe kwestie aan te kaarten waarnaar de aandacht van de werkgroep zou kunnen en moeten uitgaan. Het gaat hier om profilering. Profilering gaat erom dat men op basis van een reeks inlichtingen over een persoon of een categorie van personen een soort portret van deze persoon of categorie van personen gaat maken. Dit portret is geen foto, maar de persoon is er wel zeer

son identité. Le profilage permet aujourd'hui d'arriver à dresser des portraits comme celui-là, à propos de tout le monde et à partir d'instruments très divers, qui peuvent être utilisés à des fins commerciales mais aussi politiques, policières ou judiciaires. Elles sont donc parfois légitimes, parfois moins.

L'orateur évoque tout d'abord le profilage à partir d'Internet et des moteurs de recherche.

M. Verschueren précise que si on a l'impression, lorsqu'on se rend sur Internet, d'ouvrir une fenêtre sur le « Monde » à travers son ordinateur, on ne se rend pas compte que, du même coup, le « Monde » entre très largement chez vous.

Lorsque l'on introduit un mot dans un moteur de recherche, celui-ci conserve la requête. Il la date, identifie l'endroit d'où elle vient à travers l'adresse IP, d'autres petits logiciels « espions » sur l'ordinateur (*cookies*), certaines puces de l'ordinateur, parfois l'adresse Mac ...

Lorsqu'un résultat est donné à la requête, l'intervenante est envoyé vers des pages de résultats à partir de la page du moteur de recherche. Ce dernier suit donc le déplacement.

Le moteur de recherche « *logge* » ces informations et, il y a deux ans, les gardait pendant dix-huit mois environ. Le fait de garder ces informations jour par jour pendant dix-huit mois permet, grâce à un calcul de probabilités et d'algorithmes très complexes, de détailler petit à petit un profil très précis de la personne.

Au bout de dix-huit mois, Google peut déterminer si vous êtes un homme ou une femme, votre âge, vos préoccupations principales, votre état de santé ou le type d'affection dont vous souffrez.

Actuellement, les données ne sont conservées que durant une période de six mois. Toutefois, Google a perfectionné son algorithme de sorte qu'il ne lui est plus nécessaire de disposer de dix-huit mois pour établir un profil précis. Dans un délai plus restreint, le portrait dressé reste tout aussi précis, ce qui permet d'affirmer que Google en sait plus sur vous que vos proches et sans doute que vous-même.

Aujourd'hui, on fait quasiment tout avec son ordinateur. Si l'on a peut-être oublié ce que l'on a fait il y a six mois, Google, lui, ne l'a pas oublié. Au bout de six mois, les données sont effacées, mais le profil, lui, ne l'est pas; les données d'aujourd'hui consolident ce profil, et ainsi de suite...

Google fonctionne de manière assez simple. Il parvient même à déterminer des profils différents pour un même ordinateur, selon l'utilisateur.

herkenbaar in omdat het zeer nauwkeurige elementen bevat over de persoon en zijn of haar identiteit. Door profilering kan men tegenwoordig dergelijke portretten maken van iedereen en op basis van zeer diverse instrumenten die voor commerciële, maar ook politieke, politionele of gerechtelijke doeleinden kunnen worden gebruikt. Soms zijn ze dus legitiem en soms minder legitiem.

Spreker heeft het allereerst over profilering op basis van het internet en de zoekmachines.

De heer Verschueren wijst erop dat wie op het internet surft de indruk heeft een venster op de wereld te openen, maar zich er niet van bewust is dat hij tezelfdertijd de wereld ook massaal binnenlaat.

Wanneer men een woord invoert in een zoekmachine, bewaart die de zoekopdracht. De robot dateert de opdracht, identificeert waar ze vandaan komt via het IP-adres, andere « spionagesoftware » op de computer (cookies), bepaalde chips van de computer, soms het Mac-adres ...

Wanneer het resultaat van de zoekopdracht verschijnt, wordt de internetgebruiker doorverwezen naar de resultatenpagina's vanuit de pagina van de zoekmachine. Die volgt dus de verplaatsing.

De zoekmachine « logt » deze informatie en bewaarde ze twee jaar geleden gedurende ongeveer achttien maanden. Het feit dat deze informatie dag na dag wordt bewaard gedurende achttien maanden maakt het via kansberekeningen en zeer ingewikkelde algoritmen mogelijk om geleidelijk een zeer nauwkeurig profiel van iemand uit te werken.

Na achttien maanden kan Google uitmaken of u een man of een vrouw bent, wat uw leeftijd, uw voornaamste bezigheden en uw gezondheidstoestand zijn of aan welk soort aandoening u lijdt.

Tegenwoordig worden de gegevens slechts gedurende een periode van zes maanden bewaard. Google heeft zijn algoritme geperfectioneerd zodanig dat er geen achttien maanden meer nodig zijn om tot een nauwkeurig profiel te komen. Ook binnen een kortere termijn blijft het gemaakte portret even nauwkeurig, waardoor men kan stellen dat Google meer over ons weet dan onze naasten en wellicht meer dan wijzelf.

Tegenwoordig doen we bijna alles met de computer. Hoewel wij misschien vergeten zijn wat we zes maanden geleden hebben gedaan, is Google het niet vergeten. Na zes maanden worden de gegevens gewist, maar het profiel niet; de gegevens van vandaag versterken dit profiel, enzovoort.

Google werkt op een vrij eenvoudige manier. Het slaagt erin verschillende profielen te onderscheiden voor eenzelfde computer, naar gelang van de gebruiker.

L'exemple suivant est peut-être caricatural, mais il correspond parfois aux clichés sociaux.

Sur un même ordinateur vont se connecter plusieurs utilisateurs : un homme, une femme, et leur enfant.

Ce dernier va effectuer des consultations selon les préoccupations de son âge. La femme, qui ne travaille pas, va, dans le courant de l'après-midi, consulter un site « *monregime.com* ». L'homme se connectera après minuit et ira consulter le site « *infirmieresnues.com* ».

Ainsi, au bout de six mois d'utilisation constante, au travers des quantités énormes de recherches et de consultations qui sont faites, et de ce que le calcul de probabilités peut produire, on peut très facilement établir des profils.

La base du calcul de probabilités est simple. Imaginons qu'une personne disposant d'un GSM appelle tous les jours les trois mêmes personnes après le travail : son partenaire, sa mère, et son enfant.

Puis, réalisant qu'elle est « espionnée » au moyen de son GSM, elle décide de changer de GSM, de détruire la puce et de prendre une carte prépayée et un numéro anonyme. Ensuite, la personne va reprendre les mêmes habitudes téléphoniques. Il ne faudra pas ving-quatre heures à quelqu'un qui effectuerait des recherches pour savoir qu'il s'agit de la même personne.

Si l'on met côte à côte deux ordinateurs qui ont déjà été utilisés durant un certain temps, et que l'on procède à la même recherche sur Google, on obtiendra des résultats différents. Si la recherche est très générale, les résultats seront assez semblables. Si la recherche est plus précise, ils le seront un peu moins. En effet, le résultat est donné en fonction du profil, de ce que l'on suppose être l'intérêt de l'utilisateur.

Ainsi, dans l'exemple précité, l'homme, s'il recherche un jour des informations sur un service d'infirmières à domicile, recevra beaucoup d'informations sur des sites qui ne traitent pas nécessairement de ce sujet, alors que, s'il n'avait pas consulté régulièrement le site « infirmières nues.com », les résultats eussent été différents.

On imagine aisément ce que ce profilage peut donner s'il est manipulé à grande échelle.

Que faut-il entendre par là ?

L'orateur renvoie au livre récent d'Alain Strowel, intitulé « Quand Google défie le droit ». Il se réfère également à deux cas de jurisprudence américaine.

Het volgende voorbeeld kan misschien karikaturaal lijken, maar stemt soms overeen met de maatschappelijke clichés.

Op eenzelfde computer verbinden verschillende gebruikers zich met het internet : een man, en vrouw en hun kind.

Het kind doet opzoekingen volgens wat hem op zijn leeftijd bezighoudt. De vrouw, die niet gaat werken, consulteert in de namiddag een site over diëten. De man gaat na middernacht op het internet en bezoekt er een site waarop naakte verpleegsters te zien zijn.

Zo kan men na zes maanden ononderbroken gebruik via de enorme hoeveelheden opzoekingen en bezochte websites en de resultaten van de kansberekeningen zeer makkelijk profielen opstellen.

De basis van de kansberekening is simpel. Beelden we ons in dat iemand met een gsm elke dag na het werk dezelfde drie personen opbelt : zijn of haar partner, moeder en kind.

Wanneer de persoon vervolgens beseft dat hij of zij wordt « bespioneerd » via die gsm, besluit de persoon te veranderen van gsm, de sim-kaart te vernietigen en een prepaid-kaart en een anoniem nummer te nemen. Vervolgens neemt de betrokkene dezelfde telefoneergewoonten weer aan. Iemand die op onderzoek uitgaat, heeft geen 24 uur nodig om te weten dat het om dezelfde persoon gaat.

Indien men twee computers naast elkaar zet die al een tijdje worden gebruikt en men hiermee dezelfde zoekopdracht in Google uitvoert, krijgt men verschillende resultaten. Indien het over een zeer algemene opzoeking gaat, zullen de resultaten vrij vergelijkbaar zijn. Indien de opzoeking preciezer is, zal dat minder het geval zijn. Het resultaat wordt immers gegeven op basis van het profiel, van wat men veronderstelt dat het internet van de gebruiker is.

Wanneer de man uit het voorbeeld op een dag informatie zoekt over een dienst voor thuisverpleegkunde, zal hij op die manier veel informatie krijgen over sites die niet noodzakelijk over dat onderwerp gaan. Indien hij niet geregeld naar een website met naakte verpleegsters was gesurft, zouden de resultaten verschillend zijn geweest.

Men kan zich makkelijk voorstellen wat voor gevolgen deze profilering kan hebben indien ze op grote schaal wordt gemanipuleerd.

Wat moet men daaronder verstaan ?

Spreker verwijst naar het recente boek van Alain Strowel « *Quand Google défie le droit* ». Hij verwijst tevens naar twee gevallen van Amerikaanse rechtspraak.

Le premier concerne un patron d'entreprise qui présente ses produits sur un site. Lorsqu'il essaie, grâce aux moteurs de recherche, d'accéder lui-même à son site pour voir si sa promotion est assurée, il s'aperçoit que son site n'est jamais référencé. Il s'adresse à Google, qui lui explique qu'étant une société privée, ils ont accepté que son concurrent achète son nom et une série de profils correspondant aux personnes intéressées par ses produits. Ce concurrent a payé Google pour que, lorsque des personnes recherchent les produits en question ou font des recherches à partir de son nom, celui-ci n'apparaisse jamais. Ceci a donné lieu à un procès retentissant aux États-Unis. Le plaignant a perdu car Google a été considérée effectivement comme une société privée et l'enjeu purement commercial.

On en revient à l'observation déjà formulée par l'orateur, qui soulignait que la gratuité totale n'existe pas. On trouve ici un exemple de la manière dont cette prétendue gratuité est financée.

Un second cas de jurisprudence américaine est plus politique et donc beaucoup plus sensible.

Uns société produisant des moteurs de bateaux en Californie se voit critiquer par des militants défenseurs de l'environnement au motif que les moteurs qu'elle produit sont nocifs aux fonds marins, notamment pour les phoques de la baie de San Francisco.

Cette société a acheté chez Google le profil des personnes plutôt intéressées par ce type de matière, et donné pour instruction que, lorsque ces personnes font une recherche sur la société, ou sur les fonds marins, ou encore sur les produits que vend la société, les rapports critiques à l'égard de celle-ci figurent très loin dans le résultat de la recherche. Cela a également fait l'objet d'un procès, où les associations militantes plaignantes ont eu gain de cause, parce que l'on a considéré que la discrimination s'était faite sur un enjeu politique.

Ces deux exemples montrent ce qu'il est possible de réaliser à partir des profils générés par les sociétés comme Google.

Outre la question de la gratuité, déjà évoquée, l'orateur attire l'attention sur le fait que l'on peut certes craindre les pouvoirs publics, mais que, dans une société démocratique, ces pouvoirs sont contrôlés.

Google, au contraire, n'est pas un pouvoir public, mais une société commerciale. Comme toute personne morale, elle a une « vie », et est appelée à disparaître un jour, par le biais d'un rachat, d'une faillite, ou d'un autre événement. Son seul fonds de commerce est son extraordinaire stock d'informations sur les gens, dont

Het eerste betreft een bedrijfsleider die zijn producten op zijn site voorstelt. Wanneer hij met behulp van de zoekmachines probeert zelf toegang te krijgen tot zijn site om te zien of hij voldoende bekendheid krijgt, merkt hij dat zijn website nooit een verwijzing krijgt. Hij richt zich tot Google, dat hem uitlegt dat het als privéfirma ermee heeft ingestemd dat zijn concurrent zijn naam en een reeks profielen heeft gekocht die overeenstemmen met de personen die in zijn producten zijn geïnteresseerd. Deze concurrent heeft Google betaald om ervoor te zorgen dat wanneer mensen de producten in kwestie opzoeken of opzoekingen doen op basis van zijn naam, die naam nooit verschijnt. Dit heeft aanleiding gegeven tot een spraakmakend proces in de Verenigde Staten. De klager heeft de zaak verloren, want Google werd effectief als een privéfirma en de inzet als zuiver commercieel beschouwd.

We belanden opnieuw bij de opmerking die spreker reeds heeft gemaakt, namelijk dat volledige kosteloosheid niet bestaat. Hier vinden we een voorbeeld van de wijze waarop deze zogenaamde kosteloosheid wordt gefinancierd.

Een tweede geval van Amerikaanse rechtspraak is meer politiek getint en bijgevolg veel gevoeliger.

Een bedrijf dat bootmotoren maakt in Californië krijgt kritiek van milieuactivisten omdat zijn motoren schadelijk zouden zijn voor de zeebodem, met name voor de zeehonden in de Baai van San Francisco.

Dit bedrijf heeft bij Google het profiel gekocht van mensen die nogal geïnteresseerd zijn in deze aangelegenheid en de instructie gegeven om, wanneer deze personen een opzoeking doen over het bedrijf of over de zeebodem of over de producten die het bedrijf verkoopt, de kritische rapporten hierover zeer ver in het resultaat van de zoekopdracht te steken. Ook hierover is een proces gevoerd, waarbij de milieuverenigingen in het gelijk zijn gesteld, omdat men heeft geoordeeld dat de discriminatie gebeurd was op basis van een politieke kwestie.

Deze twee voorbeelden tonen wat men kan realiseren op basis van profielen die door bedrijven zoals Google worden gegenereerd.

Naast het reeds aangehaalde aspect kosteloosheid vestigt spreker de aandacht op het feit dat men natuurlijk bang kan zijn voor de overheid, maar dat in een democratische samenleving deze overheid wordt gecontroleerd.

Google daarentegen is geen overheid, maar een handelsvennootschap. Zoals elke rechtspersoon heeft Google een « leven » en zal op een dag bijgevolg ook verdwijnen door een terugkoop, een faillissement of een andere gebeurtenis. Zijn enige handelszaak is zijn buitengewone voorraad informatie over mensen en het

on ignore ce qu'il deviendra si cette société était amenée à se transformer ou à disparaître.

Google n'est pas qu'un moteur de recherche. C'est une société (« Doubleclic ») qui fait de la prospection commerciale. À partir des profils que Google génère, on s'adresse à des annonceurs pour envoyer des publicités par Internet à tel type de profil.

Google, c'est aussi Gmail. Les mails sont stockés sur des serveurs qui se trouvent en Californie. Les mails sont accompagnés de publicité, parce qu'ils sont scannés automatiquement par la machine. Les publicités sont sélectionnées sur la base des mots contenus dans le mail.

« Google Streetview » est un système de cartographie en trois dimensions. Il ne s'agit pas de cartographie instantanée, mais de photos. Celles-ci mettent en jeu des personnes, si elles ne sont pas floutées. Il existe à ce sujet un accord avec Google, et la Commission cherchera des accords en la matière avec ses homologues européens.

« Google Latitude » permet de suivre les déplacements d'une personne à partir de son smartphone, en sachant à quelle borne wifi elle se connecte, pour faciliter ses contacts avec ses amis. Si ceux-ci n'ont pas envie d'avoir un contact, l'information est quand même stockée. Comment ce stock d'informations est-il géré et utilisé ?

Tout cela constitue ce que l'on appelle le « cloud-computing ». On sème aujourd'hui énormément de données sous forme de poussière d'information, à travers des comportements très différents. À un moment donné, ces poussières de données peuvent être agrégées, et constituer des profils et des informations très sensibles sur des personnes déterminées.

Le profilage, ce n'est pas que cela. La télévision numérique peut aussi être utilisée à cette fin. Même si les opérateurs ne le font pas aujourd'hui, il est possible de savoir, par ce moyen, ce qu'un utilisateur regarde comme programmes. Il en va de même lorsque l'on participe aux sondages des opérateurs télécom et des chaînes de télévision.

Le profilage est aussi possible à partir d'une carte bancaire (que l'on utilise partout sur l'autoroute, dans les grands magasins, sur Internet pour des réservations ou des achats ...), de la carte d'achats d'un grand magasin, etc.

L'orateur cite l'exemple suivant. Une personne habite à Bruxelles, dans le quartier où la communauté juive est la plus représentée, et où se trouve la seule grande surface de la ville disposant d'un rayon kasher. La personne qui achète kasher le fait parce qu'elle est un membre de la communauté juive qui respecte le prescrit religieux recommandant de consommer cette nourriture. Lorsqu'elle paie et présente sa carte d'achat

is onbekend wat hiermee gebeurt als deze firma wordt hervormd of verdwijnt.

Google is niet zomaar een zoekmachine. Het is een bedrijf (« *Doubleclic* ») dat zich met marketing bezighoudt. Op basis van de profielen die Google genereert, richt men zich tot adverteerders om via het internet reclame te sturen naar een bepaald profieltype.

Google, dat is ook Gmail. De e-mails worden bewaard op servers in Californië. De e-mails worden vergezeld van reclame omdat ze automatisch door de machine worden gescand. De reclame wordt geselecteerd op basis van de woorden in de e-mail.

« Google Streetview » is een systeem van driedimensionale kaarten. Het hierbij niet om mobile mapping, maar om foto's. Hierbij komen mensen ongewild op het internet indien ze niet onherkenbaar zijn gemaakt. Hierover bestaat een akkoord met Google en de Commissie zal ter zake overeenkomsten trachten te bereiken met haar Europese tegenhangers.

« Google Latitude » maakt het mogelijk de verplaatsingen van een persoon te volgen vanaf zijn smartphone door te weten met welke hotspot hij zich verbindt, teneinde het contact met zijn vrienden te vergemakkelijken. Indien die geen zin hebben in contact, wordt de informatie toch opgeslagen. Hoe wordt deze massa informatie beheerd en gebruikt ?

Dit alles vormt wat men « *cloud computing* » noemt. Men verspreidt momenteel enorm veel gegevens in de vorm van informatiedeeltjes via zeer verschillende gedragingen. Op een gegeven moment kunnen deze informatiedeeltjes worden samengevoegd en profielen en zeer gevoelige informatie over welbepaalde personen vormen.

*Profiling* houdt meer in dan dat alleen. Digitale televisie kan eveneens hiervoor worden gebruikt. Ook al doen de operatoren dit vandaag niet, het is mogelijk om via deze weg te weten te komen naar wat voor programma's de gebruiker kijkt. Hetzelfde geldt voor deelnames aan peilingen van telecomoperatoren en televisiezenders.

Profiling is ook mogelijk aan de hand van een bankkaart (die men overal gebruikt langs de autosnelweg, in grootwarenhuizen, op het internet voor reservaties of aankopen ...), van een klantenkaart van een grootwarenhuis, enz ...

Spreker haalt het volgende voorbeeld aan. Een persoon woont in Brussel, in een wijk waar de joodse gemeenschap het sterkst vertegenwoordigd is en waar zich de enige supermarkt van de stad bevindt die over een koosjere afdeling beschikt. De persoon die koosjere artikelen koopt, doet dat omdat hij of zij een lid is van de joodse gemeenschap dat de religieuze voorschriften rond voeding naleeft. Wanneer deze

en vue d'épargner des points, son profil d'achat est constitué.

Si l'on n'avait pas été attentif et si l'on n'avait pas sécurisé le traitement de ces informations, celui-ci aurait pu aboutir à constituer le fichier de tous les juifs religieux de Bruxelles.

Le profilage, c'est encore le compteur de consommation intelligente pour la consommation d'eau, de gaz, d'électricité, la télébillétique à travers le suivi des déplacements (*cf.* l'interopérabilité prochaine de la carte Mobib à tous les opérateurs télécom ...), les communications électroniques à travers le GSM, ...

Toutes ces informations qui, aujourd'hui, sont traitées de manière distincte les unes des autres, présentent un risque, non seulement par elles-mêmes, mais aussi en cas de regroupement et de traitement global.

Le profilage peut servir à des fins commerciales. Les sociétés commerciales sont très avides de données produites par les opérateurs télécom, de transport, etc., car tout cela renforce un profil, et permet de disposer de bases de données les plus précises possibles en vue de faire du marketing direct.

La Commission traite actuellement des problèmes afférents à des opérateurs de direct marketing, qui disposent de fichiers dont on se demande comment ils ont pu être constitués. De longues enquêtes sont parfois nécessaires pour déterminer d'où viennent les informations, qui sont de tous ordres et ont parfois été stockées pendant très longtemps.

Le direct marketing est la possibilité d'offrir à la personne qui se connecte à son ordinateur un produit spécifique en fonction de sa capacité d'achat propre. Google étudie un algorithme qui permettra bientôt de vendre à une personne les articles les plus divers à un prix adapté à son profil économique.

On va ainsi renverser complètement le mode de fonctionnement économique, en « enfermant » les personnes dans ce qu'elles sont supposées aimer en fonction de leur profil, à l'exclusion des produits ne correspondant pas à celui-ci.

Cela peut constituer un obstacle considérable à l'ouverture sur le monde et à la possibilité d'y voyager sans discrimination.

Enfin, lorsqu'on se rend sur un site, une série d'adresses Internet défilent dans l'une des barres du navigateur. Il en est ainsi car la page que l'on va consulter n'est pas faite comme l'était hier la page d'un journal, qui formait un ensemble. Aujourd'hui, une page internet, ce n'est pas une adresse, mais entre vingt

persoon betaalt en zijn of haar klantenkaart toont om punten te sparen, wordt het koopprofiel van de betrokkene gevormd.

Indien men niet had opgelet en indien men de verwerking van deze informatie niet had beveiligd, had dit kunnen leiden tot de aanmaak van een bestand van alle gelovige joden van Brussel.

*Profiling* is ook de slimme verbruiksmeter voor het verbruik van water, gas, elektriciteit, telebiljetiek via het volgen van verplaatsingen (*cf.* interoperabiliteit van de Mobib-kaart met alle telecomoperatoren ...), elektronische communicatie via gsm, ...

Al deze soorten informatie die vandaag los van elkaar worden verwerkt, houden een risico in, niet alleen door de informatie op zich maar tevens in geval van samenvoeging en globale verwerking.

Profiling kan dienen voor commerciële doeleinden. Bedrijven zijn erg belust op gegevens die door de telecomoperatoren, vervoersmaatschappijen, enz. worden geproduceerd. Al deze gegevens versterken immers een profiel en bieden de mogelijkheid te beschikken over een zo nauwkeurig mogelijke databank met het oog op direct marketing.

De Commissie behandelt momenteel problemen rond operatoren die aan direct marketing doen en die beschikken over bestanden waarvan men zich de vraag stelt hoe ze tot stand zijn kunnen komen. Soms is langdurig onderzoek nodig om te bepalen waar de informatie vandaan komt. De informatie is van allerlei aard en werd soms gedurende een zeer lange periode bewaard.

Direct marketing is de mogelijkheid om iemand die zich met zijn computer in verbinding stelt een specifiek product aan te bieden op grond van zijn eigen koopkracht. Google bestudeert een algoritme dat het binnenkort mogelijk zal maken iemand de meest diverse artikelen te verkopen tegen een prijs die is aangepast aan zijn economisch profiel.

Zo gooit men de werking van de economie volledig om, door mensen « op te sluiten » in wat wordt verondersteld hun voorkeur weg te dragen op basis van hun profiel, met uitsluiting van de producten die niet aan dat profiel voldoen.

Dit kan voor mensen een aanzienlijke hindernis vormen om zich open te stellen voor de wereld en om er zonder onderscheid naartoe te kunnen reizen.

Wanneer men naar een website surft, ziet men in een van de balken van de browser verschillende internetadressen achtereenvolgens verschijnen. Dat komt doordat de pagina die men gaat raadplegen niet gemaakt is zoals vroeger de pagina van een krant, als een geheel. Tegenwoordig omvat een webpagina niet

et cent adresses différentes. Une page est constituée de ce que l'on appelle des hyperliens transclusifs. Lorsqu'on appelle une page, il y a, chez l'opérateur auquel on se connecte, non pas la photo que l'on voit à l'écran, mais une adresse internet qui se connecte à l'endroit où se trouve la photo, une autre adresse internet qui se connecte à un autre endroit ...

Ainsi, quand on consulte son journal en ligne, de la publicité commerciale figure sur la page consultée, mais cela n'est pas comparable à la publicité que l'on trouve dans la version papier de la page du journal. En même temps que l'on se trouve sur le site de l'organe de presse, on se trouve en même temps sur le site de l'annonceur publicitaire, sur celui de Google Doubleclic ou de Google Analytic, qui analyse le comportement du consultant. On se trouve aussi, en même temps, sur les pages Facebook de gens que l'on ne connaît pas, puisqu'il y a, sur la page des organes de presse, « notre page Facebook » avec tous les amis du journal, ...

Le fait de pouvoir faire de la publicité ciblée va permettre aux journaux et à n'importe quel support informatique de faire des hyperliens transclusifs sur mesure en fonction du profil d'une personne.

Si Google, aujourd'hui, ne fait pas de politique, ces banques de données sont cependant très sensibles, comme le montrent les exemples précités. Cela peut aussi servir en matière d'accès au savoir, de répression policière si celle-ci n'est pas bien mesurée ... Ainsi, si l'on recherche, sur Google, la liste de toutes les personnes qui ont consulté le Coran au cours des derniers mois, et s'il s'en trouve parmi elles qui se sont rendues un jour de Paris à Abou Dhabi et qui se trouvaient assises, dans l'avion, à côté d'une personne appelée Mohamed, ces personnes commenceront à devenir suspectes dans le cadre d'un profilage qui met en rapport ces différents types d'informations. L'enjeu n'est donc pas seulement commercial, mais beaucoup plus vaste. Il touche à de nombreux domaines : surveillance des travailleurs, développement des fichiers e-justice et e-police (légitimes car bien moins inquiétants que la multitude de petits fichiers jadis en possession des policiers et contenant parfois des informations très délicates, mais à surveiller), recherche scientifique (notamment sur les profils génétiques), biométrie ...

Pour M. Verschueren, on ne reviendra pas en arrière car les sciences et les techniques continueront d'évoluer. Elles ne constituent pas en elles-mêmes le problème. Celui-ci se situe dans l'usage que l'on en fait, et c'est là qu'il faut se donner les outils nécessaires de réflexion et de maîtrise. Tel est le message que l'on tente de faire passer, y compris à travers une politique d'éducation dans les écoles.

één adres, maar tussen twintig en honderd verschillende adressen. Een pagina bestaat uit wat men « *transclusive links* » noemt. Wanneer men een pagina oproept, is er bij de operator waarmee men zich verbindt niet de foto die men op het scherm ziet, maar een internetadres dat in verbinding staat met de plaats waar de foto zich bevindt, een ander internetadres dat in verbinding staat met een andere plek ...

Zo verschijnt er reclame op het scherm wanneer men een krant online raadpleegt, maar dit is niet vergelijkbaar met de reclame die men in de papieren versie van de pagina van de krant vindt. Terwijl men zich op de site van het persorgaan bevindt, bevindt men zich tegelijkertijd op de site van de adverteerder, op die van Google Doubleclic of van Google Analytics, dat het gedrag van de bezoeker analyseert. Men bevindt zich ook tegelijk op de Facebook-pagina's van mensen die men niet kent, aangezien er op de pagina van de persorganen een link is naar de Facebook-pagina van de krant met alle mensen die de krant « leuk » vinden, ...

Gerichte reclame zal kranten en om het even welke informaticadrager in staat stellen transclusive links op maat te maken op grond van iemands profiel.

Hoewel Google vandaag niet aan politiek doet, zijn deze databanken echter zeer gevoelig, zoals de genoemde voorbeelden ook aantonen. Dit kan ook van pas komen inzake toegang tot kennis, repressie door de politie indien die niet goed is afgemeten ... Indien men zo op Google de lijst opzoekt van alle personen die tijdens de afgelopen maanden de Koran hebben geraadpleegd en indien er binnen die groep mensen waren die op een dag van Parijs naar Abu Dhabi zijn gereisd en in het vliegtuig naast een zekere Mohammed zaten, beginnen deze personen verdacht te worden in het kader van een profiling die deze verschillende soorten informatie met elkaar in verband brengt. De inzet is bijgevolg niet louter commercieel, maar veel ruimer dan dat. Heel wat domeinen zijn hierbij in het geding : toezicht op werknemers, ontwikkeling van e-justice- en e-police-bestanden (gerechtvaardigd want heel wat minder verontrustend dan de vele bestandjes die de politieagenten vroeger bezaten en waarin soms zeer delicate informatie stond, maar dient toch nauwlettend gevolgd te worden), wetenschappelijk onderzoek (met name over genetische profielen), biometrie ...

Volgens de heer Verschueren is er geen stap terug mogelijk, want wetenschap en techniek evolueren voortdurend. Dat gegeven op zich vormt niet het probleem. Het probleem schuilt veeleer in het gebruik dat men ervan maakt en daarvoor zijn instrumenten nodig met het oog op reflectie en beheersing. Dit is de boodschap die men tracht over te brengen, onder andere via een vormingsbeleid in de scholen.

*2. Échange de vues*

M. De Padt remercie les représentants de la CPVP pour la clarté de leur exposé, qui met en lumière les dangers et les opportunités liés à l'utilisation de l'informatique.

L'intervenant souhaiterait se pencher en particulier sur la manière dont les infractions à la législation sur la protection de la vie privée sont sanctionnées dans notre pays. Il renvoie à cet égard aux chiffres qui lui ont été communiqués par le ministre de la justice, d'où il ressort que l'on enregistre chaque année en moyenne 600 infractions à la loi sur la protection de la vie privée. On a recensé plus exactement 508 déclarations en 2007, 629 en 2008 et 672 en 2009. Le nombre de déclarations est donc en augmentation. Il faut également savoir que les infractions déclarées ne donnent lieu à une citation effective devant le tribunal correctionnel que dans 5 % des cas.

L'intervenant demande si une concertation est organisée avec les parquets à intervalles réguliers afin de voir pour quel genre de faits les citoyens déposent plainte. Au vu des chiffres évoqués, on pourrait croire de prime abord que la protection de la vie privée n'est pas une question qui préoccupe le citoyen outre mesure. Est-il vrai que le citoyen n'accorde guère d'importance à ce danger ?

Quelle interaction existe-t-il entre la Commission de la protection de la vie privée et le monde judiciaire, en vue de permettre une riposte appropriée aux infractions susceptibles d'être commises dans ce domaine ?

M. Courtois conclut de ce qui vient d'être dit qu'il vaut mieux rester chez soi. Il observe aussi qu'il existe une prescription pénale, mais aucune prescription informatique.

Il s'interroge sur les moyens dont on dispose pour agir, et rejoint à cet égard la réflexion du précédent orateur. Il n'est pas certain que les parquets disposent aujourd'hui des moyens judiciaires et techniques nécessaires pour endiguer certains phénomènes et les menaces qui en découlent pour la vie privée.

En ce qui concerne les auditions à organiser, l'orateur souhaiterait que l'on entende l'association belge des banques, qui pourra aussi fournir des informations sur les problèmes afférents aux cartes de crédit.

Mme Niessen relève que M. Verschueren a fait référence à Google et à Google Streetview. Elle aimerait savoir comment la CPVP traite ces dossiers. Une fois que le ministre a demandé et obtenu l'avis de la Commission de la protection de la vie privée, qu'advient-il ensuite ? Un accord intervient-il avec l'État belge, ou une solution est-elle imposée par ce dernier ?

*2. Gedachtewisseling*

De heer De Padt dankt de CBPL voor de duidelijke uiteenzetting, die wijzen op de gevaren en mogelijke opportuniteiten binnen het gebruik van informatica.

Spreker wenst nader in te gaan op de wijze waarop de inbreuken op de privacy-wetgeving in ons land worden gesanctioneerd. Hij verwijst naar de cijfers die hem daaromtrent werden bezorgd door de minister van Justitie. Daaruit blijkt dat er jaarlijks gemiddeld zeshonderd aangiftes plaatsvinden van inbreuken op de privacywet. Meer bepaald waren er in 2007 508 aangiften, in 2008 629 en in 2009 672. Het aantal aangiftes stijgt dus. Tevens wordt er slechts in 5 % van de gevallen effectief gedagvaard voor de correctionele rechtbank.

Spreker vraagt of er regelmatig overleg plaatsvindt met de parketten om na te gaan voor welke feiten de burger juist klacht neerlegt. Men zou immers uit de cijfers kunnen afleiden, althans op het eerste gezicht, dat men niet erg bezorgd is over de privacy. Is het inderdaad zo dat de belangstelling van de burger voor dit gevaar niet al te groot is ?

Welke interferentie bestaat er tussen de privacycommissie en de gerechtelijke wereld om op een gevatte manier tegen mogelijke inbreuken te kunnen optreden ?

De heer Courtois besluit uit wat er is gezegd dat men beter thuis kan blijven. Hij merkt ook op dat er een strafrechtelijke verjaring bestaat maar geen digitale verjaring.

Hij stelt zich vragen over de beschikbare middelen om op te treden en sluit zich op dat vlak aan bij de bedenking van de vorige spreker. Hij is er niet zeker van dat de parketten momenteel over de nodige juridische en technische middelen beschikken om bepaalde verschijnselen en gevaren tegen te gaan die een inbreuk vormen op de persoonlijke levenssfeer.

Wat de hoorzittingen betreft, wenst spreker de Belgische Vereniging van Banken uit te nodigen die ook informatie kan geven over de problemen die met kredietkaarten verband houden.

Mevrouw Niessen stipt aan dat de heer Verschueren verwees naar Google en Google Streetview. Spreker zou willen weten hoe de CBPL die dossiers behandelt. Wat gebeurt er zodra de minister het advies van de commissie voor de bescherming van de persoonlijke levenssfeer heeft gevraagd en gekregen ? Is er een overeenkomst met de Belgische Staat of legt laatstgenoemde een oplossing op ?

L'oratrice aimerait également, vu l'ampleur et la dimension internationale des problèmes qui se posent, que quelques pistes soient proposées pour orienter les travaux du groupe de travail.

M. Van Rompuy souscrit à cette dernière remarque, plus précisément en ce qui concerne le droit à l'oubli. Quelles sont les propositions en la matière, à concrétiser éventuellement à brève échéance sur le plan législatif ? Quelles mesures à effet rapide pourrait-on envisager ?

Pour ce qui est de la tendance au niveau des moteurs de recherche, l'intervenant souligne qu'ils sont quand même, eux aussi, soumis à des limites commerciales. Ils risquent ainsi de se nuire à eux-mêmes.

L'orateur indique que la Commission a traité 2 783 plaintes en 2009 et 2 843 en 2010 (année pour laquelle le rapport n'a pas encore été publié). Il s'agit parfois aussi de demandes d'informations car les requêtes qui n'ont pas été introduites dans les formes sont néanmoins traitées sous la catégorie « demandes d'informations ».

La CPVP tente tout d'abord une médiation avec celui contre lequel la plainte est introduite. Si celle-ci n'aboutit pas, la Commission se prononce sur le caractère fondé ou non de la plainte.

Beaucoup de plaintes concernent le marketing direct, les caméras de surveillance et leur usage abusif, le contrôle jugé abusif de travailleurs par leur employeur, le contrôle des centrales de fichage public. Les citoyens n'ont pas d'accès direct à la banque de données policières « BNG », mais bien un accès par l'intermédiaire de la Commission, qui vérifie si les fichages sont bien légitimes. Elle traite environ cent à cent-cinquante cas de ce type par an. Dans 75 % des cas, cela aboutit à un défichage ou à une modification du fichage. Il en va de même pour la centrale de crédit à la consommation gérée par la Banque Nationale. Cette centrale procède à un double fichage : la centrale positive, qui reprend tous les crédits existants, et la centrale négative, qui mentionne tous les défauts de remboursement.

Parmi les 3 000 plaintes environ que traite annuellement la Commission, certaines sont transmises au parquet, lorsque la Commission considère qu'il existe une infraction avérée et très problématique.

L'absence de politique criminelle en la matière pose cependant problème. La législation sur le traitement de données à caractère personnel paraît souvent trop complexe au juge, qui n'y ont pas volontiers recours. La dernière application significative en date, qui a fait grand bruit, concerne la décision d'un juge de paix d'Ostende, qui a considéré que l'accès à la direction pour l'Immatriculation des Véhicules (DIV) de la part

Spreker zou ook, gelet op de omvang en de internationale dimensie van de problemen, willen dat er een aantal werkwijzen worden voorgesteld om de werkzaamheden van de werkgroep te sturen.

De heer Van Rompuy wenst aan te sluiten bij deze laatste opmerking, meer bepaald op het vlak van het recht op vergetelheid. Wat zijn de voorstellen ter zake, eventueel op korte termijn te realiseren op wetgevend vlak ? Wat zijn eventuele *quick wins* ?

Wat betreft de tendens op het niveau van de zoekrobotten, onderstreept spreker dat zij toch ook zijn onderworpen aan commerciële limieten. Zo kunnen ze zichzelf onderuit halen.

Spreker wijst erop dat de Commissie 2 783 klachten heeft behandeld in 2009 en 2 843 in 2010 (voor 2010 werd nog geen verslag bekendgemaakt). Soms gaat het ook om vragen om informatie want de verzoeken die niet ingediend werden volgens de vereiste vorm, worden toch behandeld in de categorie « vragen om informatie ».

De CBPL probeert eerst te bemiddelen bij degene tegen wie een klacht is ingediend. Als dit op niets uitdraait, spreekt de Commissie zich uit over het feit of de klacht al dan niet gegrond is.

Veel klachten gaan over direct marketing, bewakingscamera's en misbruik hiervan, ongeoorloofd toezicht op de werknemers door de werkgever, het toezicht van centrales die openbare gegevens bijhouden. Burgers hebben geen rechtstreekse toegang tot de databank van de politie « ANG », maar wel via de Commissie die nagaat of het bijhouden van de gegevens wel wettig is. Ze behandelt ongeveer 100 tot 150 dergelijke gevallen per jaar. In 75 % van de gevallen leidt dit tot het verwijderen van de gegevens of tot een wijziging van het ficheren. Hetzelfde geldt voor de centrale voor consumentenkredieten die door de Nationale Bank wordt beheerd. Die centrale registreert de gegevens op twee manieren : de positieve centrale geeft alle bestaande kredieten weer, de negatieve centrale bevat alle wanbetalingen.

Van de ongeveer 3 000 klachten die de Commissie jaarlijks behandelt, worden sommige naar het parket doorverwezen als de Commissie meent dat het om een bewezen en erg problematische inbreuk gaat.

Het ontbreken van een strafrechtelijk beleid ter zake is echter een probleem. De wetgeving over de verwerking van persoonsgegevens lijkt soms te ingewikkeld voor de rechter die er niet gemakkelijk zijn toevlucht toe neemt. De recentste relevante toepassing die veel ophef maakte, was de beslissing van de vrederechter van Oostende die meende dat de toegang van privéparkeerbedrijven tot de directie Inschrijving

de sociétés de parkings privés était illégale. Il y avait effectivement un problème d'encadrement de cette banque de données.

Il s'agissait cependant là d'un cas assez exceptionnel, que l'on peut considérer comme marginal par rapport à la réalité des enjeux.

En ce qui concerne Google Streetview, la Commission a émis une recommandation à l'égard de Google, qui s'est engagé à s'y conformer pour le produit Streetview : floutage des personnes, compétence des juridictions belges en cas de plainte lorsque celle-ci est suscitée par une photo prise en Belgique, qu'elle concerne un Belge, un étranger, un résidant sur le territoire ou pas, publicité dans les journaux et sur leur site au moment des prises de vue pour annoncer les trajets des prises de vue, abaissement de l'arbre de prise de vue à la hauteur approximative des yeux d'une personne.

Par contre, il n'y a pas eu d'accord sur le volet « Latitude », c'est-à-dire la captation par les voitures Google, qui circulent pour prendre des photos, la captation des bornes wifi, etc. Ce dossier, qui reste problématique, a été transmis au parquet le 15 décembre 2010.

Dans le même dossier, la CNIL, homologue français de la CPVP, qui a la compétence de prononcer des amendes, vient de condamner Google à 100 000 euros d'amende, soit le montant maximum possible.

En Suisse, un jugement vient d'être rendu, qui impose à Google, à propos de Google Streetview, ce que la Commission a obtenu en Belgique de manière négociée.

De son côté, la *Federal Computer Crime Unit* (FCCU), qui fonctionne bien, n'a pas vocation à poursuivre toutes les infractions à la loi sur la protection de la vie privée, mais plutôt des infractions telles que le piratage informatique, l'usurpation d'identité, le vol par voie informatique, ...

La CPVP n'a, comme déjà indiqué, de contacts avec les parquets qu'au cas par cas, et lorsqu'elle les sollicite. Elle n'a été sollicitée par les parquets que deux ou trois fois en tant qu'expert. Si une décision conduisait à adopter une politique criminelle en la matière, tout le reste en découlerait logiquement, et notamment des rencontres plus fréquentes avec la conférence des procureurs du Roi.

Pour ce qui est de l'interaction avec la police, la Commission, comme elle dénonce des faits au parquet, a en retour, en cas d'enquête, des contacts avec les services de police. L'orateur souligne l'excellente qualité des rapports que la Commission a aujourd'hui avec les services de police.

Voertuigen (DIV) onwettig was. Er was inderdaad een probleem met die gegevensbank.

Het ging hier echter om een vrij uitzonderlijk geval dat eerder bijkomstig is in vergelijking met de uitdagingen waar het werkelijk om gaat.

Wat Google Streetview betreft, heeft de Commissie een aanbeveling geformuleerd voor Google die zich ertoe verbonden heeft zich hiernaar te zullen schikken voor het product Streetview : het wazig maken van personen, bevoegdheid van de Belgische rechtbanken bij klachten naar aanleiding van een foto die in België is genomen ongeacht of het een Belg betreft, een vreemdeling, een inwoner op het grondgebied of niet, reclame in de kranten en op hun site op het ogenblik van de beeldopnames om de trajecten van de beeldopnames aan te kondigen, lagere invalshoek van de beeldopnames op ooghoogte.

Er is daarentegen geen akkoord bereikt over het onderdeel « Google Latitude », met andere woorden over wat de voertuigen van Google opvangen terwijl ze rondrijden om foto's te nemen, het opvangen van informatie van hotspots enz. Dit dossier, dat problematisch blijft, werd naar het parket doorverwezen op 15 december 2010.

In hetzelfde dossier heeft de CNIL, de Franse tegenhanger van de CBPL die ook boetes mag uitspreken, Google onlangs veroordeeld tot een boete van 100 000 euro, namelijk de hoogst mogelijke boete.

In Zwitserland werd onlangs een vonnis gewezen dat Google, in verband met Google Streetview, verplicht tot datgene wat de Commissie in België na onderhandeling verkreeg.

Anderzijds voelt de *Federal Computer Crime Unit* (FCCU), die goed werk levert, zich niet geroepen om alle schendingen van de wet op de bescheming van de persoonlijke levenssfeer te vervolgen, maar wel overtredingen zoals *hacking*, de online identiteitsroof, cyberdiefstal, ...

De CBPL neemt, zoals reeds vermeld, enkel contact op met het parket geval per geval en wanneer daarom wordt verzocht. De parketten deden slechts twee of drie keer een beroep op de Commissie als deskundige. Indien een beslissing zou leiden tot een strafrechtelijk beleid ter zake, dan zou logisch gezien al het overige hieruit voortvloeien en meer bepaald herhaaldelijke ontmoetingen met de raad van de procureurs des Konings.

Wat de interactie met de politie betreft, staat de Commisie, in geval van een onderzoek, in contact met de politiediensten, in ruil voor het feit dat zij feiten aanklaagt bij het parket. Spreker benadrukt dat de Commissie momenteel uitstekende contacten heeft met de politiediensten.

En effet, au-delà des contacts que la CPVP a avec ces services en vue de réprimer les infractions, elle surveille également leurs fichiers, leurs activités et leurs comportements.

Les services de police ont accompli un effort remarquable pour sécuriser les fichiers de la BNG, qui n'est pas une banque de données policières centralisée, mais un index qui renvoie à d'autres endroits, de sorte que la concentration de l'information n'existe pas.

Lorsqu'une personne se connecte à la base de données, cette connection est enregistrée et suivie. Si la personne souhaite avoir accès à une information, elle devra en donner la raison.

Des contrôles sont effectués par la Commission et par l'Inspection générale, et conduisent, en cas d'abus, à des mesures disciplinaires et à des renvois devant les tribunaux.

Quant aux fichiers des banques, l'orateur estime qu'ils sont effectivement inquiétants. La CPVP a des contacts avec l'association belge des banques à ce sujet.

La gestion des données dans les banques est très sécurisée. La porosité se situe plutôt au niveau de la politique de protection interne à la banque. Il peut arriver par exemple qu'un employé de banque surveille le compte de l'amant de sa femme. À partir d'une ou deux plaintes, on parvient à identifier ce genre de problème. Les banques ont généralement des politiques de sécurité très strictes permettant de réprimer les abus. Par contre, elles doivent, conformément aux lois belges et internationales, conserver des données pendant une longue période et les mettre dans certains cas à disposition des forces de police. Ces données bancaires qui sont traitées à des fins policières le sont de manière beaucoup plus strictes que, par exemple, les données des compagnies aériennes.

Les fichiers des banques sont parmi les fichiers les plus sensibles. Cela représente 13 millions de transactions par jour. Il conviendrait dès lors selon l'orateur d'entendre des représentants du secteur bancaire pour constater que les banques mènent une politique de sécurité adéquate, ou pour leur demander si elles ont besoin de moyens supplémentaires.

Répondant à M. Courtois, l'orateur déclare que le monde évolue, et qu'il faut évoluer avec lui, mais en se donnant les outils pour le maîtriser. En ce qui concerne Google, un dialogue existe et la CPVP atteint petit à petit des résultats. Il faudra trancher sur les enjeux importants que sont les bases de données américaines. Ce ne sera pas chose aisée, et devra sans doute se faire par l'adoption de normes.

À défaut de politique criminelle spécifique, il n'y a pas de moyens particuliers alloués aux parquets, si ce

Naast de contacten met die diensten om wetsovertredingen te bestraffen, houdt de CBPL ook toezicht op hun bestanden, activiteiten en gedrag.

De politiediensten hebben een opmerkelijke inspanning geleverd om de fiches van de ANG te beveiligen. Dit is geen gecentraliseerde politiedatabank maar een index die naar andere bronnen verwijst, waardoor er geen concentratie van de informatie is.

Wanneer iemand inlogt op de databank, dan wordt die login geregistreerd en gevolgd. Als die persoon toegang wil tot informatie, dan moet hij de reden meedelen.

De Commissie en de algemene inspectie houden toezicht en gaan, in geval van misbruik, over tot disciplinaire maatregelen en doorverwijzingen naar de rechtbank.

Spreker meent dat de bankgegevens daadwerkelijk verontrustend zijn. De CBPL voert hierover besprekingen met de Belgische Vereniging van Banken.

Databeheer in de banken is streng beveiligd. Het interne veiligheidsbeleid in de bank is echter niet waterdicht. Zo kan bijvoorbeeld een bankbediende de rekening van de minnaar van zijn vrouw in het oog houden. Op basis van één of twee klachten kan men de aard van dit soort problemen identificeren. De banken hebben in het algemeen een erg strikt veiligheidsbeleid dat misbruik beteugelt. Banken moeten echter, overeenkomstig de Belgische en internationale wetten, gegevens gedurende een lange periode bewaren en ze in sommige gevallen ter beschikking stellen van de politie. Bankgegevens die voor politiedoeleinden worden gebruikt, zijn aan veel striktere regels onderworpen dan bijvoorbeeld de gegevens van luchtvaartmaatschappijen.

Bankgegevens zijn één van de meest gevoelige gegevens. Het gaat om 13 miljoen transacties per dag. Spreker vindt het bijgevolg aangewezen om vertegenwoordigers van de bankensector te horen om na te gaan of de banken een passend beveiligingsbeleid voeren of om hun te vragen of zij bijkomende middelen nodig hebben.

Spreker antwoordt de heer Courtois dat de wereld verandert en dat we die veranderingen moeten volgen maar met de nodige middelen om ze in toom te houden. Over Google worden gesprekken gevoerd en de CBPL bereikt geleidelijk aan resultaten. Er moeten knopen worden doorgehakt voor de belangrijke uitdagingen van de Amerikaanse databanken. Dat zal niet gemakkelijk zijn en moet ongetwijfeld via de goedkeuring van normen gaan.

Aangezien er geen specifiek strafrechtelijk beleid is, hebben de parketten geen bijzondere middelen, buiten

n'est les moyens dont dispose la *Federal Computer Crime Unit*. Dès lors, lorsqu'un procureur veut ouvrir un dossier relevant de la protection des données à caractère personnel, il doit opérer des choix en termes de dossiers et de personnel.

Quant au budget de la CPVP, il est de 6 millions d'euros par an. La CPVP se développe au fur et à mesure et privilégie une consolidation des activités actuelles plutôt qu'une croissance impossible à gérer.

La prochaine étape sera de créer une cellule d'enquête spécifique pour procéder à des enquêtes dans des fichiers; enquêtes qui sont aujourd'hui réalisées dans les limites des moyens disponibles. La CPVP réalise l'audit de grandes banques de données, mais il faudrait le faire de manière plus systématique, ce qui suppose des moyens supplémentaires.

M. Mahoux suppose que les moteurs de recherche autres que Google sont également concernés et que les mêmes observations peuvent être formulées à leur sujet.

M. Verschueren le confirme.

M. De Padt signale qu'un ouvrage intitulé « *Big brother in Europa* », écrit par l'avocat bruxellois Raf Jespers, aurait été publié l'année dernière. Il serait peut-être utile d'entendre aussi l'auteur de ce livre.

M. Verschueren engage les parlementaires à se méfier du réflexe catastrophiste. Il est préférable d'entendre des personnes qui pourront expliquer l'état des choses et des faits.

Sur la question de Google et des algorithmes, et la manière, humaine ou purement algorithmique, dont Google intervient dans le profilage, l'orateur suggère d'entendre M. Jean-Marc Dinant, informaticien au Centre de Recherche Information, Droit et Sociétés (CRIDS) à Namur, qui pourra dresser un tableau permettant aux parlementaires de se forger leur propre opinion, plutôt que de recourir à des auteurs qui font déjà leur propre synthèse et usent parfois de raccourcis.

L'orateur ajoute, à propos du terrorisme et des fichiers policiers, qu'il existe des fichiers européens (Europol, Eurojust, Eurodac, SIS, ...). Tous ces fichiers sont surveillés par des autorités de protection des données. Si l'on constate des abus dans l'utilisation de ces fichiers, c'est au législateur à légiférer pour préciser les fins auxquelles ils peuvent ou non être exploités.

Ces fichiers, qui peuvent être inquiétants (la base de données Eurodac qui collecte les empreintes digitales des demandeurs d'asile, le fichier « Schengen » qui reproduit quasiment notre BNG et la banque de données centralisée des autres pays de l'espace

de middelen waarover de *Federal Computer Crime Unit* beschikt. Wanneer een procureur bijgevolg een dossier wil openen betreffende de bescherming van persoonsgegevens, moet hij keuzes maken inzake dossiers en personeel.

De begroting van de CBPL bedraagt 6 miljoen per jaar. De CBPL ontwikkelt zich geleidelijk aan en streeft naar een consolidering van de huidige activiteiten in plaats van naar een onbeheersbare groei.

De volgende fase is de oprichting van een specifieke onderzoekscel die databanken onderzoekt; onderzoek dat momenteel binnen de grenzen van de beschikbare middelen wordt gevoerd. De CBPL licht de grote databanken door, maar dat zou systematischer moeten gebeuren en daarvoor zijn bijkomende middelen nodig.

De heer Mahoux veronderstelt dat het ook gaat om andere zoekmachines dan Google en dat dezelfde opmerkingen ook op hen van toepassing kunnen zijn.

De heer Verschueren bevestigt dat.

De heer De Padt stipt aan dat er vorig jaar een boek « *big brother in Europa* » zou zijn verschenen, van de hand van een Brussels advocaat, met name Raf Jespers. Misschien zou het goed zijn ook deze man te horen.

De heer Verschueren vraagt de parlementsleden om zich te hoeden voor de catastrofe-reflex. Men kan beter personen horen die de stand van zaken en feiten kunnen uiteenzetten.

Wat Google en de algoritmen betreft en de manier, menselijk of puur algoritmisch, waarop Google bijdraagt aan het profileren, stelt spreker voor een hoorzitting te organiseren met de heer Jean-Marc Dinant, informaticus bij het *Centre de Recherche Information, Droit et Sociétés* (CRIDS) te Namen, die een overzicht kan schetsen waardoor de parlementsleden zelf hun mening kunnen vormen, in plaats van die te baseren op auteurs die reeds hun eigen synthese hebben gemaakt en soms snel conclusies trekken.

Spreker voegt hieraan toe dat er, wat terrorisme en politiefichiers betreft, Europese gegevensbestanden bestaan (Europol, Eurojust, Eurodac, SIS, ...). Al die gegevensbestanden worden gecontroleerd door de eenheden die belast zijn met de gegevensbescherming. Als men misbruik vaststelt bij het gebruik van die gegevensbestanden, is het de taak van de wetgever om in de wet vast te stellen waarvoor de gegevens al dan niet mogen worden gebruikt.

Die gegevensbestanden kunnen verontrustend zijn (de databasis van Eurodac bevat vingerafdrukken van asielzoekers, het « Schengen »-bestand geeft zowat heel onze BNG weer en de gecentraliseerde gegevens van de andere Schengen-landen) worden gecontro-

Schengen), font l'objet d'un monitoring par les autorités nationales de protection des données et par un superviseur européen.

Enfin, M. Mahoux propose de tracer les lignes directrices que le groupe de travail entend adopter. Il suggère de procéder par thèmes, tout en demandant, de manière transversale, au responsable d'un moteur de recherche de venir s'exprimer, de façon très générale, par rapport à une série de questions fort larges comme, par exemple, la manière dont le moteur de recherche prend en compte la vie privée.

Le premier thème qui pourrait, parallèlement, être abordé est celui du droit à l'oubli en tous ses aspects; la problématique de la vie privée dans le temps et dans l'espace étant un problème complexe.

Un second thème à aborder est celui du profilage, à la fois sur le plan technique et sur celui de l'utilisation qui en est faite.

Pour conclure, M. Mahoux retiendra deux aphorismes qui découlent de l'exposé de M. Verschueren, à savoir « Si c'est gratuit, combien ça coûte », et « Quand on ouvre une fenêtre sur le monde, c'est surtout le monde qui rentre chez vous ».

## B. Auditions du 26 avril 2011

*1. Exposé de M. Rogier Klimbie, représentant de Google*

M. Klimbie expose que la protection des données personnelles est une préoccupation permanente pour Google. Aussi, la société s'est assigné les principes directeurs suivants :

— Google utilise l'information relative à ses utilisateurs pour leur fournir des produits et services utiles et en leur donnant une plus-value. Il est important de retenir que Google ne développe un produit que s'il présente une utilité et ne va pas à l'encontre des intérêts de l'utilisateur;

— les nouveaux produits développés tentent toujours d'avoir des normes élevées de protection de données et supérieures à celles des concurrents;

— la collecte d'informations personnelles doit être la plus transparente possible;

— les utilisateurs doivent bénéficier d'un choix en termes de protection de données et ce choix doit être compréhensible pour eux;

leerd door de nationale diensten voor bescherming van privégegegevens en ook door een Europese supervisor.

De heer Mahoux stelt voor om de hoofdlijnen uit te zetten die de werkgroep wil gebruiken. Hij stelt voor thematisch tewerk te gaan en tegelijkertijd transversaal, door een directeur van een zoekmachine te vragen om uitleg te komen geven op een algemene manier, over een aantal breed opgevatte kwesties, zoals de manier waarop de zoekmachine omgaat met het privéleven.

Het eerste thema dat intussen kan worden aangesneden, is dat van het recht op verwijdering van gegevens in al zijn aspecten; de problematiek van de persoonlijke levenssfeer in de tijd en ruimte is immers ingewikkeld.

Een tweede thema dat besproken dient te worden is dat van het profileren, zowel vanuit technisch oogpunt als betreffende het gebruik dat er wordt van gemaakt.

Om af te sluiten wil de heer Mahoux nog twee aforismen onthouden die uit de uiteenzetting van de heer Verschueren voortvloeien : « als het gratis is, hoeveel gaat het dan kosten » en « als men een venster op de wereld openzet, is het vooral de wereld die naar binnenkomt ».

## B. Hoorzittingen van 26 april 2011

*1. Uiteenzetting van de heer Rogier Klimbie, vertegenwoordiger van Google*

De heer Klimbie legt uit dat de bescherming van persoonlijke gegevens een voortdurende bekommernis is voor Google. Het bedrijf volgt dan ook de volgende beleidslijnen :

— Google gebruikt de informatie die betrekking heeft op zijn gebruikers om hen nuttige producten en diensten aan te bieden en daarbij een meerwaarde te bieden. Men moet zeker onthouden dat Google alleen producten ontwerpt die nuttig zijn en de belangen van de gebruiker niet tegenwerken.

— als men nieuwe producten ontwikkelt, tracht men steeds hoge normen te hanteren op het vlak van de gegevensbescherming, strenger dan bij de concurrentie;

— het verzamelen van persoonlijke informatie dient op zo'n transparant mogelijke manier te gebeuren;

— de gebruikers moeten keuzes hebben wat de gegevensbescherming betreft en die keuzes moeten hen duidelijk zijn uitgelegd;

— Google en tant que détenteur d'une quantité importante d'information est conscient de sa responsabilité et a donc développé une politique de sécurité interne très stricte quant à la sauvegarde et au stockage de ces données. Cette politique est mise en œuvre par le biais de standards technologiques élevés ainsi que par des systèmes de sécurité informatiques importants.

Les données collectées par Google

Google collecte des données pour trois raisons différentes :

— les données sont collectées pour améliorer les produits et services de Google;

Google utilise l'information collectée pour améliorer ses résultats de recherche. L'objectif est d'obtenir une information agrégée suite à l'interaction des utilisateurs avec le moteur de recherche Google en vue de l'améliorer et de la rendre plus appropriée. L'algorithme est donc à chaque fois amélioré pour obtenir de meilleurs résultats de recherche.

Ainsi, si un mot est mal encodé dans le moteur de recherche, Google propose automatiquement un autre mot. Or, ceci n'est possible que si Google analyse et utilise l'information de ses utilisateurs et dont il résulte qu'une autre recherche est plus adéquate. De la même manière, Google achève le mot encodé dans le moteur de recherche dès que les premières lettres sont encodées. C'est un exemple d'utilisation de l'information en vue de créer une plus-value pour l'utilisateur.

— les données sont collectées afin de combattre des pratiques nuisibles telles que le *phishing*;

Google vise également à rendre le web plus sécurisé et utilise à cette fin une technologie (« *safe browsing technology* ») qui analyse en permanence deux types de sites internet. D'une part, les sites qui contiennent des virus (codes) qui s'introduisent dans les ordinateurs des utilisateurs (malware, chevaux de Troie) et, d'autre part, les sites avec « *phishing* » qui tentent de soustraire des données personnelles comme des données bancaires. Ces sites sont identifiés et renseignés par Google comme étant des sites pouvant causer des dommages aux ordinateurs des utilisateurs. M. Klimbie souligne que Google a mis cette technologie à disposition et que, par exemple, Apple l'a reprise dans son « safari browser ».

— les données sont collectées pour développer de nouveaux produits et services.

Ainsi, les « log data » sont collectés et utilisés pour créer de nouveaux services et produits. M.Klimbie cite à titre d'exemple le service de « Google translate ». Par le biais de données (« *computer data* ») détenues par Google, un moteur de recherche dédié a été créé et

— Google is bewaarder van een grote hoeveelheid informatie en beseft dat dit een grote verantwoordelijkheid is; daarom is er een zeer strikt intern veiligheidsbeleid wat het bewaren en opslaan van die gegevens betreft. Dit beleid wordt uitgevoerd dankzij hoge technische normen en een zwaar beveiligingssysteem voor de informatica.

De gegevens die Google verzamelt

Google verzamelt gegevens om drie redenen :

— de gegevens worden verzameld om de producten en de diensten van Google te verbeteren;

Google gebruikt de verzamelde informatie om zijn zoekresultaten te verbeteren. Het is de bedoeling om samengevoegde informatie te verkrijgen door interactie van de gebruikers met de zoekmachine van Google, om deze laatste te verbeteren en meer « *to the point* » te maken. Het algoritme wordt dus elke keer verbeterd om nog betere zoekresultaten te verkrijgen.

Als een woord bijvoorbeeld slecht in de zoekmachine wordt ingevoerd, zal Google automatisch een ander woord voorstellen. Dit is alleen mogelijk als Google de informatie van zijn gebruikers analyseert en gebruikt om te besluiten dat een andere zoekopdracht gepaster is. Op dezelfde manier maakt Google het in de zoekmachine ingevoerde woord af zodra er een paar letters staan. Dit toont aan hoe informatie gebruikt kan worden om voor de gebruiker een meerwaarde te creëren.

— de gegevens worden verzameld om schadelijke praktijken als phising tegen te gaan;

Google wil internet ook veiliger maken en gebruikt hiervoor een technologie (« *safe browsing technology* ») die voortdurend twee types van internetsites analyseert. Enerzijds gaat het om sites die virussen (codes) bevatten die zich in de computer nestelen (*malware*, Trojaanse paarden) en anderzijds om sites die aan phising doen, m.a.w die pogen persoonlijke gegevens te achterhalen, zoals bankgegevens. Die sites worden door geïdentificeerd en vermeld als sites die schade kunnen toebrengen aan de computers van de gebruikers. De heer Klimbie benadrukt dat Google deze technologie beschikbaar stelt en dat Apple haar bijvoorbeeld heeft overgenomen in zijn « safaribrowser ».

— de gegevens worden verzameld om nieuwe producten en diensten te ontwikkelen.

Zo worden de « log data » verzameld en gebruikt om nieuwe producten en diensten te ontwerpen. Als voorbeeld vermeldt de heer Klimbie de « Google translate » dienst. Via de gegevens (« computer data ») waarover Google beschikt is er een speciale zoek-

permet, sur base des données agrégées, d'améliorer à chaque fois le résultat d'une traduction. « Google translate » permet actuellement une traduction vers cinquante-sept langues différentes et vise un objectif de cent langues. M.Klimbie souligne qu'il importe d'avoir à l'esprit qu'il s'agit de données agrégées qui sont utilisées par Google et non de données individualisées.

Google collecte les informations suivantes :

— les « *log data* » étant les informations conservées par Google lors de l'interaction de l'ordinateur de l'utilisateur avec les services de Google. Google ignore donc qui est l'utilisateur. Ces données sont utilisées par exemple pour combattre le « spam » et d'autres pratiques comme le « *phishing* »;

— les « *account data* » étant les données liées aux comptes que l'utilisateur décide lui même d'ouvrir lorsqu'il se connecte à un service comme « gmail » ou « picasa ». Ces données sont conservées mais l'utilisateur dispose toujours de la faculté de décider de ce qu'il souhaite conserver et de la manière dont ces données doivent être conservées. L'utilisateur peut aussi à chaque instant décider de supprimer son compte et ses données.

— Les « *product data* » étant des données qui ne sont pas liées à des individus comme Google Earth par exemple.

M. Klimbie donne un exemple de « *log data* » conservés par Google lorsqu'une recherche est effectuée dans « Google Search ». Ces données ne sont pas reliées à un individu. À partir d'un extrait d'une « log line », M. Klimbie décrit les différentes références affichées :

— il y a tout d'abord l'adresse IP qui est utilisée afin d'améliorer les résultats de la recherche et pour se protéger des attaques informatiques provenant de l'extérieur;

— les données relatives à la date et à l'heure qui sont utilisées pour, par exemple, analyser l'ordre des recherches dans une période donnée et examiner la relation entre différentes recherches et rendre celles-ci plus relevantes;

— l'« *URL including query* » qui indique ce qui est recherché;

— le « *user agent* » qui indique le type de navigateur (*browser*) et d'« *operating system* »;

— le « *cookie ID* ».

L'ensemble de ces données sont neutralisées après neuf mois à l'exception du « *cookie ID* » qui est neutralisé après dix-huit mois. Cette différence s'ex-

machine gemaakt die, op basis van alle samengevoegde gegevens, elke keer een betere vertaling levert. « Google translate » vertaalt momenteel in 57 verschillende talen. Het is de bedoeling dit op te drijven tot 100 talen. De heer Klimbie benadrukt dat men niet uit het oog mag verliezen dat Google samengevoegde gegevens gebruikt, geen individuele gegevens.

Google verzamelt de volgende gegevens :

— de « *log data* » : dat zijn de gegevens die Google bewaart wanneer de computer van de gebruiker interageert met de diensten van Google. Google weet dus niet wie die gebruiker is. De gegevens worden gebruikt om bijvoorbeeld spam en andere praktijken, zoals phishing, tegen te gaan;

— de « *account data* », dat zijn de gegevens die verband houden met de accounts die de gebruiker zelf besluit te openen wanneer hij inlogt op diensten als « gmail » of « picasa ». Die gegevens worden bewaard, maar de gebruiker beschikt altijd over de mogelijkheid om te beslissen wat hij wil bewaren en hoe die gegevens worden bewaard. De gebruiker kan ook op ieder moment beslissen om zijn account en de bijbehorende gegevens te wissen.

— De « *product data* » : dat zijn gegevens die niet gelinkt zijn aan individuen, zoals Google Earth.

De heer Klimbie geeft een voorbeeld van « log data » die door Google worden bewaard nadat er een zoekopdracht is uitgevoerd in « Google Search ». Die gegevens zijn niet gelinkt aan een individu. Op basis van een uittreksel van een « log line » beschrijft de heer Klimbie de verschillende referenties die verschijnen :

— eerst en vooral is er het IP-adres, dat gebruikt wordt om de zoekresultaten te verfijnen en om zich te beschermen tegen cyberaanvallen van buitenaf;

— de gegevens die de datum en het uur vermelden en die gebruikt worden om bijvoorbeeld de volgorde van de zoekopdrachten binnen een bepaalde periode te analyseren, of de relatie tussen verschillende zoekopdrachten, om op die manier de zoekopdrachten relevanter te maken;

— de « *URL including query* » : dit geeft aan wat er gezocht wordt;

— de « *user agent* » die aangeeft welke browser en welk « *operating system* » er gebruikt werden;

— de « *cookie ID* ».

Al die gegevens worden na negen maanden geneutraliseerd, behalve de « *cookie ID* », die pas na achttien maanden wordt geneutraliseerd. Dat verschil

plique par le fait que l'utilisateur peut lui-même décider de conserver ces cookies en fonction des modalités de protection choisies (« *privacy settings* »). Ce n'est pas possible avec l'adresse IP par exemple et par conséquent la durée est plus courte. L'objectif de la conservation de ces données par Google est d'améliorer les services offerts aux utilisateurs et l'exactitude des recherches.

Initiatives en termes de protection des données

Ces initiatives se catégorisent en termes de transparence et de contrôle, de sécurité et de simplification. M. Klimbie en cite quelques-unes. Par le truchement du « tableau de bord google », l'utilisateur peut visualiser en un seul endroit du site Google l'ensemble des données de son compte et des services qu'il utilise. Google estime qu'il est capital que les utilisateurs puissent effectivement opérer un choix quant à l'activation de certains services et contrôler ces choix.

Google affiche également par le biais d'un « *transparency report* » le nombre de requêtes formulées par les gouvernements aux fins d'obtenir des informations sur des utilisateurs. M. Klimbie souligne que Google coopère régulièrement avec les autorités dans plusieurs domaines et plus particulièrement dans la lutte contre la pédopornographie. Par contre, en ce qui concerne les données personnelles de ces utilisateurs, Google adopte une politique très stricte en ce sens que la requête doit toujours émaner d'une autorité judiciaire et qu'en tout état de cause Google conserve un pouvoir d'appréciation au cas par cas pour contester en justice ladite requête.

Enfin, le « *privacy center* » rassemble toutes les informations relatives à la protection des données personnelles de l'utilisateur : « google dashboard », « preferences manager », « date liberation front ». L'idée maîtresse est que l'utilisateur conserve un choix quant à l'étendue de la protection de ses données personnelles.

*2. Exposés de Mme De Vinck et MM. Somers et Schröder, représentants de l'Asbl ISPA*

Mme De Vinck précise que l'association regroupe les fournisseurs internet de Belgique; soit toutes les sociétés qui ont une activité dans le secteur de l'Internet (fournisseurs d'accès, sociétés d'hébergement, des « data center ») mais aussi des fournisseurs de services comme Microsoft. En tant qu'organisation faîtière, ISPA essaie autant que possible d'adopter des positions dans l'intérêt général du secteur.

wordt verklaard door het feit dat de gebruiker zelf kan beslissen om de cookies te behouden, door de beschermingsgraad zelf in te stellen (« privacy settings »). Dit is niet mogelijk met het IP-adres bijvoorbeeld, dus wordt dat minder lang bewaard. Google bewaart die gegevens om zo de diensten die aan de gebruikers worden aangeboden te verbeteren en de zoekopdrachten te verfijnen.

Initiatieven met betrekking tot de bescherming van gegevens

Die initiatieven kunnen gerangschikt worden volgens graad van transparantie en controle, veiligheid en vereenvoudiging. De heer Klimbie noemt er een paar. Door middel van het « Google dashboard » kan de gebruiker op één enkele plaats een overzicht krijgen van al de gegevens van zijn Google-accounts en de diensten die hij gebruikt. Google vindt het essentieel dat de gebruikers zelf kunnen kiezen welke diensten ze activeren en dan ook de controle houden over die keuzes.

Google geeft ook met een « transparency report » het aantal pogingen weer dat door regeringen is gedaan om informatie over de gebruikers te verkrijgen. De heer Klimbie onderstreept dat Google geregeld samenwerkt met overheden op verschillende vlakken en meer bepaald bij de strijd tegen de kinderpornografie. Wat de persoonlijke gegevens van die gebruikers betreft voert Google echter een zeer strikt beleid : het verzoek dient altijd uit te gaan van een gerechtelijke instantie en Google behoudt het recht elk geval te beoordelen om het verzoek desgevallend voor de rechtbank te weigeren.

Het « *privacy center* » ten slotte verzamelt alle informatie die te maken heeft met de bescherming van de persoonlijke gegevens van de gebruiker : « google dashboard », « *preferences manager* », « *date liberation front* ». De basisidee is dat de gebruiker zelf kan kiezen in hoeverre hij zijn persoonlijke gegevens beschermt.

*2. Uiteenzettingen van mevrouw De Vinck en de heren Somers en Schröder, vertegewoordigers van de VZW ISPA*

Mevrouw De Vinck verduidelijkt dat de vereniging de internetbedrijven van België groepeert; dat zijn de bedrijven die een activiteit hebben in de internetsector (providers, serverbedrijven, « data centers ») maar ook dienstverleners als Microsoft. De overkoepelende organisatie ISPA probeert zoveel mogelijk standpunten in te nemen die in het algemene belang van de sector zijn.

M. Geert Somers représente quant à lui le cabinet d'avocats Time.lex qui est l'un des partenaires de l'ISPA et qui se propose d'aborder des questions juridiques liées à la protection des données personnelles.

Paradoxe en matière de protection de la vie privée

M. Somers constate l'existence d'un paradoxe en matière de protection de la vie privée. Bien que la vie privée soit un sujet sensible pour les utilisateurs, ces derniers la divulguent de plus en plus. Ils le font volontairement ou non et ne sont généralement pas conscients de l'impact que cela a sur leur vie privée :

— divulgation volontaire : par les « réseaux sociaux » (Facebook, Myspace); Youtube, Twitter, blogs ...

— divulgation involontaire : par les moteurs de recherche (les critères de recherche sont conservés et liés à l'utilisateur), par le scannage de l'Internet à des fins de profilage (Spokeo, par exemple), par des *cookies* tiers et des logiciels espions, qui révèlent machinalement le comportement des utilisateurs.

Par ailleurs, il y a la réalité technologique de l'Internet, qui présente trois caractéristiques importantes :

— mémoire illimitée du web. Contrairement à ce qui était le cas dans le passé, des informations et des photos peuvent, en principe, être conservées éternellement sur l'Internet;

— duplication illimitée de l'information. L'information et les photos sont de plus en plus dupliquées dans des archives, « *caches* », « *mirrors* », ou par d'autres utilisateurs (sur des blogs, des forums, par exemple). Même si un site web efface l'information, il est fort probable qu'elle soit déjà présente ailleurs;

— collecte de l'information; il est aisé de rassembler des informations très dispersées. L'on oublie que le scannage et la collecte de données n'ont jamais été aussi faciles.

Impact

Les implications sont énormes.

Par exemple :

— des photos prises au temps de la jeunesse folle peuvent être utilisées ultérieurement dans le cadre d'une sollicitation à un emploi,

— les États-Unis ont refusé l'accès à son territoire à un psychologue canadien parce qu'il avait consommé

De heer Geert Somers vertegenwoordigt een advocatenkantoor, Time.lex, dat één van de partners van ISPA is en dat de juridische kwesties behandelt die met de bescherming van persoonlijke gegevens te maken hebben.

Privacy paradox

De heer Somers stelt vast dat er een privacy paradox bestaat. Ondanks gevoeligheid van de gebruikers voor privacy geven ze meer en meer privacy weg. Dit gebeurd vrijwillig of onvrijwillig en de gebruikers zijn meestal onbewust van hun impact op hun privacy :

— vrijwillig : « social network » sites (Facebook, Myspace); Youtube, Twitter, blogs ...

— onvrijwillig : via zoekmachines (de zoektermen worden bijgehouden en gelinkt aan de gebruiker, via het scannen van Internet voor profiling doeleinden (bijvoorbeeld Spokeo) en via « third party cookies » en « spyware » die onbewust en onvrijwillig prijsgeven van gedrag.

Anderzijds is er de technologische realiteit van het internet met drie belangrijke punten :

— oneindig geheugen van het web. In tegenstelling tot vroeger kunnen informatie en foto's op internet in principe eeuwig behouden blijven;

— oneindige duplicatie van informatie. Informatie en foto's worden meer en meer gedupliceerd in archieven, « *caches* », « *mirrors* », of gedupliceerd door andere gebruikers (bijvoorbeeld in blogs, forums). Zelfs zou een website informatie verwijderen is de kans zeer groot dat die ondertussen op andere plaatsen reeds bestaat;

— samenbrengen van informatie; zeer verspreide informatie kan gemakkelijk bij elkaar gebracht worden. Mensen vergeten dat scannen en verzamelen van gegevens gemakkelijker dan ooit is geworden.

Impact

De impact daarvan heeft verregaande implicaties.

Bijvoorbeeld :

— foto's uit de wilde studentenjaren kunnen later gebuikt worden in het kader van een sollicitatie,

— een Canadese psycholoog kon geen toegang krijgen tot de VS wegens het gebruik van drugs

de la drogue trente ans plus tôt, information qui était librement accessible sur Internet;

— la commission espagnole de la protection de la vie privée a reçu différentes demandes visant à faire effacer des données gênantes. Par exemple, une recherche sur Google concernant un chirurgien plasticien espagnol a comme résultat un premier lien donnant accès à des publicités et des photos glamour; le deuxième lien concerne par contre une plainte d'une patiente à la suite d'une opération qui a échoué. Des sociétés telles que Google mettent la disponibilité de l'information sur le même pied que sa pertinence alors qu'il va de soi que ce n'est pas forcément le cas du point de vue de l'utilisateur.

Il existe à présent des services commerciaux qui se chargent d'améliorer la réputation en ligne; on peut se demander dans quelle mesure la vérité historique peut parfois être falsifiée.

Réglementation relative à la protection de la vie privée

M. Somers insiste sur le fait que la loi sur la protection de la vie privée de 1992 concernait surtout le traitement des données à caractère personnel dans des bases de données qui étaient toutefois relativement contrôlables et tenues à jour de façon centralisée. Cette possibilité de contrôle et cette centralisation ne sont plus d'actualité dans le contexte de l'Internet.

Les questions suivantes se posent à présent :

— le délai de conservation « pertinent » qui est limité pour les données recueillies conformément à la législation relative à la protection de la vie privée est-il applicable à l'Internet ?

— *quid* de la diffusion de données au moyen de forums, de blogs, de Twitter, d'anciennes archives ?

— existe-t-il un droit de consultation et de correction, un droit d'effacement, un point de contact ?

— qu'est-ce que le « traitement » de données, qui est le « responsable pour le traitement », quel est le point de contact ?

— aspect international : les collecteurs de données établis à l'étranger, les régimes plus souples.

Droit à l'oubli

Le droit à l'oubli est déjà ancré en partie dans la loi relative à la protection de la vie privée de 1992 et est loin d'être nouveau. Il existait déjà et était en tout cas reconnu dans la jurisprudence et la doctrine. On peut donc parler d'une reconnaissance explicite du droit à l'oubli.

30 jaar geleden; informatie die op internet terug te vinden was;

— de Spaanse privacy commissie heeft verschillende aanvragen tot verwijdering van gênante gegevens gekregen. Zo heeft een Spaanse plastisch chirurg in de zoekresultaten van Google een eerste link met reclame en glamourfoto's maar de tweede link gaat over claim van een patiënte wegens een mislukte operatie. Voor maatschappijen zoals Google staat de beschikbaarheid van informatie gelijk met de relevantie van de informatie terwijl dit uiteraard vanuit de standpunt van de gebruiker het niet per se het geval is.

Commerciële diensten bestaan nu voor het verbeteren van online reputatie waarvan men de vraag mag stellen in hoeverre dat daar soms de historische waarheid vervalst kan worden.

Privacyregelgeving

De heer Somers benadrukt het feit dat de privacywet van 1992 vooral gebaseerd was op het verwerken van persoonsgegevens in databanken die echter vrij controleerbaar waren en op gecentraliseerde wijze werden bijgehouden. Die controleerbaarheid en die centralisering zijn geen elementen meer die toepassing vinden in het context van internet.

De volgende vragen rijzen nu :

— is de beperkte « relevante » bewaartermijn voor gegevens toepasbaar op internet ?

— wat met verspreiding van gegevens via forums, blogs, Twitter, oude archieven ?

— bestaat er een recht van inzage en correctie — recht van verwijdering ? Aanspreekpunt ?

— wat is « verwerking » van gegevens, wie is de « verantwoordelijke voor de verwerking », aanspreekpunt ?

— internationaal aspect : collectors gevestigd in buitenland, soepeler regimes.

Recht op vergetelheid

Het recht op vergetelheid is reeds gedeeltelijk ingebouwd in de privacywet 1992 en is zeker niet nieuw. Het bestond al en was zeker erkend in de rechtspraak en de rechtsleer. Er is dus een expliciete erkenning van het recht op vergetelheid.

Dans le contexte du droit pénal, un détenu ou un ancien détenu a le droit de ne pas être poursuivi par son passé. Les principes qui sous-tendent ce droit se basent sur les principes relatifs à un procès équitable (CEDH), sur la présomption d'innocence et sur le droit à la réinsertion sociale (jurisprudence relative au droit des médias). Cependant, le droit à l'oubli garde des contours vagues et oppose des intérêts contradictoires : d'un côté, le droit à l'information du public, la connaissance de la vérité, la recherche historique et la liberté de la presse et, de l'autre, le respect de la vie privée des délinquants et leur droit à la réinsertion sociale.

L'arrêt Lebach de la Cour constitutionnelle allemande (*Bundesverfassungsgericht*) est un arrêt qui fait date en la matière. Il porte sur un documentaire, relatif à un meurtre, qui a été diffusé par la ZDF et dans lequel plusieurs noms ont été cités. Un des complices présumés, qui avait été acquitté, a porté plainte parce que son nom avait encore été mentionné. Le plaignant a obtenu gain de cause au motif que l'identification n'était pas proportionnelle au but poursuivie. Reste toutefois à savoir dans quelle mesure la jurisprudence relative aux médias peut être étendue à l'Internet.

Le droit à l'image qui s'applique aux photos peut également être invoqué pour faire valoir le droit à l'oubli. On peut également citer l'exemple d'un reportage de RTL TVI qui présentait une reconstitution d'une évasion ayant eu lieu dans un établissement pénitentiaire. Estimant que l'information en question n'était plus pertinente, l'un des intéressés a porté plainte, faisant valoir son droit à l'oubli (« *the right to be left alone* »).

Selon M. Somers, plusieurs questions restent toutefois sans réponse :

— Le « consentement » à l'utilisation et à la diffusion de photos (par exemple, des photos sur lesquelles figurent des amis ou un « ex », des photos de jeunesse compromettantes, etc.) est-il implicite et/ou irrévocable ?

— Qu'en est-il des personnes publiques et des personnes relativement publiques ?

— Ne met-on pas trop l'accent sur la protection contre une utilisation commerciale ?

— Les contours du droit à l'oubli restent vagues.

Profilage

De nombreux éléments sur Internet permettent de réaliser un profilage : les centres d'intérêt déterminés à partir des recherches effectuées dans les moteurs de recherche (à l'aide, notamment, des termes de recherche), les visites enregistrées sur les sites Internet (par le biais de cookies et d'espiogiciels ou « *spyware* »), la

In het strafrechtelijk context heeft een gedetineerde of ex-gedetineerde het recht om niet vervolgd te worden door zijn verleden. De principes die daarachter zijn baseren zich op de principes inzake eerlijke proces (EVRM), vermoeden van onschuld en op het recht op resocialisatie (rechtspraak inzake mediarecht). Maar de contouren van dat recht blijven vaag en er zijn tegengestelde belangen : enerzijds het recht op informatie van het publiek, de waarheid, het historisch onderzoek of de persvrijheid en anderzijds het privé-leven van de delinquenten en hun recht op resocialisatie.

Een mijlpaal arrest is het arrest-Lebach van het Bundesverfassungsgericht waarbij een documentaire was uitgezonden door ZDF over een moord met de vermelding van verschillende namen. *In casu* heeft een medeplichtige die vrijgesproken werd een klacht ingediend omdat zijn naam nog altijd gebruikt werd. Die betrokkene heeft gelijk gekregen omdat de identificatie niet proportioneel was. De vraag blijft echter in hoeverre men de mediarechtspraak kan doortrekken in de internet context.

Het portretrecht voor foto's kan ook gebruikt worden om het recht op vergetelheid te doen gelden. Hier is ook een voorbeeld van een reportage van RTLTVI waarbij een gevangenisuitbraak werd gereconstrueerd en waarbij een klacht werd ingediend door iemand die betrokkene was. Volgens hem was die informatie niet meer relevant en heeft hij door die manier zijn recht op vergetelheid doen gelden (« *the right to be left alone* »).

Maar er blijven volgens de heer Somers nog vragen open :

— is de « toestemming » voor gebruik en verspreiding van foto's (foto's met vrienden, met ex, compromitterende jeugdfoto's..) impliciet en/of onomkeerbaar ?

— wat met publieke en relatief publieke personen ?

— is er teveel nadruk op de bescherming tegen commercieel gebruik ?

— de contouren blijven vaag.

Profiling

De mogelijkheden tot profiling op internet zijn belangrijk via de interesses die men toont in zoekmachines (bijvoorbeeld via zoektermen), door de website gedrag (via cookies, spyware), door het weggeven van gevoelige gegevens (burgerlijke stand, geloof, etc.) en cookies van derde partijen (« *third parties cookies* »)

communication de données sensibles (état civil, convictions religieuses, etc.) et les cookies tierce partie (« *third parties cookies* ») qui permettent un échange d'informations, souvent sans que l'internaute ne sache que ses centres d'intérêt seront communiqués aux tiers concernés. Les possibilités de déterminer le comportement d'un internaute sont à ce point étendues qu'une nouvelle réglementation est en cours d'élaboration au niveau européen pour rendre obligatoire la régulation par les internautes de l'utilisation des cookies. Les internautes devraient avoir davantage leur mot à dire sur les cookies et devraient donner leur consentement plus souvent.

Difficultés

Le « consentement » à l'utilisation de données constitue-t-il encore un critère crucial dans le contexte de l'Internet ?

— Les internautes ne connaissent pas toutes les implications qu'auront leur consentement (par exemple, lorsqu'ils acceptent des cookies ou utilisent des moteurs de recherche).

— Les internautes oublient que malgré le consentement ou la diffusion volontaire et active de données privées ou de photos, la situation n'est pas statique mais évolutive (songeons par exemple aux années folles de la vie estudiantine).

Droit d'effacement ?

Dès lors, faut-il instaurer, sur le plan juridique, un « droit d'effacement » général ? Selon M. Somers, la question est trop simpliste. De plus, il serait difficile d'instaurer un droit à l'oubli/un droit d'effacement distinct étant donné qu'un tel droit est déjà partiellement prévu dans la réglementation relative au respect de la vie privée et qu'il est déjà difficile à appliquer. M. Somers estime que la solution devra venir de la responsabilisation des internautes et de la technique. Il faudra également collaborer davantage avec les fournisseurs de services Internet (FSI) et tenir compte du respect de la vie privée lors de la conception des systèmes (concept de « *privacy by design* »).

Ce concept part du principe qu'à un stade précoce de l'élaboration du traitement de données, on réfléchit à un bon usage des données à caractère personnel, à la nécessité d'utiliser et de protéger ces données. Inclure dès le développement de systèmes la protection des données à caractère personnel et de la vie privée maximalise les chances de succès.

Le FSI est un terme générique qui désigne tant les fournisseurs d'accès à Internet que les fournisseurs de services. Il va de soi que ce domaine est réglementé.

waarmee informatie wordt uitgewisseld en waarvan de gebruiker vaak niet weet dat zijn interesses worden gecommuniceerd aan die derde partijen. Omdat de mogelijkheden tot het volgen van een gedrag van een gebruiker zo enorm zijn is er nieuwe regelgeving op Europees vlak op komst die stelt dat het gebruik van cookies gereguleerd zou moeten worden door gebruikers. Gebruikers zouden meer macht moeten krijgen over cookies en ook meer toestemmingen moeten geven.

Moeilijkheden

Is de « toestemming » tot gebruik van gegevens nog een cruciaal criterium in de internet context ?

— gebruikers kennen de volledige impact van hun toestemming niet (bijvoorbeeld het accepteren van cookies, gebruiken van zoekmachines),

— gebruikers vergeten dat zelf met toestemming of actieve vrijwillige verspreiding van private gegevens of foto's dit geen statisch gegeven maar evolutief (bijvoorbeeld De wilde studentenjaren)

Recht van verwijdering ?

Moet er dan juridisch een algemeen « recht van verwijdering » komen ? de heer Somers vindt dat deze vraag te simplistisch is en ook moeilijk haalbaar zal zijn om een aparte recht op vergetelheid/verwijdering in te voeren omdat het reeds voor een stuk vervat is in de privacyregelgeving en dit reeds moeilijk toe te passen is. De heer Somers meent dat de oplossing zal moeten komen vanuit de responsabilisering van de gebruiker en in de techniek Er moet ook meer samenwerking met de leveranciers van internet diensten (ISP) zijn en voor « *privacy by design* » zorgen.

« *Privacy by Design* » gaat uit van het principe dat er in een vroeg stadium nagedacht wordt over het goede gebruik van persoonsgegevens binnen een organisatie, de noodzaak van het gebruik van deze gegevens en de bescherming ervan. Door al bij het ontwikkelen van systemen privacy en bescherming van persoonsgegevens in te bouwen in technologie is de kans op het succes ervan het grootst.

ISP is een algemeen begrip dat bestaan zowel uit leveranciers van toegang tot internet alsook de leveranciers van diensten. Uiteraard is daar regel-

Selon M. Somers, la responsabilité du fournisseur d'accès à Internet ne peut pas être mise en cause étant donné qu'il ne fait rien de plus que de transmettre de l'information.

M. Bruno Schröder précise qu'il s'exprimera au nom d'ISPA bien qu'il soit par ailleurs directeur technologique chez Microsoft. Il se propose d'exposer l'aspect technologique des applications Internet et des modèles de valorisation commerciale des services proposés. Il ne s'agit en aucune façon d'une recommandation sur ce qui devrait se faire ou être autorisé.

M. Schröder souligne que le droit à l'oubli et le profilage sont des phénomènes très différents et ont des causes et implications très différentes. Les parties prenantes sont également différentes. Aussi, ces phénomènes peuvent-ils être traités de manière totalement indépendante.

Droit à l'oubli

Contrairement aux informations rendues involontairement publiques ou par une organisation, le droit à l'oubli concerne essentiellement des informations rendues volontairement publiques et généralement par un utilisateur individuel. Pour M. Schröder, il est fondamental d'avoir à l'esprit que, quel que soit le mécanisme de publication, la nature d'Internet rend impossible le contrôle de toutes les instances de l'information. La suppression des données ne permet pas de garantir la disparition effective des informations de l'Internet. En effet, l'orateur rappelle qu'Internet a été conçu au départ sur le plan technique pour être « incontrôlable »; le but du jeu étant de mettre en place une infrastructure de communication entre forces armées qui puisse résister à toutes les tentatives de contrôle et de destruction. Il y a au cœur du fonctionnement d'Internet des mécanismes qui en rendent le contrôle centralisé impossible. Si une information se trouve répandue sur Internet, on peut la faire effacer chez le fournisseur de service ou la personne qui est le premier récepteur de l'information mais l'on ne saura jamais avec certitude si cela n'a pas été copié par quelqu'un d'autre. Par exemple, certains services d'archives prennent des vues des pages web à un moment donné et les conservent pour des raisons d'archivage et des raisons historiques. Si la page photographiée est dans un service d'archives, celle-ci pourra resurgir à un moment donné.

Le droit à l'oubli est donc techniquement difficile à contrôler.

La propriété de l'information pose également problème car cette propriété peut être partagée entre plusieurs personnes ayant des opinions différentes sur le droit à l'oubli. Ainsi, il peut exister un conflit dans un couple divorcé au sujet des photos de leur vie commune. De même, les enfants de criminels ont un

geving voor. Volgens de heer Somers kan de leverancier van toegang tot internet niet aansprakelijk worden gesteld omdat hij niet meer doet dan informatie doorgeven.

De heer Bruno Schröder verklaart dat hij zich in naam van ISPA zal uitdrukken, hoewel hij ook technologisch directeur bij Microsoft is. Hij wil een uiteenzetting geven over het technologische aspect van de internettoepassingen en de commercialiseringsmodellen van de aangeboden diensten. Het gaat geenszins om een aanbeveling over wat moet gebeuren of worden toegestaan.

De heer Schröder onderstreept dat het recht op vergetelheid en profilering heel verschillende verschijnselen zijn, met heel verschillende oorzaken en implicaties. De betrokken partijen verschillen ook. Die verschijnselen kunnen dan ook volledig los van elkaar worden behandeld.

Recht om vergeten te worden

Anders dan de informatie die onvrijwillig of door een organisatie publiek wordt gemaakt, behelst het recht om vergeten te worden hoofdzakelijk informatie die vrijwillig publiek is gemaakt, meestal door een individueel gebruiker. Volgens de heer Schröder is het van fundamenteel belang dat men beseft dat, ongeacht het publicatiemechanisme, de aard van het internet het onmogelijk maakt controle te hebben over alle informatiefora. Het verwijderen van gegevens garandeert niet dat de gegevens werkelijk van het internet verdwijnen. Spreker herinnert er immers aan dat het internet bij de start technisch ontworpen werd om « oncontroleerbaar » te zijn; het was de bedoeling een communicatie-infrastructuur tussen strijdkrachten op te zetten die bestand was tegen alle pogingen tot controle en vernietiging. Het internet werkt op basis van mechanismen die centrale controle erover onmogelijk maken. Informatie die op het internet is verspreid, kan men laten verwijderen bij de provider of bij de persoon die er de eerste ontvanger van is, maar men kan nooit met zekerheid weten of het niet door iemand anders is gekopieerd. Bepaalde archiefdiensten bijvoorbeeld maken op een bepaald tijdstip afbeeldingen van webpagina's en bewaren ze om ze te archiveren of om historische redenen. Indien de gefotografeerde pagina zich in een archief bevindt, kan ze op een bepaald ogenblik weer opduiken.

Het recht om vergeten te worden is dus technisch moeilijk te controleren.

De eigendom van de informatie brengt eveneens een probleem met zich, want die eigendom kan worden gedeeld door verscheidene personen met verschillende meningen over het recht op vergetelheid. Er kan bijvoorbeeld een conflict bestaan tussen een gescheiden paar over de foto's van hun gezamenlijk

intérêt à mettre en œuvre un droit à l'oubli; droit qui s'oppose à un droit à l'histoire.

En matière de droit à l'oubli, M. Schröder estime qu'il importe que le législateur s'intéresse à ce sujet et tranche ce conflit car il s'agit fondamentalement d'un problème d'intégration sociale de la technologie et de ses applications. Un parallèle pourrait être fait avec l'éditeur responsable en matière de publication. Qui est responsable de la mise à disposition de l'information et quels sont les critères qui doivent être appliqués à l'effacement ou au droit au maintien de l'information ?

Le profilage

Le profilage est encore plus complexe dans la mesure où il concerne des données relatives à un utilisateur, collectées ou générées automatiquement par une organisation lors de l'utilisation de ses services. Il s'agit essentiellement des données liées au login, nom, âge, adresse, code postal, IP, signature de configuration, aux cookies ou à l'historique comportemental.

Le profilage est au cœur des nouveaux modèles commerciaux sur Internet, basés sur la monétisation des informations collectées au sujet des utilisateurs de services gratuits (Google, Skype, FaceBook, etc.). Au lieu de mettre à disposition des logiciels ou des services Internet en échange d'une redevance, ceux-ci sont mis à disposition en échange d'informations liées à la vie privée. Le fournisseur de services revend de manière directe ou indirecte à des sociétés actives dans le secteur de la publicité ciblée ce qu'il peut extraire des données précitées. Le modèle publicitaire est aujourd'hui le modèle par excellence.

Ces services gratuits remportent un franc succès chez les utilisateurs. Or, le maintien de la compétitivité de ces modèles de monétisation et l'augmentation de leur production ne peut se faire qu'en augmentant l'efficacité du profilage. Il faut par conséquent mieux connaître les utilisateurs que ses concurrents. Ces modèles commerciaux de fournitures de services gratuits sur Internet sont donc invasifs sur le plan de la vie privée. Leur futur et leur compétitivité reposent sur une meilleure connaissance des utilisateurs.

Il faut toutefois reconnaître que ce sont des modèles extrêmement bien adoptés par les consommateurs malgré les politiques de ciblage. Ainsi, Gmail a plusieurs centaines de millions d'utilisateurs et Facebook près de 650 millions.

En conséquence, il existe actuellement une dialectique Internet entre deux modèles « business » : le modèle « Microsoft » par lequel l'utilisateur paie directement l'acquisition d'un logiciel et le modèle « Google » où le service est finalement monnayé par

leven. Kinderen van misdadigers hebben evenzeer belang bij een recht om vergeten te worden; een recht dat tegenover het recht op geschiedenis staat.

De heer Schröder meent dat het belangrijk is dat de wetgever belangstelling toont voor het recht om vergeten te worden en dat conflict beslecht, omdat het fundamenteel om een probleem van maatschappelijke integratie van de technologie en haar toepassingen gaat. De zaak is vergelijkbaar met de verantwoordelijke uitgever van een publicatie. Wie is verantwoordelijk voor het ter beschikking stellen van de informatie en welke criteria moeten worden gehanteerd bij de verwijdering of bij het recht op het handhaven van de informatie ?

Profilering

Profilering is nog complexer, omdat het om gegevens over een gebruiker gaat, die door een organisatie automatisch ingezameld of gegenereerd werden bij het gebruik van haar diensten. Het gaat hoofdzakelijk om data in verband met de log in, naam, leeftijd, adres, postcode, IP, configuratiehandtekening, cookies of de geschiedenis.

Profilering neemt een centrale plaats in in de nieuwe handelsmodellen op internet, die gebaseerd zijn op het te gelde maken van informatie over de gebruikers van kosteloze diensten (Google, Skype, Facebook, enz. ...). In plaats van softwarepakketten of internetdiensten ter beschikking te stellen voor een bijdrage, gebeurt dat in ruil voor informatie uit de persoonlijke levenssfeer. De dienstverlener verkoopt wat hij uit die gegevens kan halen rechtstreeks of onrechtstreeks aan ondernemingen die actief zijn in de sector van de gerichte reclame. Dat reclamemodel is momenteel het belangrijkste.

Die kosteloze diensten kennen heel wat succes bij de gebruikers. De modellen van monetisatie kunnen echter hun concurrentiekracht slechts behouden en hun productie slechts opvoeren door de efficiëntie van de profilering op te voeren. Men moet de gebruikers dus beter kennen dan zijn concurrenten. Die handelsmodellen van kosteloze dienstverlening op het internet zijn dus invasief op het gebied van de privacy. Hun toekomst en concurrentiekracht berusten op een betere kennis van de gebruikers.

Men moet echter erkennen dat de consumenten uiterst meegaand zijn in die modellen, ondanks het beleid van het vormen van doelgroepen. Gmail heeft verscheidene honderden miljoen gebruikers en Facebook bijna 650 miljoen.

Er bestaat nu bijgevolg een internetdialectiek tussen twee « business »-modellen : het « Microsoft »-model, waar de gebruiker de aankoop van een softwarepakket betaalt en het « Google »-model, waar de dienst uiteindelijk te gelde wordt gemaakt aan de hand van

des données personnelles et des informations relatives à la vie privée. L'un des enjeux actuels tient au choix qui va être opéré par les utilisateurs en matière de modèle. Si dans le futur, le modèle « Google » devait être prédominant, il est certain que des sociétés comme Microsoft sont déjà prêtes pour l'adopter.

Dans le modèle de profilage, l'anonymisation des données est utile dans certaines circonstances et peut réduire les risques de transmission d'informations sensibles. Toutefois, l'anonymisation ne réduit pas le profilage car l'un des grands domaines de recherche et d'investissement technologique chez les fournisseurs de telles technologies a précisément trait aux technologies de désanonymisation des données. En effet, les informations que l'on capture ou que l'on mesure sur un utilisateur dans un contexte donné ne sont jamais que des données partielles. L'efficacité du modèle dépend de la précision du ciblage et il est donc fondamental d'arriver à regrouper des éléments ou des assemblages de données dont les critères d'identification sont totalement différents. C'est un champ d'investigation très actif pour le moment. À titre d'exemple, M. Schröder affirme que la combinaison des données relatives à la population belge (soit 10 millions de belges) et à l'espérance de vie (80 ans d'espérance de vie en moyenne), soit 29 200 dates de naissance différentes, ainsi que le nombre de codes postaux (589) permet d'identifier de manière unique n'importe quel belge (soit 0.58 individu en moyenne par combinaison de date de naissance/CP). En ajoutant le critère du sexe, on arrive à 0.29 individu possibles. Cela représente donc trois fois le seuil statistique d'identification d'une personne. La désanonymisation des données est donc un processus facile en sachant que la signature technique du browser se mesure aisément et est unique, à l'instar de la signature hardware du pc.

Il importe donc de déterminer ce qui est généré et ce qui est conservé au sujet de différentes personnes. Différentes protections restent possibles mais aucun mécanisme n'est complet. Il s'agit des mécanismes technologiques de protection de la vie privée tels que la protection contre le « *tracking* » (technologie IE9) ou des mécanismes d'identification qui utilisent une tierce partie certifiant que vous avez bien la caractéristique requise pour l'accès (technologie U-Prove).

La protection fondamentale va toutefois émaner de l'éducation des utilisateurs car, de manière générale, on constate que la majorité des utilisateurs n'ont pas réellement de problèmes avec le profilage et qu'ils sont plutôt intéressés par les informations personnalisées et la publicité ciblée.

Une autre protection émanera de la compétition entre sociétés mais à la condition que les utilisateurs

persoonlijke gegevens en informatie over het privéleven. Een van de huidige uitdagingen draait rond de keuze die de gebruikers zullen maken tussen de modellen. Mocht het « Google »-model in de toekomst gaan overheersen, dan staan ondernemingen als Microsoft ongetwijfeld klaar om het over te nemen.

In het profileringsmodel is het anoniem maken van de data in bepaalde omstandigheden nuttig en kan het de risico's op het overdragen van gevoelige informatie verminderen. Gegevens anoniem maken, vermindert echter de profilering niet, want een van de grote gebieden van onderzoek en investeringen in technologie bij leveranciers van dergelijke technologieën heeft precies te maken met de technologieën van het ontanonimiseren van data. De informatie die men opvangt of die men meet over een gebruiker in een bepaalde context, is immers steeds slechts partiële informatie. De efficiëntie van het model is afhankelijk van de nauwkeurige gerichtheid en het is dus fundamenteel dat men erin slaagt de gegevens of gehelen van gegevens met volstrekt verschillende identificatiecriteria opnieuw samen te brengen. Dat is nu een heel actief onderzoeksgebied. Als voorbeeld haalt de heer Schröder aan dat de combinatie van de data over de Belgische bevolking (10 miljoen Belgen) en over de levensverwachting (gemiddelde levensverwachting van 80 jaar), wat neerkomt op 29 200 verschillende geboortedata, alsook met het aantal postcodes (589), het mogelijk maakt om het even welke Belg op unieke wijze te identificeren (gemiddeld 0.58 individu per combinatie geboortedatum/PC). Wanneer men er het criterium van het geslacht aan toevoegt, komt men tot 0.29 mogelijke individu's. Dat is dus driemaal de statistische drempel om een persoon te identificeren. De ontanonimisering van de data is dus een gemakkelijk proces wanneer men weet dat de technische handtekening van de browser gemakkelijk kan worden gemeten en uniek is, net als de hardware-handtekening van de pc.

Het is dus belangrijk te bepalen wat er gegenereerd en bewaard wordt over verschillende personen. Er blijven diverse beschermingen mogelijk, maar geen enkel mechanisme biedt volledige bescherming. Het gaat om technologische mechanismen voor de bescherming van de privacy, zoals bescherming tegen « *tracking* » (IE9-technologie) of identificatiemechanismen waarbij gebruik wordt gemaakt van een derde partij die waarborgt dat u de vereiste kenmerken voor toegang hebt (U-Prove-technologie).

De fundamentele bescherming zal echter uit de vorming van de gebruikers voortkomen, want algemeen stelt men vast dat de meerderheid van de gebruikers niet echt problemen hebben met profilering en dat ze veeleer belangstelling hebben voor gepersonaliseerde informatie en gerichte reclame.

Een andere bescherming zal ontstaan uit de concurrentie tussen ondernemingen, maar dan op voor-

valorisent leur attachement à la protection de la vie privée. Ce mécanisme d'autorégulation se mettra en place dès qu'un fournisseur d'accès ou de services constatera que des utilisateurs migrent vers un concurrent qui offre une meilleure protection en matière de données personnelles.

Conclusion

Le droit à l'oubli est une problématique publique que la technologie ne peut résoudre. Aucune garantie ne peut être offerte si l'information première a été copiée ailleurs que sur le premier site. Par ailleurs, l'effacement des informations est une solution d'une efficacité relative.

Le profilage est en fait une question de validité de modèle commercial sur Internet. Pour M. Schröder, le fait de considérer comme acceptable le paiement de services avec des données personnelles est finalement un choix de société. Si l'on constate aujourd'hui que les utilisateurs souscrivent massivement au modèle de paiement au moyen d'éléments de vie privée, on ignore toutefois quel sera le modèle internet qu'ils choisiront *in fine*.

L'anonymisation n'est pas une solution efficace car on peut générer des méta-données ou faire application de techniques de « dés-anonymisation ».

Enfin, l'impact de l'adoption des technologies Internet par les entreprises n'est pas économiquement neutre, dans la mesure où cette adoption effective permettrait, selon une étude de l'université de Milan, de créer en Belgique 7 500 entreprises et près de 45 000 emplois dans les trois ans à venir. La non-adoption desdites technologies limiterait la création à 1 500 entreprises et 11 000 emplois.

Un certain nombre de contraintes de protection de la vie privée (*privacy by design*) devraient faire partie des règles de base de la technologie ou des services. L'un des rôles du législateur national ou européen consisterait à définir dans le cadre du « privacy by design » ce qui est acceptable et ce qui ne l'est pas. M. Schröder cite l'exemple du modèle de la banque carrefour de la sécurité sociale qui a déterminé ce que l'administration était en droit de faire en matière d'utilisation de données de sécurité sociale.

*3. Échange de vues*

Mme Turan aimerait avoir des éclaircissements à propos d'une intervention du représentant d'ISPA Belgique, qui affirmait que l'on ne peut pas reprocher à ISPA des erreurs commises par d'autres. Mais à qui peut-on s'adresser dans ce cas ?

waarde dat de gebruikers meer blijk geven van hun gehechtheid aan de bescherming van de privacy. Dat zelfreguleringsmechanisme zal er komen zodra provider of een dienstverlener vaststelt dat gebruikers overstappen naar een concurrent die meer bescherming inzake persoonsgegevens biedt.

Conclusie

Het recht om vergeten te worden is een publieke problematiek die de technologie niet kan oplossen. Er zijn geen garanties mogelijk wanneer de eerste informatie van de eerste site naar elders is gekopieerd. Overigens is het verwijderen van de gegevens maar een relatief efficiënte oplossing.

Eigenlijk is profilering een kwestie van validiteit van het handelsmodel op internet. Voor de heer Schröder is het de samenleving die moet beslissen of zij het betalen van diensten met persoonlijke gegevens al dan niet aanvaardbaar acht. Vandaag stelt men weliswaar vast dat gebruikers het model van betaling met gegevens uit het privéleven massaal onderschrijven, maar we weten niet voor welk internetmodel zij uiteindelijk zullen kiezen.

Anonimisering is geen efficiënte oplossing, omdat men metagegevens kan genereren of technieken van « ontanonimisering » kan toepassen.

De impact van het gebruik van internettechnologieën door ondernemingen is economisch niet neutraal, omdat het effectieve gebruik het volgens een onderzoek van de universiteit van Milaan mogelijk maakt om de komende drie jaar in België 7 500 ondernemingen op te richten en bijna 45 000 banen te scheppen. Wanneer ze die technologieën niet gaan toepassen, zullen slechts 1 500 ondernemingen worden opgericht en de 11 000 banen worden gecreëerd.

Een aantal verplichtingen inzake de bescherming van de privacy (*privacy by design*) moeten deel uit maken van de basisregels van de technologie of de diensten. Één van de rollen van de nationale of Europese wetgever bestaat erin in het raam van de « *privacy by design* » te bepalen wat aanvaardbaar is en wat niet. De heer Schröder geeft het voorbeeld van de kruispuntbank van de sociale zekerheid, die bepaald heeft wat de administratie mocht doen inzake het gebruik van gegevens van de sociale zekerheid.

*3. Gedachtewisseling*

Mevrouw Turan vraagt verduidelijking over de tussenkomst van ISPA, waar zij stelden dat ISPA moeilijk kon worden opgezadeld met blunders van anderen. Bij wie kan men dan wel terecht ?

En ce qui concerne le droit à l'oubli, l'intervenante a surtout compris que cela n'était pas toujours techniquement possible. La meilleure solution serait de responsabiliser les utilisateurs. L'intervenante pense ici, principalement, aux jeunes et à l'enseignement. À quelle formule les intervenants pensent-ils principalement lorsqu'ils parlent de sensibilisation et de responsabilisation ? À quel propos les jeunes utilisateurs doivent-ils être informés en particulier et quelles dispositions pourrait-on prévoir en matière de sécurité ?

M.Courtois souhaite obtenir des informations complémentaires sur l'ISPA et sur les initiatives législatives prises dans les pays voisins.

M. Mahoux précise que les prochaines auditions seront consacrées à l'audition d'un juge d'instruction spécialisé en la matière et du Centre d'informatique et Droit (CRID). Il y aura une approche théorique sur l'ensemble des législations en la matière et une approche plus pratique avec l'audition d'un juge d'instruction.

Mme Turan abonde dans ce sens et souligne que le Parlement néerlandais a déjà une nette longueur d'avance. En outre, il s'agit ici d'une problématique internationale qui doit également être abordée dans les forums internationaux. Où en est l'Europe dans ce domaine ?

Mme Faes se pose des questions de fond.

L'intervenante souhaite savoir comment fonctionne exactement le profilage dans le service Gmail. Les courriels expédiés sont souvent accompagnés de publicités. Le profilage ne devrait-il pas être mieux réglé ?

L'intervenante se réfère également aux informations concernant Streetview, et plus exactement à la collecte involontaire de données de communication. Comment ce système fonctionne-il ? Le représentant de Google pourrait-il fournir des précisions sur ce point ?

Quelle est la meilleure méthode pour protéger les utilisateurs ?

La législation actuelle qui s'applique aux blogs et forums est-elle suffisante ou doit-elle être renforcée ? *Quid* si ces blogs diffusent, par exemple, des propos racistes ou haineux ?

*Quid* de la réglementation actuelle relative à la durée de stockage de données ?

Enfin, l'intervenante se réfère aux délits de presse, qui sont soumis à un système de responsabilité en cascade. Faut-il instaurer un système comparable pour l'Internet ?

Wat betreft het recht om vergeten te worden, heeft spreekster vooral begrepen dat dit technologisch niet altijd mogelijk is. De beste bescherming zou zijn de gebruikers te responsabiliseren Spreekster denkt hierbij vooral aan jongeren en onderwijs. Waaraan denken sprekers vooral bij sensibilisering en responsabilisering ? Waarover moeten jonge gebruikers vooral worden ingelicht en welke veiligheidsvoorschriften kunnen worden ingebouwd ?

De heer Courtois wenst bijkomende informatie over ISPA en de wetgevende initiatieven in de buurlanden.

De heer Mahoux verklaart dat de volgende vergaderingen gewijd zullen zijn aan hoorzittingen met een onderzoeksrechter die in deze aangelegenheid gespecialiseerd is, en met het *Centre d'informatique et Droit* (CRID). Er zal dus een meer theoretische uiteenzetting zijn over de verschillende wetgevingen, en een meer praktische benadering door de onderzoeksrechter.

Mevrouw Turan sluit hierbij aan en stipt aan dat het Nederlands parlement al heel wat verder zit. Bovendien gaat het hier om een internationaal probleem dat ook op internationale fora dient te worden aangekaart. Hoever staat men in Europa op dit vlak ?

Mevrouw Faes heeft enkele inhoudelijke vragen.

Met betrekking tot de profiling, wenst spreekster te weten hoe dit juist in zijn werk gaat bij Gmail. Vaak wordt reclame gelinkt aan de mails die worden verstuurd. Moet de *profiling* niet beter worden geregeld ?

Verder verwijst spreekster naar de berichtgeving over de streetview, namelijk het onopzettelijk verzamelen van inhoudelijke communicatiegegevens. Hoe is dit in zijn werk gegaan ? Kan de vertegenwoordiger van Google dit even verduidelijken ?

Wat is de beste manier om de gebruikers hiertegen te beschermen ?

Volstaat de huidige wetgeving voor blogs en fora of moet deze worden verstrengd ? Wat bijvoorbeeld als op die blogs racistische en haatdragende informatie wordt verspreid ?

Wat met de huidige regeling met betrekking tot de duur van gegevensopslag ?

Ten slotte verwijst spreekster naar de drukpersmisdrijven, waar een cascadesysteem bestaat op het vlak van aansprakelijkheid. Moet er voor het internet een gelijkaardig systeem worden ingebouwd ?

M. Van Rompuy se réfère au « droit à l'oubli » et à la force contraignante de ce droit. Si ce droit venait à être introduit en Belgique ou en Europe, quelle serait la juridiction compétente ? Quel est le point de vue des intervenants en la matière ? Estimera-t-on que cette réglementation n'est pas applicable, étant donné que les serveurs sont hébergés hors de l'Europe par exemple ? Les instances belges et européennes ont-elles malgré tout un moyen d'imposer l'intégration de certains systèmes, par exemple via les fournisseurs d'accès internet ?

Il va de soi que ledroit à l'oubline peut être absolu, étant donné que l'Internet est aux mains d'une multitude d'acteurs. Il serait toutefois envisageable d'utiliser des systèmes comparables à Google, qui effaceraient toutes les informations relatives à un mot clé donné. Cela doit donc aussi pouvoir se faire de manière automatisée.

M. Mahoux a le sentiment, à l'issu des exposés, que les orateurs estiment qu'il est difficile de légiférer dans un secteur où la technologie aura toujours une longueur d'avance. Les différents orateurs semblent affirmer que le droit à l'oubli ou l'anonymatisation des données ne pourront jamais être parfaits. Or, M. Mahoux estime qu'il convient toutefois de progresser dans ces problématiques et ce d'autant plus qu'une société comme Microsoft est prête à changer de « *business mode*l » si nécessaire.

Par rapport à Google, M. Mahoux demande quelle est la loi applicable et à quelles autorités judiciaires la société répond-t-elle ? Quel est le processus et en fonction de quelle législation ?

Par rapport à l'ISPA, M. Mahoux s'interroge quant au statut et à la responsabilité civile et pénale du fournisseur d'accès internet. Ce dernier est-il assimilable aux sociétés comme « Rossel » ou « Corelio » dès lors qu'il véhicule de l'information comme le ferait un organe de presse, même si dans le cas du fournisseur d'accès, il n'existe pas de lien de subordination ?

Enfin, M. Mahoux estime qu'il faudrait à côté du droit à l'oubli et à la dépersonnalisation des données également envisager une troisième voie qui serait la possibilité de prévoir l'utilisation de données mais que dans des conditions spécifiques.

Mme De Vinck précise qu'elle est la coordinatrice de l'ASBL ISPA. L'ASBL regroupe différentes sociétés afin d'améliorer la fourniture des services internet et la société de l'information en Belgique. Concrètement, l'ASBL regroupe en Belgique des sociétés qui ont une liste de prix pour des services du protocole internet. Actuellement, l'ISPA a comme objectif d'informer ses membres, le public et les autorités sur la complexité d'internet et des nouvelles technologies et de définir des positions communes. L'ISPA représente une trentaine de membres comme des fournis-

De heer Van Rompuy verwijst naar « *the right to forget* » en naar de afdwingbaarheid ervan. Indien dit in België of Europees vlak zou worden ingevoerd, welke jurisdictie is dan bevoegd ? Hoe staan de sprekers hier tegenover ? Gaat men zeggen dat deze regeling niet van toepassing is, omdat de servers bijvoorbeeld buiten Europa staan ? Zijn er toch dan toch mogelijkheden voor de nationale of Europese overheid om het inbouwen van bepaalde systemen te verplichten, bijvoorbeeld via de netwerkproviders ?

Het recht om vergeten te worden kan vanzelfsprekend niet absoluut zijn, omwille van het feit dat internet in handen is van een veelheid aan actoren. Men zou wel kunnen werken met systemen, vergelijkbaar met Google, die via een zoekterm alle informatie hierover gaat schrappen. Dit kan dus ook op een geautomatiseerde manier.

De heer Mahoux heeft na de uiteenzettingen de indruk dat de sprekers menen dat het moeilijk is om wetgevend op te treden in een sector waarin technologie altijd een voorsprong zal hebben. De sprekers lijken te bevestigen dat het recht om vergeten te worden of op het anoniem maken van gegevens nooit volledig zal kunnen zijn. De heer Mahoux meent echter dat er vooruitgang moet worden geboekt, temeer daar een bedrijf als Microsoft bereid is om indien nodig van *businessmodel* te veranderen.

Wat Google betreft, vraagt de heer Mahoux welke wet van toepassing is en voor welke gerechtelijke overheid het bedrijf verantwoording moet afleggen. Wat is de procedure en volgens welke wetgeving ?

Wat ISPA betreft, vraagt de heer Mahoux zich af wat het statuut en de burgerlijke aansprakelijkheid is van de internetprovider. Wordt hij gelijkgesteld met vennootschappen als Rossel of Corelio omdat hij net als een persagentschap informatie overbrengt, ook al is er bij een internetprovider geen ondergeschikt verband ?

Ten slotte meent de heer Mahoux dat men naast het recht om vergeten te worden en depersonaliseren van gegevens een derde weg zou moeten bewandelen, met name de mogelijkheid om te voorzien in het gebruik van gegevens, maar alleen onder bepaalde voorwaarden.

Mevrouw De Vinck preciseert dat zij coördinator is bij de VZW ISPA. De VZW verenigt verschillende vennootschappen om internetdiensten en de informatiemaatschappij in België te verbeteren. Concreet verenigt de VZW vennootschappen die een prijslijst hebben voor diensten van het internetprotocol. Het huidige doel van ISPA is het informeren van haar leden, het publiek en de overheid over de complexiteit van het internet en de nieuwe technologieën en gemeenschappelijke standpunten te bepalen. ISPA vertegenwoordigt een dertigtal leden, waaronder in-

seurs de réseaux internet (Belgacom, Telenet, KPN), des hébergeurs d'informations ou encore des sociétés de services comme Microsoft. La question de la responsabilité est complexe car les acteurs sont nombreux et leurs responsabilités sont différentes. ISPA estime qu'il convient d'assimiler les fournisseurs de réseaux aux constructeurs de route de sorte que leur responsabilité devrait être limitée à ce que le réseau soit fonctionnel. L'hébergeur a physiquement l'information et a donc une responsabilité différente car il peut en théorie agir sur l'information.

En outre, il faut s'intéresser aux travaux de la Commission européenne qui a initié une consultation en vue d'une révision de la Directive 95/46 et sur laquelle EURO-ISPA a réagi.

Enfin, Mme De Vinck rappelle que le droit à l'oubli existe déjà mais qu'il devrait être adapté au nouvel environnement internet. Enfin, toute législation devrait être efficace et éviter d'annihiler la compétition qui existe dans le secteur.

M. Schröder attire l'attention des membres du groupe de travail sur le fait que des solutions qui sembleraient adéquates peuvent avoir un sens si l'on ne connaît pas les mécanismes internes et techniques d'internet. Toutefois, elles rateront leurs objectifs. Ainsi, la désanonymisation des données ou la suppression des « cookies » ne régleront pas la problématique du profilage. Des possibilités d'injonction visant à obliger des sites de réseaux sociaux comme Facebook de supprimer des informations pour faire respecter le droit à l'oubli ne seront pas satisfaisantes. Elles peuvent être une composante d'une solution qui devra être plus fondamentale. La responsabilisation de l'utilisateur est à cet égard importante. M. Schröder rappelle à cet égard que les utilisateurs internet sont des jeunes entre dix-huit à vingt-quatre ans et que même 60 % des jeunes de dix à treize ans ont un identifiant internet et un compte sur un réseau social alors que c'est interdit. 60 % des jeunes de dix à treize ans ont donc menti sur leur âge pour avoir accès à un compte. C'est un phénomène où pour la première fois le savoir n'est pas transmis par les anciens car les jeunes ont plus de capacité dans ce domaine que les anciens. On est confronté à une période de quinze à vingt ans; le temps que les jeunes d'aujourd'hui deviennent eux-mêmes parents et puissent transmettre leur savoir à leur enfants. La question est donc de savoir ce que l'on fait au cours de ces quinze ans à venir ?

Microsoft donne ainsi dans les écoles des cours de sécurité et de comportement sur internet et ce en collaboration avec Child Focus. Si il y a trois ans, on visait les deux premières années du secondaire aujourd'hui on vise les deux dernières années du primaire. Il y a aussi un centre Microsoft qui s'intéresse à l'anthropologie du web et qui étudie la

ternetleveranciers (Belgacom, Telenet, KPN), *hosting providers* of nog dienstenbedrijven als Microsoft. Aansprakelijkheid is een ingewikkelde kwestie, omdat er vele actoren zijn met telkens andere vormen van aansprakelijkheid. ISPA meent dat netwerkproviders moeten worden gelijkgesteld met wegenbouwers zodat hun aansprakelijkheid wordt beperkt tot het operationeel houden van hun netwerk. Eenhosting providerherbergt fysiek de informatie en heeft dus een andere aansprakelijkheid aangezien hij in theorie iets met die informatie kan doen.

Bovendien moet men rekening houden met de werkzaamheden van de Europese Commissie, die een consultatieronde heeft opgestart met het oog op een herziening van richtlijn 95/46, waarop EURO-ISPA gereageerd heeft.

Mevrouw De Vinck herinnert eraan dat het recht op vergetelheidreeds bestaat, maar dat het moet worden aangepast aan de nieuwe internetomgeving. Ten slotte moet iedere wetgeving efficiënt zijn en mag zij de mededinging in de sector niet tenietdoen.

De heer Schröder vestigt de aandacht van de leden van de werkgroep op het feit dat sommige oplossingen zinvol kunnen lijken wanneer men de interne en technische mechanismen van het internet niet kent, maar dat zij hun doel zullen missen. Zo zullen het opheffen van de anonimiteit van gegevens of va *cookies* het probleem van de *profiling* niet oplossen. Dagvaardingen om sociale netwerksites als Facebook te verplichten informatie te wissen om het recht op vergetelheid te doen eerbiedigen, zullen niet volstaan. Zij kunnen wel een onderdeel vormen van een oplossing die fundamenteler moet zijn. Het is in dit opzicht belangrijk om de gebruiker op zijn verantwoordelijkheden te wijzen. De heer Schröder herinnert eraan dat vele internetgebruikers jongeren tussen achttien en vierentwintig jaar zijn en dat zelfs 60 % van de kinderen tussen tien en dertien jaar een internet-ID en een account op een sociaal netwerk hebben, terwijl dat verboden is. 60 % van de jongeren tussen tien en dertien jaar hebben dus gelogen om een account te kunnen aanmaken. Voor de eerste maal wordt kennis niet door ouderen doorgegeven en is er een domein waarin jongeren bekwamer zijn dan ouderen. Er komt nu een periode van 15 tot 20 jaar tot de jongeren van vandaag zelf ouders worden en hun kennis aan hun kinderen zullen doorgeven. De vraag is dus wat men zal doen in de komende vijftien jaar.

Zo geeft Microsoft in samenwerking met Child Focus in scholen cursussen over veiligheid en gedrag op het internet. Drie jaar geleden waren zij bedoeld voor de twee eerste jaren van de middelbare school, terwijl zij nu gericht zijn op de twee laatste jaren van de lagere school. Er is ook een afdeling van Microsoft die webantropologie bestudeert, onder meer de manier

manière dont les adolescents construisent leur identité sur internet.

M. Schröder confirme qu'ils appliquent la loi belge et répondent à toutes les demandes des autorités judiciaires. Par ailleurs, en dehors d'une obligation légale, Microsoft a mis en place une ligne spéciale Microsoft. Des personnes de référence dans la magistrature et dans *Federal Computer Crime Unit* ont ainsi la possibilité d'accéder directement au système Microsoft pour introduire des demandes valables de demande d'information sur des comptes MSN ou email. En généralement, la demande est traitée en vingt-quatre heures.

M. Schröder n'a pas connaissance d'un cadre légal satisfaisant à l'étranger car on est au début de l'intégration sociale; les citoyens n'ayant pas encore une bonne compréhension du modèle. On découvre pour le moment les effets de premier ordre alors qu'il y a des effets de second ordre. L'effacement de l'adresse IP est un exemple d'effet de premier ordre. On est au début de la réflexion et il faudra sans doute encore quinze ans.

M. Klimbie précise la structure juridique de Google. Il s'agit d'une société américaine, mais qui respecte évidemment les règles locales et européennes. Il y a un conseiller juridique pour le Benelux, qui suit de près toutes les lois et les règles et qui en discute avec la direction américaine; c'est le système américain qui prévaut, mais Google se conforme aux règles et à la législation locales. C'est une position comparable à celle de Microsoft.

En ce qui concerne la responsabilisation, l'intervenant indique que Google, tout comme Microsoft, diffuse des informations en ligne à l'intention des parents et des enfants afin de les renseigner sur la manière dont ils peuvent naviguer sur Internet en toute sécurité. Dans ce cadre, les Pays-Bas viennent de lancer un *child safety centre* en ligne et la Belgique devrait, cette année encore, créer elle aussi un site identique.

Plusieurs questions ont également été posées au sujet du droit à l'oubli. L'intervenant estime qu'il est capital de donner aux personnes la possibilité de choisir les informations qu'elles souhaitent donner et ce qu'elles veulent en faire. Si elles veulent quitter les services proposés, Google s'efforce de répondre au plus vite à leur demande en veillant à faire disparaître toute trace d'information à leur sujet. C'est une procédure en trois étapes. Elle peut être appliquée si un utilisateur souhaite quitter Gmail par exemple. Il ne subsiste alors aucune information sur l'intéressé, mais celui-ci peut par exemple transférer ses contacts chez un concurrent. Il est important que les utilisateurs aient le choix.

waarop jongeren hun identiteit op het internet opbouwen.

De heer Schröder bevestigt dat dit conform de Belgische wetgeving geschiedt en dat zij ingaan op alle eisen van het gerecht. Bovendien heeft Microsoft zonder enige wettelijke verplichting een speciale Microsoft-lijn opgericht. Contactpersonen van het gerecht en van de *Federal Computer Crime Unit* van de politie kunnen zo rechtstreeks toegang verkrijgen tot het Microsoft-systeem en geldige informatie-aanvragen indienen over msn- of e-mailaccounts. In het algemeen wordt de aanvraag binnen vierentwintig uur behandeld.

De heer Schröder heeft geen weet van een bevredigend wettelijk kader in het buitenland omdat men pas aan het begin staat van de maatschappelijke integratie; burgers hebben nog geen goed begrip van het model. Momenteel ontdekt men de onmiddellijke gevolgen, terwijl er ook secundaire gevolgen zijn. Het wissen van een IP-adres is een voorbeeld van een onmiddellijk gevolg. Men begint het probleem nog maar te vatten en dat zal waarschijnlijk nog vijftien jaar in beslag nemen.

M. Klimbie licht de juridische structuur toe van Google. Het gaat om een Amerikaans bedrijf, maar uiteraard worden de lokale en Europese regels nageleefd. Er is een juridisch adviseur voor de Benelux, die alle wetten en regels doorneemt en bespreekt met de Amerikaanse directie; het Amerikaanse systeem is leidend, maar Google houdt zich aan lokale regels en wetgeving. Deze positie is vergelijkbaar met die van Microsoft.

Met betrekking tot de responsabilisering, antwoordt spreker dat Google, net als Microsoft, online informatie geeft voor ouders-kinderen over hoe ze veilig kunnen internetten. In Nederland werd aldus onlangs het *child safety centre* online gelanceerd en ook in België zou dat dit jaar nog moeten worden opgericht.

Er werden ook meerdere vragen gesteld over het recht om vergeten te worden. Spreker meent dat het cruciaal is dat mensen de keuze hebben over wat ze geven aan informatie en wat ze daarmee willen doen. Als mensen willen weggaan uit de diensten, probeert Google dit zo snel mogelijk te realiseren, zonder dat deze personen iets achter laten. Dit gebeurt in drie stappen. Als men bijvoorbeeld uit Gmail wil stappen, kan dat na deze drie stappen. De betrokkene laat dan niets achter maar kan bijvoorbeeld wel zijn contacten meenemen naar een concurrent. Het is belangrijk dat de gebruikers de keuze hebben.

Le droit à l'oubli est d'application lorsque l'utilisateur a publié quelque chose.

En ce qui concerne l'activité Wifi, l'intervenant se dit conscient du fait que Google a commis en l'espèce une erreur monstrueuse. Il y a eu en effet une erreur d'encodage lors de l'élaboration de « Google streetview ». C'est ainsi qu'on a collecté des données qui n'auraient en fait jamais dû l'être. Ces données n'ont jamais été utilisées. Dès que l'erreur a été découverte, toute l'opération a été stoppée. Plusieurs mesures ont été prises afin d'éviter que cela ne se reproduise dans le futur. Ainsi, on a élaboré un système « privacy by design » qui permet de tester tous les produits à l'aune du critère de respect de la vie privée avant leur diffusion.

En ce qui concerne le profilage, l'intervenant souligne que Google ne vend pas de données à caractère privé à des tiers. La société n'a d'ailleurs absolument pas l'intention d'utiliser des données relatives à des individus; le but n'est pas de recueillir des informations individuelles spécifiques. Dans un mail ayant pour objet l'Italie par exemple, des informations peuvent être jointes au sujet de la location de maisons de vacances dans ce pays. Si l'utilisateur ne souhaite pas recevoir ce complément d'informations, il suffit qu'il le signale. Il a donc le choix. C'est là un aspect capital. Google part du principe que l'utilisateur est demandeur de ces informations publicitaires pertinentes mais, en fait, celui-ci a le choix.

## C. Audition du 11 mai 2011

*1. Exposé de M. Luc Beirens, chef de service de la Federal Computer Crime Unit (FCCU)*

Respect de la vie privée : généralités

M. Beirens rappelle que tant l'article 8 de la CEDH que l'article 22 de la Constitution consacrent le droit au respect de la vie privée, c'est-à-dire le droit d'une personne de mener sa vie comme elle l'entend sans contrôle, ingérence ou entrave de la part d'une autorité publique, d'un employeur, d'organisations ou de personnes. Il ne peut y avoir d'ingérence dans l'exercice de ce droit que pour autant que celle-ci soit autorisée par la loi.

En réalité, la protection de la vie privée est garantie par :

— l'instauration d'interdictions de contrôle (inviolabilité du domicile, secret de la correspondance, interdiction de prendre connaissance de l'existence ou du contenu de données télécoms);

Het recht om vergeten te worden geldt als de gebruiker iets heeft gepubliceerd.

Wat betreft het Wifi-gebeuren, is spreker zich bewust van het feit dat Google hier een ontzettend domme fout heeft begaan. Er is een coderingsfout gemaakt bij het maken van « Google streetview ». Daardoor zijn gegevens verzameld die eigenlijk nooit mochten zijn verzameld. Die gegevens zijn nooit gebruikt. Zodra de fout werd ontdekt, werd ze ook stopgezet. Een aantal maatregelen werden genomen om dit in de toekomst te voorkomen, zoals « *privacy by design* », waarbij alle producten op privacy worden getest alvorens ze de deur uitgaan.

Wat betreft de profilering, onderstreept spreker dat Google geen privégegevens aan derden verkoopt. Zij willen trouwens helemaal geen gegevens van individuen gebruiken; het gaat niet om het verzamelen van specifieke individuele informatie. Er kan bij een mail met als onderwerp « Italië » bijvoorbeeld informatie worden meegestuurd over het huren van vakantiehuizen in Italië, maar men kan dit ook vermijden door te kennen te geven dat men dit niet wil. De gebruiker heeft dus de keuze en dat is cruciaal. Google gaat ervan uit dat de betrokkene deze relevante reclame wil, maar de gebruiker heeft de keuze.

## C. Hoorzitting van 11 mei 2011

*1. Uiteenzetting door de heer Luc Beirens, Directeur* Federal Computer Crime Unit *(FCCU)*

Privacy in het algemeen

De heer Beirens herinnert eraan dat zowel artikel 8 van het EVRM als artikel 22 van de Grondwet een recht op privacy bepalen. Het is een recht van een persoon om zonder controle, inmenging of hinder van overheid, werkgever, organisaties of personen, zijn leven te leiden zoals hij wil. Het is ook zo dat een aantasting van privacy slechts toegestaan is voor zover dit wettelijk is toegestaan.

De privacy wordt in werkelijkheid beschermd door :

— het opleggen van verboden op toezicht (onschendbaarheid van de woning, het briefgeheim, verbod op kennisname van het bestaan of inhoud van telecomgegevens);

— l'instauration d'obligations lors du traitement de données à caractère personnel ou lors de la publication de données.

Les infractions à la législation sont évidemment passibles de sanctions. M. Beirens souligne qu'il faut toutefois donner à la police les moyens d'enquêter sur les faits punissables.

Il souligne également que la protection de la vie privée est liée aussi à l'identité d'une personne. On constate de plus en plus souvent que les personnes qui créent un profil sur Internet sont victimes d'une usurpation d'identité. Il va sans dire que cela a un effet direct sur la protection de leur vie privée. Cela signifie que, si l'on veut garantir à une personne le respect de sa vie privée, on doit aussi pouvoir garantir le respect de son identité et pouvoir, si nécessaire, faire disparaître les fausses informations figurant sur Internet. À cet égard, il s'agit non seulement d'exercer le droit à l'oubli mais aussi de supprimer des informations calomnieuses.

Principales tendances

M. Beirens a relevé plusieurs faits majeurs qui ont un effet sur la vie privée :

— l'utilisateur est mobile en ce qu'il utilise davantage les smartphones dont les données ne figurent plus sur l'ordinateur familial mais sont aujourd'hui disséminées sur Internet;

— il y a un transfert progressif des informations vers le nuage de sorte que celles-ci sont de plus en plus tenues à jour par le fournisseur d'accès;

— les types de données se diversifient;

— il y a une géolocalisation des applications, l'objectif étant de pouvoir offrir des services en fonction de la localisation de l'utilisateur. Les fournisseurs de services vont donc aussi tenir ces informations à jour pour pouvoir améliorer leurs produits. Le problème est que la plupart des utilisateurs ignorent quelles données sont tenues à jour et pendant combien de temps;

— il faut aussi être conscient du fait que tous les échanges sur twitter sont stockés pour toujours;

— un nombre croissant de fournisseurs de services sont établis à l'étranger et possèdent des plateformes sur lesquelles d'autres développeurs peuvent installer des applications complémentaires. Le risque est que ces développeurs ne soient pas toujours contrôlés par les fournisseurs en question. Ainsi, Facebook ne contrôle pas tous les développeurs ayant ajouté une sous-application et ne sait donc pas exactement à quoi servent toutes ces nouvelles applications. Dans la majorité des cas, elles ont simplement été écrites dans

— het opleggen van verplichtingen bij de verwerking van persoonlijke gegevens of bij publicatie van gegevens.

Inbreuken op de wetgeving zijn uiteraard strafbaar. De heer Beirens benadrukt dat de politie wel de middelen moet krijgen om de strafbare feiten te kunnen onderzoeken.

Hij benadrukt tevens dat privacy ook te maken heeft met de identiteit van een persoon. Men stelt meer en meer vast dat de personen die een profiel op het internet aanmaken slachtoffer worden van een identiteitsdiefstal. Dit heeft natuurlijk onmiddellijk een impact op hun privacy. Het is dus van belang dat, als de privacy gegarandeerd moet worden, men ook de identiteit van een persoon moet kunnen garanderen, en indien nodig, valse informatie te kunnen verwijderen van het internet. Hierbij gaat het niet alleen om een recht op vergetelheid uit te oefenen maar ook lasterlijke informatie te verwijderen.

Belangrijke trends

De heer Beirens meldt een aantal bevindingen die een impact hebben op de privacy :

— de mobiliteit van de gebruiker die meer gebruik maakt van smartphones waarvan de gegevens niet meer thuis op de computer staan maar die nu verspreid staan op internet;

— de informatie verschuift meer en meer naar de « *cloud* » (« de wolken ») en wordt daardoor meer en meer door de provider bijgehouden;

— diversificatie van datatypes;

— de geolokalisatie van toepassingen die als doel hebben diensten te kunnen aanbieden naar gelang de lokalisatie van de gebruiker. Bijgevolg gaan de dienstenleveranciers ook die informatie bijhouden om hun producten te kunnen verbeteren. Het probleem is dat de meeste gebruikers niet weten welke gegevens bijgehouden worden en voor hoelang;

— men moet ook beseffen dat alles dat wordt « getwitterd » voor de eeuwigheid wordt opgeslagen;

— steeds meer dienstenleveranciers zijn in het buitenland gevestigd en hun platformen bieden de mogelijkheid voor andere ontwikkelaars om bijkomende toepassingen (« *applications* ») te gaan schrijven. Het risico ligt in het feit dat deze ontwikkelaars niet altijd gecontroleerd worden door de degene die het platform aanbiedt. Zo gaat Facebook geen controle uitvoeren van alle ontwikkelaars die een sub application hebben toegevoegd en weet dus ook niet met zekerheid wat die applicaties doen. Vaak is het zo dat

le but d'entrer dans le profil d'un utilisateur final et de toucher aux données privées;

— la traçabilité devient difficile en raison du passage d'adresses IPv4 à des adresses IPv6;

— on constate que toutes les nouvelles applications s'appuient sur de vieux systèmes d'identification (nom de l'utilisateur et mot de passe); à voir jusqu'où vont les cybercriminels, on peut dire que ces systèmes sont dépassés depuis longtemps.

Pressions sur la vie privée

Différents facteurs portent de plus en plus atteinte à la vie privée.

Le principal danger a pour origine la personne elle-même qui divulgue ses données sur Internet (sur Facebook, par exemple). L'on exprime toujours davantage ses sentiments et son état émotionnel. Il s'agit de données intéressantes pour des criminels qui comptent exercer un chantage ou recourir à la fraude. Une personne qui déclare être « à la recherche d'une nouvelle partenaire », ne tarde généralement pas à recevoir des propositions de femmes étrangères, qui sont une incitation à l'escroquerie.

M. Beirens s'étonne également du genre de photos que certains utilisateurs postent sur Internet, non seulement d'eux-mêmes mais aussi d'amis. Ces derniers ignorent généralement qu'ils figurent sur Internet vu que la publication de ces photos se fait souvent sans qu'ils aient créé leur propre profil. En fait, toutes ces données sont privées et elles sont fréquemment utilisées pour sécuriser un compte Internet. En effet, si l'on oublie son mot de passe, on est invité à répondre à une question spécifique concernant par exemple le nom de sa mère ou de son chien. Si ces données privées sont déjà disponibles dans un profil, elles peuvent être utilisées par des cybercriminels. D'après M. Beirens, les gens oublient que ce type d'informations sert aussi à protéger leur vie privée.

L'évolution qui a vu les données se retrouver sur Internet est par exemple illustrée par le fait qu' « Office » est à présent proposé en ligne dans l'environnement Microsoft de « Windows Live » de sorte que les informations se trouvent sur le compte Internet. Il ne faut donc plus s'introduire dans un pc (*hardware*), mais il suffit d'entrer dans un compte Internet.

Grâce à une application telle que « Foursquare », il est possible de découvrir (via la téléphonie mobile ou un ordinateur portable) qui propose des offres spéciales dans les environs de l'endroit où l'on se trouve, où se trouvent ses amis , ou de signaler où l'on se trouve soi-même. En outre, d'autres personnes fournissent des

die applicaties gewoon geschreven worden om binnen te geraken in een profiel van de eindgebruiker en om aan de private data te geraken;

— traceerbaarheid wordt bemoeilijkt door de overgang van IPv4 adressen naar IPv6 adressen;

— in alle nieuwe applicaties ziet men dat ze allen terugvallen op oude identificatiesystemen (gebruikersnaam en paswoord); dit is allang voorbijgestreefd als je ziet hoe ver cybercriminelen staan.

Privacy onder druk

Privacy wordt meer en meer aangetast door verschillende factoren.

Het grootste risico komt van de persoon zelf die zijn gegevens vrijgeeft op het internet (bv Facebook). Men uit meer en meer zijn gevoelens en zijn emotionele toestand. Dit zijn interessante gegevens voor criminelen die afpersing of fraude willen plegen. Als men aangeeft « op zoek naar een nieuwe partner », dan krijgt men meestal snel aanbiedingen van buitenlandse vrouwen die een aanzet zijn voor oplichting,

De heer Beirens verbaast zich ook over de soort foto's die door gebruikers op internet worden geplaatst, niet enkel van hun zelf, maar ook van vrienden. Deze weten meestal niet dat ze op internet staan, aangezien dit vaak gebeurt zonder dat ze een eigen profiel hebben aangemaakt. Welnu dit zijn allemaal private gegevens die men vaak gebruikt om een internetaccount te beveiligen. Het is namelijk zo dat indien men zijn paswoord vergeten is men een specifieke vraag krijgt over bijvoorbeeld de naam van zijn moeder of hond. Als deze private gegevens reeds beschikbaar zijn in een profiel kunnen ze dan ook door cybercriminelen gebruikt worden. Volgens de heer Beirens vergeten de mensen dat dit soort informatie ook dient om hun privacy te beschermen.

De verschuiving van data naar het internet wordt bijvoorbeeld aangetoond door het feit dat « *Office* » nu aangeboden wordt op internet in de Microsoft omgeving « Windows Live » zodanig dat de informatie op de internet account staat. Het is dus voldoende om in een internet account te geraken en niet meer in een pc (*hardware*).

Met een toepassing zoals « Foursquare » kan men (via een mobiel of laptop) ontdekken wie er, in de omgeving waar men zich bevindt, bijzondere aanbiedingen heeft, waar je vrienden zich bevinden, of melden waar men zich bevindt. Bovendien krijgt men tips van anderen over de plaats waar men zich bevindt. Dat

informations sur l'endroit où l'on se trouve. Toutes ces informations sont divulguées. Mettre à jour sa localisation au moyen d'Internet n'est pas sans risque. Une entreprise internet a lancé la discussion en créant le site «*pleaserobme.com*». «*Please Rob Me*» utilise «Twitter» et «Foursquare» pour chercher des messages d'utilisateurs qui indiquent ne pas être à la maison. Des cambrioleurs potentiels apprécient beaucoup ces indications puisqu'ils obtiennent ainsi une vue d'ensemble des endroits à dévaliser. «Please rob me» a été mis sur pied simplement pour attirer l'attention sur les dangers de ce genre de sites et de la divulgation d'informations. Après le Japon et les USA, l'Europe est à présent elle aussi confrontée à ce type de violations de la vie privée.

Pour les employeurs, il est cependant nécessaire de pouvoir se faire une certaine idée de ce qui se passe sur leurs réseaux. M. Beirens ne va pas se prononcer quant à savoir s'il faut autoriser ou non le recours aux réseaux sociaux dans l'environnement professionnel. Il souligne que les articles 259*bis* et 314*bis* du Code pénal punissent la prise de connaissance ou l'enregistrement intentionnels de télécommunications privées. Il n'y a pas d'exception pour des faits commis dans le milieu professionnel. Bien que les employeurs invoquent actuellement la CCT n° 81, déclarée obligatoire par un arrêté royal du 12 juin 2002, pour contrôler les communications électroniques de leurs employés (du moins dans le secteur privé), M. Beirens estime que cette CCT ne constitue pas une base légale permettant de faire une exception aux dispositions pénales. Les articles pertinents de la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, et de la loi du 13 juin 2005 relative aux communications électroniques, qui contiennent des dispositions pénales, ont un caractère contraignant. Par conséquent, l'on ne peut y déroger par une CCT, de sorte que les dispositions de la CCT n° 81 ne peuvent être appliquées en cas d'incompatibilité avec la loi contre les écoutes et la loi relative aux communications électroniques. En outre, rien n'est prévu pour le secteur public.

De même, les nouvelles technologies utilisées par les fournisseurs de services sont une source de pressions sur la vie privée. Les configurations par défaut appliquées à la protection de la vie privée sont toujours moins strictes. M. Beirens constate que, lors de la création d'un profil sur Facebook en 2005, par exemple, on était automatiquement relié au réseau «*Belgium*». Tous les Belges avaient donné accès aux données qui étaient divulguées pour leur réseau. Les configurations par défaut ont été à ce point étendues en 2010 que la moitié du monde peut accéder aux mêmes données. Il convient dès lors d'être attentif et de définir les configurations appropriées lors de la création d'un profil.

Sur la base de cookies et des caractéristiques technologiques de chaque PC, les opérateurs identi-

zijn allemaal informaties die vrijgegeven worden. Je locatie updaten via internet kent zijn gevaren. Een internetbureau heeft deze discussie aangesneden door de website «*pleaserobme.com*» in het leven te roepen. «*Please Rob Me*» gebruikt «Twitter» en «Foursquare» om naar berichten te zoeken van gebruikers die aangeven niet thuis te zijn. Zo ontstaat een overzicht van leeg te halen locaties. Inbrekers kunnen het zeer waarderen wanneer je aangeeft niet thuis te zijn. «*Please rob me*» was gewoon opgezet om de aandacht van mensen te vestigen op de gevaren van zulke sites en het vrijgeven van informatie. Na Japan en de VS is nu ook Europa geconfronteerd met zulke schendingen van de privacy.

Voor werkgevers is het noodzakelijk voor een stuk kennis te krijgen van wat er gebeurt op hun netwerken. De heer Beirens gaat zich niet uitspreken over het feit of de sociale netwerken al dan niet toegestaan dienen te worden binnen de werksfeer. Hij wijst erop dat artikelen 259*bis* en 314*bis* van het Strafwetboek de opzettelijke kennisname of opname van de inhoud van privételecommunicaties bestraffen. Er wordt ook geen uitzondering gemaakt voor feiten gepleegd in de werksfeer. Alhoewel de werkgevers zich nu beroepen op een CAO 81 die algemeen verbindend werd verklaard door een koninklijk besluit van 12 juni 2002 om elektronische telecommunicaties van hun werknemers te controleren (althans in de privésector) is de heer Beirens van mening dat die CAO geen wettelijke basis is om een uitzondering te vormen op strafrechtelijke bepalingen. Als zijnde strafrechtelijke bepalingen hebben de relevante artikels van de Afluisterwet van 30 juni 1994 en de wet Elektronische Communicatie (WEC) van 13 juni 2005 een dwingend karakter. Bijgevolg kan er niet van worden afgeweken bij CAO, zodat de bepalingen van CAO 81 in geval van strijdigheid met de Afluisterwet en de WEC geen toepassing kunnen vinden. Bovendien is er niets voorzien voor de openbare sector.

De privacy is natuurlijk ook onder druk komen te staan door de nieuwe technologieën die door dienstenleveranciers worden gebruikt. Zo worden steeds lossere «*default settings*» gezet op de privacy. De heer Beirens stelt vast dat men tijdens het opmaken in 2005 van een profiel op Facebook bijvoorbeeld automatisch gelinkt werd met het netwerk «*Belgium*». Alle Belgen hadden toegang gegeven tot de gegevens die vrijkwamen voor hun netwerk. In 2010 zijn de «*default settings*» zo uitgebreid dat de helft van de wereld toegang kan krijgen tot dezelfde gegevens. Men moet dus oplettend zijn en de juiste «*settings*» bepalen wanneer men een profiel aanmaakt.

Op basis van cookies en technologische kenmerken van iedere PC identificeren de operatoren de mensen

fient les utilisateurs, dressent des profils et les associent au comportement de ces utilisateurs sur les sites web. De même, il arrive rarement que les opérateurs procèdent au cryptage des données. La protection de la vie privée de l'utilisateur dépend donc du niveau de sécurisation utilisé par l'opérateur. Manifestement, la Playstation de Sony, qui a été hackée récemment, a été trop peu sécurisée et des données privées de milliers de membres ont ainsi été perdues. Facebook a également divulgué involontairement des données d'utilisateurs. On ne peut donc pas prétendre, selon M. Beirens, que la responsabilité des fournisseurs est inexistante à ce niveau.

Il n'existe actuellement que 4 milliards d'adresses IPv4 (*Internet Protocol version 4*) et elles sont d'ores et déjà épuisées au niveau mondial. Selon les dernières statistiques, il n'y aura plus d'adresses IPv4 disponibles en Europe au début de l'année 2012. Cela signifie que les adresses IP que l'on alloue actuellement devront être élargies d'une manière ou d'une autre. Une nouvelle génération IPv6 est déjà au point, mais les opérateurs et les fournisseurs de services n'y sont pas encore tout à fait préparés. Il faudra donc passer par une période de transition pendant laquelle les opérateurs hébergeront, grâce à un « carrier grade NAT », plusieurs utilisateurs finaux sous une adresse IPv4 unique. La FCCU ne trouvera dès lors sur Internet qu'une adresse IPv4 unique étant donné que le numéro complémentaire associé à l'adresse IP et servant à l'identification ne sera pas transmis. Ce numéro complémentaire ne sera enregistré nulle part sur Internet. Les autorités verront donc leurs capacités de recherche entravées car, dans un avenir proche, lorsqu'un juge d'instruction par exemple demandera à un fournisseur d'accès d'identifier une adresse IP, celui-ci lui fournira une liste de plusieurs dizaines d'internautes.

À cela s'ajoute la menace de voir des cybercriminels commettre des usurpations d'identité en créant de faux profils ou en prenant le contrôle de comptes existants. Les conséquences d'une telle usurpation d'identité sont que vos amis établissent le contact avec votre profil, permettant ainsi au cybercriminel d'établir une fausse communication et d'utiliser vos listes de contacts. L'intrusion d'un cheval de Troie, qui est un logiciel malveillant (« *malware* » en anglais), fait perdre à l'utilisateur tout contrôle de son PC et permet à des criminels d'accéder, par exemple, à des données bancaires. Une guerre ouverte oppose donc, d'une part, l'industrie des antivirus et, d'autre part, les criminels. Ce type de logiciel malveillant analyse d'abord le programme antivirus installé sur le PC et tente ensuite de bloquer les mises à jour.

en gaan ze profielen aanmaken en deze koppelen met het gedrag van de gebruikers op websites. Er is ook heel weinig encryptie van data bij operatoren. De privacy van de gebruiker hangt dus af van het beveiligingsniveau van zijn operator. Sony Playstation dat gehackt is geweest was blijkbaar onvoldoende beveiligd en is zo private gegevens van duizenden leden kwijt geraakt. Facebook heeft ook gegevens van gebruikers onvrijwillig vrijgegeven. Men kan dus volgens de heer Beirens niet beweren dat de verantwoordelijkheid van de providers op dat vlak onbestaande is.

Er bestaan nu slechts 4 miljard Internet Protocol versie 4 (Ipv4) adressen en die zijn nu uitgeput op wereldniveau. Volgens de laatste statistieken zijn in Europa begin 2012 geen Ipv4 adressen meer beschikbaar. Dit wil zeggen dat de IP-adressen die nu gegeven worden op een of andere manier uitgebreid zullen moeten worden. Een nieuwe generatie IPv6 is reeds klaar maar de operatoren en dienstleveranciers zijn er nog niet klaar voor. Men zal dus in een overgangsperiode geraken (« carrier grade NAT ») waarbij de operatoren verschillende eindgebruikers achter een uniek IPv4 adres gaan verbergen. Bijgevolg zal de FCCU op internet maar een enkel IPv4 adres vinden gezien het bijkomende nummer die aan het IP adres gekoppeld wordt en dat voor identificatie doeleinden dient niet meegegeven zal worden. Dat bijkomend nummer wordt nergens op internet opgeslagen. De opsporingscapaciteiten van de overheden zullen dus verhinderd worden gezien men op korte termijn geconfronteerd zal worden met het feit dat een provider een lijst van tientallen gebruikers zal geven wanneer bijvoorbeeld een onderzoeksrechter hem zal vragen om een IP adres te identificeren.

Er is ook de dreiging van cybercriminelen om identiteitsdiefstal te plegen door het creëren van valse profielen of het overname van bestaande accounts. De gevolgen zijn dat de vrienden die u kennen zich met uw profiel gaan verbinden en zo ontstaat valse communicatie met vrienden en wordt er gebruik van de contactenlijsten gemaakt. Door injectie met Trojaanse paarden (malware) verliest men de volledige controle over de pc en kunnen criminelen toegang krijgen tot bijvoorbeeld bankgegevens. Er is dus een strijd tussen de antivirus industrie en de criminelen. Een malware analyseert eerst welk antivirus systeem op de pc staat en tracht de updates te blokkeren.

Initiatives en matière de protection de la vie privée

Face aux menaces précitées, de nouveaux outils de protection de la vie privée, ayant une influence sur le travail de la FCCU, ont été développés.

« Tor », par exemple, est une application qui permet à chacun et chacune d'améliorer le respect de sa vie privée ainsi que sa sécurité sur Internet. La grande variété des utilisateurs Tor renforce la sécurité de l'application. En tant qu'utilisateur Tor, vous vous fondez en effet parmi les autres utilisateurs du réseau Tor. Plus les utilisateurs sont nombreux, au mieux la protection de l'anonymat et de la vie privée est assurée. Les communications en question sont cryptées.

« Freenet » est un autre exemple de réseau où l'utilisateur met une partie de son disque dur à la disposition d'autres utilisateurs Freenet. On ne sait pas ce qui y est sauvegardé et tout est crypté. Il s'agit effectivement d'un formidable outil de protection de la vie privée, mais il est également beaucoup utilisé par des criminels.

Cadre légal actuel

Il n'existe pas de disposition spécifique relative à l'usurpation d'identité. À l'heure actuelle, on se base le plus souvent sur diverses dispositions du droit pénal (articles 210*bis* et 231 du Code pénal) pour poursuivre certaines infractions.

Plus problématique est la mise en ligne sur des blogs de propos relevant de la calomnie ou de la diffamation. Pour le moment, ces faits sont considérés comme un délit de presse pour lequel seule la cour d'assises est compétente. Selon M. Beirens, cette situation n'est pas réaliste et devrait être adaptée.

Le nombre de personnes qui tentent de faire respecter un droit à l'image par le biais d'une procédure civile est également minime. Il ne s'agit pas non plus de faits punissables.

Le problème majeur réside dans l'application territoriale limitée du droit belge. Si le siège de la société est établi à l'étranger ou que le traitement des données a lieu à l'étranger, la loi belge sur la protection de la vie privée ne trouve pas à s'appliquer. Dans ce cas, il faut se tourner vers des opérateurs étrangers.

La réglementation relative à la rétention des données définit le type de données devant être conservées au niveau de la communication afin qu'une identification puisse être effectuée par la suite. Pour qu'une infraction (par ex. le piratage d'un profil déterminé) puisse être constatée, il faut que la FCCU dispose des traces pour pouvoir rechercher l'auteur. M. Beirens regrette que la directive sur la rétention des

Reactie privacy bewegingen

In reactie op deze dreigingen werden er nieuwe *privacy tools* ontwikkeld die ook een impact hebben op het werk van de FCCU.

« Tor » is bijvoorbeeld een applicatie waarmee iedereen in staat wordt gesteld om zijn of haar privacy en veiligheid op internet te verbeteren. De grote variëteit van « Tor » gebruikers maakt Tor veiliger. « Tor » verbergt jou namelijk tussen andere gebruikers van het Tor-netwerk. Des te meer gebruikers des te beter de anonimiteit en de privacy worden beschermd. Deze communicaties zijn gecrypteerd.

« Freenet » is een ander voorbeeld van netwerk waarbij men een stuk van zijn harde schijf ter beschikking stelt van andere Freenet gebruikers. Men weet dus niet wat erop komt en alles is gecrypteerd. Het is een weliswaar fantastische privacy tool maar deze wordt ook veel door criminelen gebruikt.

Situatie wettelijk kader

Er bestaat geen specifieke bepaling voor identiteitsdiefstal. Men gebruikt nu meestal diverse bepalingen van het strafrecht (artikel 210*bis* en artikel 231 Strafwetboek) om bepaalde misdrijven te vervolgen.

Een groter probleem is de problematiek van blogging waarbij sprake kan zijn van laster en eerroof. Voorlopig moet dit als een persmisdrijf beschouwd worden waarvoor enkel het assisenhof bevoegd is. Dit is volgens de heer Beirens niet realistisch en dit zou aangepast moeten worden.

Het aantal mensen die een procedure gaan inschakelen om een portretrecht af te dwingen via een burgerlijke procedure is ook te miniem. Het is ook niet strafbaar.

Het grootste probleem ligt in de beperkte territoriale werking van het Belgisch recht. Als de zetel van de maatschappij als wel de verwerking van de data in het buitenland gebeuren dan is de Belgische privacywet niet van toepassing. Men moet dan terugvallen op buitenlandse operatoren.

De regelgeving met betrekking tot de dataretentie bepaalt welke gegevens op niveau van de communicatie bijgehouden moeten worden om later te kunnen gaan identificeren. Als men een misdrijf wil gaan vaststellen (bv « hacking » op een bepaald profiel) dan moet de FCCU de sporen krijgen om de dader te gaan opzoeken. De heer Beirens betreurt het feit dat de dataretentierichtlijn van 2006 nog altijd niet geïmple-

données de 2006 n'ait pas encore été mise en œuvre. Par ailleurs, cette directive est déjà dépassée car la problématique IPv6 n'a pas pu être prise en compte.

Les méthodes de recherche Internet doivent être étendues. Si les criminels prennent des précautions pour préserver leur vie privée (cacher les preuves ou utiliser un cryptage), la FCCU devrait également être autorisée à utiliser des techniques visant à contourner la sécurité. M. Beirens plaide pour qu'elle puisse par exemple utiliser les méthodes prévues dans la loi MPR. C'est aussi nécessaire pour les enquêtes judiciaires ordinaires.

Faut-il considérer une adresse IP ou une adresse Mac (numéro de série de la carte réseau) comme une donnée privée ? M. Beirens estime qu'il ne s'agit pas d'une donnée à caractère personnel tout simplement parce qu'à terme, la même adresse IP pourra être allouée à plusieurs utilisateurs. De plus, les adresses IP sont en général les adresses des routers, qui n'ont rien à voir avec les personnes elles-mêmes. Une telle adresse peut tout au plus être considérée comme un indice permettant de retrouver une identité.

*2. Exposé de M. Philippe Van Linthout, juge d'instruction*

M. Van Linthout explique que la rétention de données est un outil majeur dans la lutte contre la cybercriminalité mais qu'elle sert aussi à protéger la vie privée. En effet, des dérogations au respect de la vie privée doivent être autorisées, sous le contrôle des juges, pour garantir précisément la protection de la vie privée. En tant que juge d'instruction spécialisé en matière de terrorisme, M. Van Linthout souligne que dans presque tous les dossiers qu'il traite, il est confronté à des matières liées à Internet.

Il précise qu'il ne s'agit en l'occurrence pas seulement de cybercriminalité de haut vol mais aussi d'opérations qu'un enfant d'une dizaine d'années est capable de réaliser à l'aide d'applications disponibles sur la toile. Il cite quelques exemples.

• *www.anoniemsms.be*

L'entreprise, dont le siège semble être établi aux Pays-Bas, permet d'envoyer un sms de manière anonyme à partir d'un site Internet payant. M. Van Linthout fait une démonstration de l'application en envoyant, au nom d'un sénateur, un sms à un autre sénateur. En tant que juge d'instruction, il trouve cela terrifiant. Il est souvent confronté à des dossiers de violence intrafamiliale dans lesquels le partenaire violent se voit offrir une dernière chance et est laissé en liberté sous conditions. L'une de ces conditions peut être une interdiction totale de contacts, en ce

menteerd is. Ze is tevens reeds voorbijgestreefd gezien er geen rekening kon gehouden worden met de IPv6 problematiek.

Internetrecherches-methoden moeten uitgebreid worden. Als de criminelen hun privacy gaan afschermen (bewijs materiaal verstoppen en encryptie gebruiken) zou men ook de FCCU moeten toelaten om technieken te gebruiken met als doel de beveiliging te overschrijden. De heer Beirens pleit ervoor om bijvoorbeeld de methodes voorzien in de BIM wet te kunnen gebruiken. Dit is voor gewoon gerechtelijke onderzoeken ook noodzakelijk.

Is een IP adres of een Mac adres (serie nummer van de netwerkkaart) een privaat gegeven of niet ? De heer Beirens is van mening dat dit geen persoonlijk gegeven is gewoon omdat op termijn hetzelfde IP adres aan verschillende gebruikers toegekend kan worden. Bijkomend zijn meestal de IP adressen de adressen van routers die niets te maken hebben met de personen zelf. Het kan enkel als een spoor naar een identiteit beschouwd worden.

*2. Uiteenzetting door de heer Philippe Van Linthout, onderzoeksrechter*

De heer Van Linthout verduidelijkt dat de dataretentie een belangrijke sleutel is in het gevecht tegen cybercriminaliteit maar ook dient om de privacy te beschermen. Men moet inderdaad toelaten de privacy te schenden onder controle van de rechters om deze juist te beschermen. Als onderzoeksrechter gespecialiseerd in terrorismemisdrijven benadrukt de heer Van Linthout dat hij bijna in elk dossier geconfronteerd wordt met materies gelinkt met internet.

De heer Van Linthout benadrukt het feit dat het hier niet alleen gaat om zeer ingewikkelde cybercriminaliteit maar ook om zaken die kinderen van pakweg 10 jaar kunnen doen met applicaties die op het internet te verkrijgen zijn. Hij haalt een paar voorbeelden aan.

• *www.anoniemsms.be*

Het bedrijf lijkt in Nederland te zijn gevestigd en laat u toe om anoniem een sms te verzenden. De website is betalend. De heer Van Linthout geeft een demonstratie waarbij hij een sms verzendt van de ene senator naar de andere. Als onderzoeksrechter vindt hij dit angstaanjagend. Hij wordt veel geconfronteerd met dossiers van intra-familiaal geweld waarbij een laatste kans aan de partner geboden wordt en waarbij men deze in vrijheid stelt onder voorwaarden. Een van die voorwaarden kan een absoluut contactverbod zijn inclusief sms. Met deze website is het niet uitgesloten

compris les sms. Avec le site web précité, il n'est pas exclu que la femme s'envoie elle-même un sms pour faire arrêter par la police son partenaire, qui affirmera évidemment n'avoir rien envoyé. Et le comble, c'est que l'opérateur n'a aucun moyen de constater qu'il s'agit d'un sms truqué. C'est donc un cas d'usurpation d'identité dans lequel le juge d'instruction est contraint d'investiguer davantage, à la recherche d'autres éléments lui permettant de déterminer qui a effectivement envoyé le sms. De la même manière, il est également possible d'envoyer un courriel anonyme.

M. Van Linthout précise aussi que lorsqu'il cherche à savoir qui a usurpé une identité et a porté atteinte à la vie privée d'autrui, il se retrouve la plupart du temps confronté à une entreprise qui n'est pas établie en Belgique. Et même si cette entreprise a conservé les données, le temps joue contre le juge d'instruction. M. Van Linthout explique qu'une adresse IP (c'est-à-dire une sorte de « jeton ») est attribuée quand on se connecte à Internet. Le fournisseur d'accès retiendra seulement qu'à un moment « x », monsieur « y » a reçu un jeton. C'est alors que le travail de recherche peut commencer.

• *www.stopkinderporno.be*

Toujours au nom de la « liberté d'expression », il existe actuellement des sites Internet qui vous permettent d'accéder à un site en utilisant l'accès d'une autre personne (en « empruntant un jeton »). Il est donc possible de se faire passer pour quelqu'un d'autre sur Internet, mais aussi de s'approprier l'identité d'une autre personne grâce à des systèmes disponibles gratuitement sur Internet (« Tor »,"proxy4free »).

Les recherches effectuées par le juge d'instruction dans le but d'identifier l'auteur de faits répréhensibles peuvent l'amener dans un autre pays, auquel cas il devra attendre plusieurs semaines avant d'obtenir une commission rogatoire. Étant donné que les cybercriminels changent souvent de pays, il est difficile de les localiser.

Toutefois, si un lien peut malgré tout être établi avec l'adresse IP initiale, il est important que le juge d'instruction puisse obtenir les données de l'utilisateur auprès de Belgacom ou de Telenet. Si l'on permet à ces sociétés de tout effacer après six mois, le risque est grand que l'auteur ne soit jamais retrouvé.Il faut donc toujours mettre en balance les intérêts en présence.

En tant que juge d'instruction, M. Van Linthout est confronté quotidiennement à des dossiers ayant trait à « Netlog.be ». Il s'agit d'un forum d'échange de contacts qui s'adresse en particulier aux jeunes. Malheureusement, ce forum est également fréquenté par de nombreux « prédateurs » qui créent de faux profils. Voyant qu'une nouvelle génération maîtrisant

dat de vrouw naar zichzelf een sms verzendt juist om haar partner door de politie te laten arresteren. Die partner zal beweren niets te hebben verstuurd, en het buitengewone is dat de operator zelf niet kan zien dat de sms getrukeerd is. Hier is dus sprake van overname van een identiteit waarbij de onderzoeksrechter eigenlijk gedwongen wordt om verder te investeren naar andere sporen om te bepalen wie de sms effectief verstuurd heeft. Zo kan men ook anoniem een mail versturen.

De heer Van Linthout deelt ook mee dat, als hij wil achterhalen wie een identiteit heeft overgenomen en iemands privacy heeft geschonden, hij meestal terechtkomt bij een bedrijf dat niet in België gevestigd is. Zelfs heeft dat bedrijf de gegevens bijgehouden speelt de tijd in het nadeel van de onderzoeksrechter. De heer Van Linthout legt uit dat men een IP adres toegekend (« soort jeton ») krijgt als men op het internet gaat. De internetprovider gaat gewoon noteren dat op moment x meneer y een jeton heeft gekregen en dan begint het recherchewerk.

• *www.stopkinderporno.be*

Ook omwille van « *Freedom of speech* » zijn er nu websites die u toelaten toegang te krijgen op een site door gebruik te maken van iemand anders zijn toegang (« een jeton lenen »). Men kan zich dus als iemand anders voordoen op het internet maar ook de identiteit van iemand anders overnemen met systemen die gratis op het internet bestaan (« Tor », »proxy4free »).

In zijn zoek naar de dader zal de onderzoeksrechter wellicht in een ander land terecht komen en het zal weken duren vooraleer hij op rogatoire commissie zal kunnen gaan. Gezien de cybercriminelen vaak van land wisselen wordt het moeilijk om deze te kunnen opsporen.

Maar als men toch slaagt een link te maken met het oorspronkelijke IP-adres is het van belang dat de onderzoeksrechter bij Belgacom of Telenet de gegevens van de gebruiker kan verkrijgen. Indien men hen toelaat om na zes maanden alles te wissen dan is de kans groot dat de dader nooit terug gevonden zal worden. Men moet dus altijd een evenwicht van belangen maken.

Als onderzoeksrechter wordt de heer Van Linthout dagelijks geconfronteerd met dossiers van « Netlog.be ». Het is een forum voor jongeren om met elkaar in contact te komen. Helaas zitten daar er ook veel « predatoren » tussen die valse profielen aanmaken. Hij vreest ook dat men meer en meer geconfronteerd zal worden met cybercriminaliteit omdat er een

les nouvelles technologies est en marche, l'intervenant craint aussi que la cybercriminalité devienne de plus en plus fréquente.

• *Skype*

Skype crypte ses communications et utilise la technologie du « Voice over IP ». Dès lors, si une communication est enregistrée conformément aux dispositions de la législation actuelle sur les écoutes téléphoniques, elle ne pourra pas être écoutée par la suite. Notre législation est donc dépassée. La recherche sur réseau implique également une masse importante d'informations où tout n'est pas clairement délimité.

Le juge d'instruction

L'instruction est conduite sous la direction et l'autorité du juge d'instruction, qui doit assurer la manifestation de la vérité et veiller à la légalité des moyens de preuve ainsi qu'à la loyauté avec laquelle ils sont rassemblés. Il doit donc être possible de déroger au respect de la vie privée afin de garantir précisément la protection de la vie privée, d'autant plus que le délai de conservation des preuves n'est que de 6 mois alors que le délai de prescription est de 5 ans (ou de 10 ans en cas de suspension). À défaut, la lutte contre la criminalité est perdue d'avance. Par ailleurs, tout le monde s'accorde à dire qu'un intérêt supérieur peut primer le respect de la vie privée, par exemple en cas de disparition d'un enfant en bas âge.

Il ne faut pas non plus oublier que le juge d'instruction mène l'instruction à charge et à décharge.

M. De Padt se demande jusqu'à quel point il faut renoncer au respect de la vie privée pour des raisons de sécurité.

M. Van Linthout insiste sur la nécessité d'être conscient que les opérateurs conservent déjà beaucoup d'informations à des fins commerciales sans qu'aucune limitation ne leur soit imposée par le législateur. Il faudrait donc aussi donner au juge d'instruction les moyens de lutter contre la criminalité.

L'intervenant déplore également que la Belgique n'ait toujours pas ratifié la convention sur la cybercriminalité signée à Budapest en 2001.

Il tient enfin à souligner qu'en l'occurrence, il ne s'agit pas du contenu de la communication, mais seulement de savoir, par exemple, que telle personne a passé aujourd'hui un appel téléphonique à tel endroit. Le but est simplement de pouvoir établir des liens et de procéder à des identifications. L'intervenant plaide pour que les données en question puissent être conservées dans le respect d'une réglementation

nieuwe generatie die de nieuwe technologieën beheerst op komst is.

• *Skype*

Skype encrypteert zijn communicatie en gaat over die IP (« voice over IP ») zodanig dat als er getapt wordt met de huidige tapwetgeving in feite niet kan afgeluisterd worden. Onze wetgeving is dus voorbijgestreefd. Netwerkzoeking impliceert ook veel informatie waarbij alles niet zo afgebakend is.

De onderzoeksrechter

Hij heeft de leiding en het gezag van het onderzoek. Hij is op zoek naar de waarheid en waakt over de wettigheid van de bewijsmiddelen en de loyauteit waarmee ze worden verzameld. Men moet dus mogelijkheden hebben om in de privacy in te breken om juist de privacy te garanderen. Des te meer als de verjaringstermijn 5 jaar bedraagt (10 in geval van schorsing) maar de bewaringstermijn van het bewijsmateriaal slechts 6 maanden is. Dan is de strijd tegen de criminaliteit verloren. Iedereen is trouwens akkoord dat er een hoger belang kan bestaan dan privacy, bijvoorbeeld als een peuter vermist is.

Men moet ook niet vergeten dat de onderzoeksrechter het onderzoek voert ten laste en ten ontlaste.

De heer De Padt vraagt zich af hoeveel privacy men moet opgeven voor veiligheidsredenen ?

De heer Van Linthout wenst te benadrukken dat men zich moet beseffen dat de operatoren reeds veel informatie bijhouden voor commerciële doeleinden zonder enige beperking door de wetgever. Men zou dus ook de middelen moeten geven aan de onderzoeksrechter om de criminaliteit te bestrijden.

Hij betreurt ook het feit dat België nog altijd niet de conventie tegen cybercriminaliteit (Boedapest 2001) geratificeerd heeft.

Uiteindelijk wil de heer Van Linthout benadrukken dat het hier niet over de inhoud gaat maar enkel over het feit dat men bijvoorbeeld vandaag heeft gebeld op een bepaalde plaats. Het is gewoon om linken te zetten en te identificeren. Hij pleit voor het feit dat deze gegevens bijgehouden kunnen worden met een strikte regelgeving eventueel in analogie met artikel 90*ter* van het Strafwetboek. Het misbruik van deze regel-

stricte, qui pourrait éventuellement s'inspirer de l'article 90*ter* du Code d'instruction criminelle. L'abus de cette réglementation devrait également être punissable. L'intervenant plaide donc pour la conservation des données en question.

*3. Échange de vues*

M. De Padt constate qu'il existe des tensions entre les personnes qui plaident en faveur d'une conservation obligatoire aussi courte que possible des données et la FCCU qui demande un délai plus long de manière à pouvoir dépister les criminels.

M. Beirens ajoute que la majorité des fournisseurs de services conservent d'ores et déjà ces données. Il ne s'agit donc pas d'une obligation supplémentaire. La seule nouvelle obligation concernerait le courrier électronique (qui envoie un e-mail à qui ?). Le contenu de la directive sur la conservation des données n'est pas nouveau.

Mme Turan retient surtout qu'il faut du temps pour que le juge d'instruction puisse recueillir certaines informations contenues dans les réseaux. Elle renvoie à une affaire concrète concernant la disparition, il y a environ trois semaines, d'une Anversoise après qu'elle s'était rendue dans un garage. Étant donné que l'on soupçonne qu'elle aurait eu un rendez-vous via un site de rencontre, on espérait trouver rapidement des pistes par cette voie. Le délai de trois semaines est vraisemblablement beaucoup trop court. L'intervenante reconnaît que, dans de tels cas, on est prêt à renoncer à une grande partie de sa vie privée afin de pouvoir retrouver des parents ou des amis.

L'intervenante a noté quelques cris d'alarme poussés par les deux orateurs. M. Beirens a ainsi surtout insisté sur la nécessité de préciser certaines choses dans l'arrêté royal du 12 juin 2002, dans lequel il subsiste manifestement une zone d'ombre pour le secteur privé et où rien n'est prévu pour le secteur public.

M. Beirens souhaite également que la responsabilité des fournisseurs soit précisée. L'intervenante demande à cet égard si la conservation des adresses IP, dont M. Van Linthout parlait, concerne également les fournisseurs.

M. Van Linthout répond que le marché compte différents acteurs qui pourraient conserver des données.

Premièrement, il y a les fournisseurs d'accès à l'Internet, comme Telenet et Skynet par exemple, qui peuvent contrôler à qui ils ont donné « un jeton ». Parfois, ces derniers sont également les fournisseurs de services de courrier électronique. Ils sont alors aussi les fournisseurs de services. Le problème est que

geving zou eveneens strafbaar moeten zijn. Er is dus een pleidooi voor het bewaren van deze gegevens.

*3. Gedachtewisseling*

De heer De Padt stelt vast dat er een spanningsveld bestaat tussen de personen die pleiten om de gegevens zo kort mogelijk te moeten bijhouden en de FCCU die een langere periode vraagt om aldus de criminelen te kunnen opsporen.

De heer Beirens voegt eraan toe dat de meeste dienstenleveranciers die gegevens reeds nu bijhouden. Het is dus geen bijkomende verplichting. De enige nieuwe verplichting zou de email betreffen (wie zendt een email aan wie ?) De inhoud van de richtlijn over dataretentie is niet nieuw.

Mevrouw Turan onthoudt vooral dat het een hele tijd duurt alvorens de onderzoeksrechter bepaalde informatie van netwerken kan opsporen. Zij verwijst naar een concrete zaak waarbij een vrouw uit het Antwerpse is verdwenen na een garagebezoek een drietal weken geleden. Aangezien het bericht circuleert dat zij via datingsite een afspraak zou hebben gehad, hoopte men aldus snel via deze weg pistes te vinden. Waarschijnlijk is drie weken een veel te korte termijn. Spreekster beaamt dat men in dergelijke gevallen bereid is veel van zijn privacy op te geven om familie of vrienden te kunnen terugvinden.

Spreekster heeft enkele noodkreten genoteerd van beide sprekers. Zo hamerde de heer Beirens vooral op de noodzaak van een wettelijke verduidelijking op het vlak van het koninklijk besluit van 12 juni 2002, waarbij nog een schemerzone blijkt te bestaan voor de private sector en er helemaal niets bestaat voor de publieke sector.

Ook verwacht de heer Beirens verduidelijking op het vlak van de verantwoordelijkheid van de providers. Spreekster vraagt op dat vlak of het bijhouden van de IP-adressen, waarover de heer Van Linthout het had, ook de providers betreft.

De heer Van Linthout antwoordt dat er verschillende spelers zijn op de markt, die gegevens kunnen bijhouden.

Ten eerste heeft men de access providers, die de toegang tot het net verlenen, bijvoorbeeld Telenet en Skynet, die kunnen nagaan aan wie ze « een jeton » hebben gegeven. Soms zijn dit ook de dienstaanbieders bijvoorbeeld van mailservice. Dan zijn ze ook de serviceproviders. Het probleem is dat men vaak met

l'on a souvent affaire à des fournisseurs de services étrangers, tels que hotmail, qui ne collaborent pas vraiment à l'enquête. Dans ce cas, le magistrat instructeur n'obtient pas l'information qu'il recherche parce que l'on passe par l'étranger, alors que le service est effectivement fourni sur le territoire belge et que la communication par courrier électronique s'est faite intégralement sur ce même territoire. Les fournisseurs de services disent en l'espèce que l'enquêteur doit demander les données dans le pays où est établi le fournisseur de services, ce qui dure des mois. Sur le plan économique, il est toutefois fréquent que ces fournisseurs de services adoptent une autre attitude. Un arrêt récent de la Cour de cassation semble indiquer que le fournisseur de services doit collaborer à une enquête belge s'il est actif en Belgique, ce qui n'est que normal. Le chauffeur d'un camion immatriculé à l'étranger, par exemple, doit également fournir toutes les données en cas de contrôle sur le territoire belge.

M. Beirens ajoute qu'il faut recourir à la procédure des commissions rogatoires pour la demande de données à l'étranger et tout ce qui a trait à la conservation de données. Tout cela prend beaucoup de temps.

Concernant la position de l'ISPA, M. Van Linthout souligne qu'il faut toujours tenir compte du fait que les fournisseurs de services ont un intérêt commercial. Le législateur doit veiller à ce que la sécurité nécessaire soit intégrée.

M. Beirens renvoie au délai qui est prévu dans la directive européenne, soit une durée de six mois minimum et vingt-quatre mois maximum. Une étude a été réalisée sur la base des réquisitions qui ont été traitées par la FCCU en 2007 pour le parquet fédéral. Avec un an de capacité de stockage, 66 % de toutes les réquisitions ont pu être traitées, avec dix-huit mois et vingt-quatre mois de capacité de stockage, ce taux est de 85 % et de plus de 90 %, respectivement. L'identification est souvent le début du dossier. Il faut tenir compte du fait que les seules pistes sont celles qui sont trouvées dans le cyberespace, auprès des opérateurs. Il n'est pas possible de trouver des empreintes digitales, un cheveu pouvant être analysé, etc. Si les pistes ne sont pas trouvées chez les opérateurs, il est impossible de monter le dossier en tant que tel. C'est pourquoi la conservation de données est si importante. L'intervenant est favorable à un délai de deux ans. Si l'on veut harmoniser le délai dans l'ensemble de l'Union, il faudrait s'orienter vers un délai d'un an. Il importe également que, dans ce cas, les données demandées soient fournies dans les plus brefs délais (*cf.* arrêté royal). Personne ne conteste d'ailleurs qu'un accès rapide aux données soit accordé dans le cadre d'une enquête. L'intervenant renvoie également aux propos de l'avocat Van Steenbrugge, pour lequel la protection de la vie privée est une matière très importante et qui ne comprend pas pourquoi l'on discute encore de la

buitenlandse serviceproviders te maken krijgt, zoals hotmail, die niet echt meewerken met het onderzoek. De onderzoekende magistraat krijgt dan niet de informatie waar hij op zoek naar is, omdat men via het buitenland gaat, terwijl de service nochtans wel degelijk op het Belgisch grondgebied is aangeboden en de mail zich volledig afspeelt op het Belgisch grondgebied. De dienstverleners zeggen dan dat de onderzoeker de gegevens dient op te vragen in het land waar de serviceprovider is gevestigd. Dat duurt maanden. Op economisch vlak nemen deze serviceproviders nochtans vaak een andere houding aan. Een recent arrest van het Hof van Cassatie lijkt te zeggen dat de serviceprovider dient mee te werken aan een Belgisch onderzoek als hij in België actief is. Dit is ook normaal. Een vrachtwagen met buitenlandse nummerplaat bijvoorbeeld dient ook alle gegevens te verstrekken bij een controle op het Belgische grondgebied.

De heer Beirens voegt eraan toe dat de opvraging van gegevens in het buitenland en alles wat te maken heeft met dataretentie, via de procedure van rogatoire opdrachten dient te gebeuren. Dit neemt heel veel tijd in beslag.

De heer Van Linthout wijst erop dat men niet mag vergeten dat bij de stelling van ISPA steeds rekening moet worden gehouden met het feit dat zij een commercieel belang hebben. De wetgever moet zorgen dat de nodige veiligheid wordt ingebouwd.

Wat betreft de termijn, verwijst de heer Beirens naar de in de Europese richtlijn voorziene termijn, namelijk tussen 6 en 24 maanden. Er is een studie gemaakt op basis van de vorderingen die door de FCCU in 2007 werden behandeld voor het federaal parket. Met één jaar opslagcapaciteit, kon 66 % van alle gedane vorderingen worden opgelost, met achttien maanden opslagcapaciteit 85 % en met vierentwintig maanden meer dan 90 %. De identificatie is vaak het begin van het dossier. Men moet rekening houden met het feit dat hier de enige sporen de sporen zijn die worden gevonden in cyberspace, bij de operatoren. Er is geen mogelijkheid tot het vinden van vingerafdrukken, haar waarop men een analyse kan verrichten, enz. Als de sporen bij de operatoren niet worden gevonden, kan het dossier zelfs niet worden opgestart. Daarom is dataretentie zo belangrijk. Spreker is voorstander van een termijn van 2 jaar. Als men de termijn in de hele Unie wil harmoniseren, lijkt het eerder naar één jaar te gaan. Het is ook belangrijk dat de opgevraagde gegevens dan zo snel mogelijk worden verleend (zie koninklijk besluit). Dat men bij een onderzoek snelle toegang krijgt tot de gegevens, is trouwens door niemand betwist. Spreker verwijst ter zake ook naar de woorden van advocaat Van Steenbrugge, die zich nochtans erg inzet voor de bescherming van privacy, en die niet snapt waarom er nog discussie bestaat rond de dataretentierichtlijn, die eigenlijk een bevestiging is

directive sur la conservation des données, qui est en réalité une confirmation de la situation existante. Il convient bien entendu de protéger aussi les données et de réserver leur accès à un juge d'instruction.

Mme Faes demande si la police dispose des connaissances suffisantes pour traiter des dossiers ayant un rapport avec Internet. Les connaissances sont-elles transmises correctement ?

M. Van Linthout doit constater que dans des dossiers à ce point spécialisés, il faut effectivement disposer de policiers, magistrats du parquet et juges d'instruction maîtrisant la matière. La force de la chaîne toute entière est déterminée par le maillon le plus faible. Le juge présent à l'audience doit également avoir des connaissances en la matière. Aujourd'hui, il reste encore du travail pour atteindre cet objectif. La volonté de l'Europe est d'oeuvrer à la formation dans ce domaine et toutes sortes d'initiatives sont dès lors prises. Il faut partir du principe que chaque policier, chaque procureur, chaque juge d'instruction, chaque juge devrait bénéficier de cette formation. Il est rassurant que, pour l'heure, les avocats ne s'occupent pas vraiment non plus de cette matière.

L'intervenant estime qu'il faut investir dans de bons outils, ce qui n'est pas le cas actuellement. Un rattrapage est nécessaire.

M. Beirens précise que la FCCU compte actuellement trente-trois personnes, et les CCU régionales cent cinquante personnes. Un petit nombre de celles-ci sont du personnel administratif chargé de missions de soutien. Le CCU est à la recherche de personnes intéressées qui travaillent volontiers dans cette matière. Il ne s'agit pas uniquement d'informaticiens. Une formation complémentaire est fournie. Toutefois, la capacité reste insuffisante.

## D. Auditions du 24 mai 2011

*1. Exposés de Mme de Terwangne et M. Van Gyseghem, représentants du CRIDS (centre de recherche informatique, droit et société)*

Mme de Terwangne précise qu'elle traite, depuis plus de vingt ans déjà, la matière de la protection des données à caractère personnel. À ce titre, elle s'était déjà penchée sur le projet de loi qui allait devenir la loi de 8 décembre 1992 alors qu'Internet n'était pas encore entré dans les mœurs (l'Internet s'est répandu en Belgique en 1996). La législation belge actuelle est donc antérieure à tous les nouveaux bouleversements technologiques. Même la Directive 95/46 est encore trop marquée par tout ce qui ressort de l'informatique et moins de ce qui ressort des « réseaux internet ». Au fil du temps, les législations ont donc présenté quelques lacunes. Il ne s'agit pas de bouleverser la législation car elle est a-technologique mais il s'agit de

van de bestaande situatie. Uiteraard dienen de gegevens ook worden beschermd en dient de toegang te gebeuren door een onderzoeksrechter.

Mevrouw Faes vraagt of er op het politieniveau voldoende kennis bestaat om om te gaan met de dossiers die met internet zijn gerelateerd. Is er een goede doorstroming ?

De heer Van Linthout moet vaststellen dat men in zo'n gespecialiseerde dossiers inderdaad een politieman, een parketmagistraat en een onderzoeksrechter moet hebben die de materie kennen. De keten is maar zo sterk als de zwakste schakel. Ook de rechter ter zitting moet kennis hebben van de materie. Vandaag schiet men nog tekort. Het is de wil van Europa om op dat vlak vormend te werken en er worden dan ook allerhande initiatieven genomen. Men moet ervan uitgaan dat elke politieman, elke procureur, elke onderzoeksrechter, elke rechter en elke procureur die opleiding zou moeten hebben. Het is wel een geruststelling dat op dit ogenblik ook de advocaten niet echt bezig zijn met deze materie.

Spreker meent wel dat investeringen in goede middelen nodig zijn. Dit is nu niet het geval. Een inhaalbeweging is nodig.

De heer Beirens verduidelijkt dat de FCCU momenteel drieëndertif personen telt, en de regionale CCU honderdvijftig personen. Een klein aantal personen zijn administratieve personeelsleden voor ondersteuning. De CCU is op zoek naar geïnteresseerde personen die graag werken in deze materie. Het zijn niet allen informatici. Er wordt wel een bijkomende opleiding verschaft. De capaciteit is echter nog onvoldoende.

## D. Hoorzittingen van 24 mei 2011

*1. Uiteenzettingen van mevrouw de Terwangne en de heer Van Gyseghem, vertegenwoordigers van het CRIDS (*Centre de Recherche Informatique, Droit et Société*).*

Mevrouw de Terwangne preciseert dat zij zich al meer dan twintig jaar toelegt op het onderwerp van de bescherming van de persoonsgegevens. In die hoedanigheid bestudeerde zij al het wetsontwerp dat de wet van 8 december 1992 zou worden. Van internet was toen nog geen sprake (internet werd in België verspreid in 1996). De huidige Belgische wetgeving dateert dus van voor alle nieuwe technologische omwentelingen. Zelfs richtlijn 95/46 is nog te veel gericht op alles wat voortkomt uit informatica en minder op wat « internetnetwerken » voortbrengen. In de loop der tijd zijn er dus enkele lacunes in de wetgevingen ontstaan. Het is niet de bedoeling de wetgeving ingrijpend te wijzigen want ze is a-

la compléter face à certains risques comme les techniques de localisation des individus.

Par ailleurs, la technologie est devenue accessible et à la portée des individus mais le contenu aussi qui est mis sur internet devient accessible à un public important. Si notre environnement numérique ne cesse de se modifier, il ne faut toutefois pas être versé dans la technologie pour comprendre cette matière et prendre la mesure de ce qui se passe. Aujourd'hui, il importe toutefois que le choix d'être présent sur Google ou Facebook soit un choix fait en connaissance de cause. En d'autres termes, il convient de dompter les nouvelles technologies et ce d'autant plus que des études démontrent que dans un monde virtuel les individus ne réfléchissent plus de la même manière, sont plus crédules et acceptent plus facilement des violations de leur sphère privée.

À titre d'exemple, Mme de Terwangne rappelle que, lorsqu'on surfe sur un site, de nombreuses données personnelles sont également déposées sur ce site. Ce sont les « traces » (adresse IP, langue, ...) qui sont, selon le navigateur, plus ou moins importantes. Ainsi, les logiciels Microsoft laissent beaucoup d'informations quant à l'internaute et déposent par exemple son adresse mail sur tous les sites qu'il a fréquentés.

L'objectif de Mme de Terwangne est donc de pointer les problèmes qui ont surgi depuis l'application de la loi du 8 décembre 1992.

Évolution de l'Internet

L'évolution d'internet est d'une complexité croissante. Ainsi, il y a ce qu'on appelle le « *cloudcomputing* » (« internet dans les nuages ») qui implique que lorsqu'on dispose d'une adresse Gmail ou d'un agenda sur un site, on ignore en réalité dans quel pays se situe le serveur qui héberge cet agenda ou sa boîte de réception. On se connecte sur internet pour lire ses messages et son agenda mais ceux-ci sont « dans les nuages » car non localisés à un seul endroit mais répartis sur plusieurs serveurs. Des informations sont donc échangées entre différents serveurs pour finalement faire apparaître l'intégralité des informations stockées, ce qui génère un tas de flux entre différents intervenants et qui échappent au contrôle de l'internaute. Alors quelle peut être la réponse juridique à apporter à ce phénomène ?

Rappel des définitions

Il est tout d'abord important de rappeler certains principes et définitions. Ainsi, il convient de distinguer la vie privée de la protection des données. Ce sont deux droits parents mais qui ne se confondent

technologisch, maar wel ze aan te vullen voor bepaalde risico's zoals de technieken voor lokalisatie van personen.

Bovendien is de technologie toegankelijk geworden en binnen ieders bereik, maar ook de inhoud die op internet wordt geplaatst, wordt toegankelijk voor een groot publiek. Ook al verandert onze digitale omgeving voortdurend, men moet geen expert in technologie zijn om die materie te begrijpen en in te zien wat er gebeurt. Momenteel is het echter van belang dat de keuze om op Google of Facebook te staan een bewuste keuze is. Met andere woorden, de nieuwe technologieën moeten in toom worden gehouden want studies tonen aan dat een individu in een virtuele wereld niet meer op dezelfde manier nadenkt, goedgeloviger is en gemakkelijker schendingen van zijn privacy duldt.

Mevrouw de Terwangne herinnert er bijvoorbeeld aan dat wanneer men naar een website surft er veel persoonlijke gegevens op die site achterblijven. Dit zijn « cookies » (IP-adres, taal ...) die naar gelang van de browser, vrij talrijk zijn. Software van Microsoft laat veel informatie over de internetgebruiker achter en plaatst bijvoorbeeld zijn e-mailadres op alle websites die hij heeft bezocht.

Mevrouw de Terwangne wil dus de problemen aanstippen die sinds de toepassing van de wet van 8 december 1992 zijn opgedoken.

Evolutie van internet

De evolutie van internet wordt steeds complexer. Zo is er « *cloudcomputing* » (« internet in de wolken »). Dit houdt in dat, wanneer men een Gmail-adres of een agenda op een website heeft, men in werkelijkheid niet weet in welk land de server zich bevindt waarop de agenda of de inbox in kwestie staan. Men maakt een verbinding met internet om berichten te lezen en de agenda te bekijken, maar die bevinden zich « in de wolken » want ze zitten niet op één enkele plaats maar zijn verspreid over meerdere servers. Informatie wordt dus uitgewisseld tussen verschillende servers waarbij uiteindelijk alle opgeslagen informatie verschijnt. Dit zorgt voor een grote informatiestroom tussen verschillende tussenpersonen en hierover heeft de internetgebruiker geen controle. Wat kan de juridische oplossing zijn voor dit verschijnsel ?

Herhaling van de definities

Het is in de eerste plaats belangrijk een aantal beginselen en definities te herhalen. Zo moet er een onderscheid worden gemaakt tussen privacy en bescherming van gegevens. Het zijn twee verwante

pas. Le but de la législation relative à la protection des données du 8 décembre 1992 vise non pas la vie privée mais l'auto-détermination informationnelle. Cette notion provient d'un arrêt de la Cour constitutionnelle allemande de 1981 qui énonce que chaque individu doit pouvoir faire des choix existentiels et maîtrisés. En l'espèce, un individu doit pouvoir déterminer lui-même les informations qui circulent sur lui. C'est l'idée du contrôle par chacun de ses informations à caractère personnel (« Qui sait quoi sur moi et qui en fait quoi ? »).

Le terme légal concerne la protection des données à caractère personnel et non pas les données personnelles. La nuance est importante. La protection n'est pas limitée aux données privées mais portent sur toutes les informations d'un individu (données personnelles, professionnelles, publiques). Cette dernière notion est donc plus large que la sphère de la vie privée. Ce n'est pas la vie privée au sens de l'intimité qui est protégée mais l'autonomie par rapport à des données. Le droit à l'auto-détermination informationnelle est dérivé mais pas assimilé au droit à la vie privée. Malheureusement, l'intitulé de la loi du 8 décembre 1992 peut induire en erreur dès lors qu'il mentionne qu'elle est relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Une confusion est donc possible et il existe d'ailleurs des cas de jurisprudence où le juge a estimé que des données professionnelles n'étaient pas couvertes par la loi au motif erroné que la loi n'accordait une protection qu'aux données ressortant de la vie privée.

Environnement européen

Mme de Terwangne fait un rappel du contexte européen en la matière. Il y a tout d'abord la Charte européenne des droits fondamentaux de 2000 qui est l'instrument international le plus moderne et récent en terme de « catalogue » de droits fondamentaux. La Charte prévoit expressément la protection de la vie privée (article 7) et la protection des données (article 8). C'est le seul instrument juridique international qui prévoit clairement cette distinction et qui protège les données à caractère personnel.

La loi belge s'inscrit également dans un environnement juridique européen et doit donc respecter les normes supérieures. En ce qui concerne les libertés fondamentales, il y a tout d'abord l'article 8 de la Convention européenne des droits de l'homme et les articles 7 et 8 de la Charte européenne des droits fondamentaux. Bien que la CEDH date de 1950, la Cour de justice a déclaré de longue date qu'elle avait le droit d'adopter une interprétation dynamique de la Convention. Elle a donc pu insérer la protection des données dans l'article 8. Il existe donc une très large jurisprudence fondée sur l'article 8 de la CEDH.

rechten maar ze mogen niet worden verward. De wet betreffende de bescherming van de gegevens van 8 december 1992, beoogt niet de privacy maar de zelfbeschikking over informatie. Dit begrip komt uit een arrest van 1981 van het Duits Grondwettelijk Hof dat bepaalt dat elk individu existentiële en beheerste keuzes moet kunnen maken. *In casu*, een individu moet zelf kunnen bepalen welke informatie over hem in omloop is. Het is de idee dat iedereen zijn persoonlijk gegevens kan controleren (« Wie weet wat over mij en wie doet er wat mee ? »).

De wettelijke term betreft de bescherming van persoonsgegevens en niet de persoonlijke gegevens. Die nuance is belangrijk. De bescherming is niet beperkt tot privégegevens maar betreft alle informatie van een individu (persoonlijke, professionele, openbare gegevens). Laatstgenoemd begrip reikt dus veel verder dan de persoonlijke levenssfeer. Het is niet het privéleven in de intieme betekenis dat wordt beschermd maar de autonomie ten opzichte van die gegevens. Het recht op zelfbeschikking over informatie is afgeleid van maar niet gelijkgesteld met het recht op privacy. Helaas kan het opschrift van de wet van 8 december 1992 misleidend zijn aangezien ze bepaalt dat dit een wet is tot de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens. Er is dus verwarring mogelijk en er is trouwens rechtspraak waarbij de rechter meent dat beroepsgegevens niet onder die wet vallen om de foutieve reden dat de wet slechts gegevens uit de persoonlijke levenssfeer beschermt.

Europese omgeving

Mevrouw de Terwangne herhaalt de Europese context ter zake. Ten eerste is er het Europees Handvest van de grondrechten van 2000, het modernste en recentste internationaal instrument als « catalogus »van de grondrechten. Het Handvest bepaalt uitdrukkelijk de bescherming van het privéleven (artikel 7) en de bescherming van persoonsgegevens (artikel 8). Het is het enige internationale juridische instrument dat duidelijk dit onderscheid maakt en persoonsgegevens beschermt.

De Belgische wet past ook in een Europese juridische omgeving en moet dus de hogere normen naleven. Wat de fundamentele vrijheden betreft, is er in de eerste plaats artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de artikelen 7 en 8 van het Europees Handvest van de grondrechten. Hoewel het EVRM dateert van 1950, verklaart het Hof van Justitie al heel lang dat het een dynamische interpretatie mag geven aan het Verdrag. Het heeft dus de bescherming van de persoonsgegevens in dit artikel 8 kunnen invoegen. Er bestaat dus een ruime rechtspraak op basis van artikel 8 van het EVRM.

Ensuite, il existe également la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données. Cette convention est actuellement en cours de modernisation très avancée car c'est le plus ancien instrument contraignant international en la matière. Enfin, la Directive 95/46 du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données est également en cours de révision. Tous ces instruments sont antérieurs à l'ère internet. C'est le lien avec internet et ses périphériques qui est l'enjeu des réflexions en cours. Les défis sont encore plus importants aujourd'hui car toutes les actions humaines dans un environnement technologique laissent des traces (achat sur internet, carte Mobib, accès à un journal électronique)

Vervolgens is er ook Verdrag nr. 108 van de Raad van Europa van 28 januari 1981 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens. Dat verdrag wordt momenteel grondig bijgewerkt want ze is het oudste internationale bindende instrument ter zake. richtlijn 95/46 van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens wordt, ten slotte, ook bijgewerkt. Al die instrumenten dateren van voor het internettijdperk. Het is de link tussen internet en de randapparatuur die centraal staat in de huidige discussie. De uitdagingen zijn vandaag nog groter want alle menselijke handelingen in een technologische omgeving laten sporen na (aankopen op internet, Mobib-kaart, toegang tot een elektronische agenda).

Compétences des entités fédérées

En terme de compétence, l'article 22 de la Constitution énonce que la loi, le décret ou la règle garantissent la protection de la vie privée. Toutefois, pour porter atteinte à la vie privée, seul le pouvoir législatif fédéral est compétent. Or, une législation de protection de données précise les limites et donc les atteintes à la vie privée.

Les entités fédérées, en exerçant leurs propres compétences, peuvent arriver à créer des bases de données spécifiques. À plus d'une occasion, la Cour constitutionnelle a été confrontée à ce partage de compétences et a considéré qu'une entité fédérée avait le droit de porter atteinte à la vie privée lorsque c'était nécessaire à l'exécution d'une de ses compétences. Toutefois, elle a précisé que les décrets des communautés et des régions ne pouvaient garantir un niveau de protection inférieur à celui de la LPVP.

Pour Mme de Terwangne, c'est assez étrange d'un point de vue juridique car en principe si l'entité fédérée est compétente elle ne doit pas respecter une loi fédérale. La position de la Cour constitutionnelle a été critiquée et en 2010 il y a eu une évolution de la jurisprudence puisque désormais il ne faut pas vérifier si l'entité fédérée a respecté la loi de 1992 mais si elle a respecté les obligations internationales qui découlent de la Directive et de la Convention n° 108 auxquels la loi de 1992 donne exécution. Cela permet de ne pas s'arrêter à la loi de 1992 mais de se référer aux instruments juridiques internationaux auxquels la loi de 1992 donne une exécution. C'est le nouveau raisonnement de la Cour qui, sur la base de l'article 22 de la Constitution (compétence), permet de se référer à un ensemble de normes internationales. Le législateur peut dès lors également adopter d'autres législations en se référant à ces normes internationales sans que la loi

Bevoegdheden van de deelstaten

Inzake bevoegdheid bepaalt artikel 22 van de Grondwet dat de wet, het decreet of de regel de bescherming van het privéleven waarborgen. Alleen de federale wetgevende macht is echter bevoegd om de privacy te schenden. Een wetgeving voor de bescherming van gegevens preciseert de beperkingen en dus de schendingen van de privacy.

De deelstaten kunnen binnen hun eigen bevoegdheden specifieke databanken opstellen. Bij meer dan één gelegenheid werd het Grondwettelijk Hof geconfronteerd met die gedeelde bevoegdheden en het meent dat een deelstaat het recht heeft om de privacy te schenden wanneer dat nodig is voor de uitvoering van één van zijn bevoegdheden. Het heeft echter gepreciseerd dat de gemeenschaps- en gewestdecreten geen minder grote bescherming mochten waarborgen dan de WBPL.

Voor mevrouw de Terwangne is dat vanuit een juridisch standpunt bekeken, erg vreemd want in principe, moet de deelstaat bij de uitoefening van zijn bevoegdheden, de federale wet niet naleven. Er kwam kritiek op het standpunt van het Grondwettelijk Hof en in 2010 veranderde de rechtspraak want voortaan moet er niet meer worden nagegaan of de deelstaat de wet van 1992 heeft nageleefd, maar of hij de internationale verplichtingen heeft nageleefd die voortvloeien uit de richtlijn, het Verdrag nr. 108 waaraan de wet van 1992 uitvoering geeft. Daardoor moet men zich niet beperken tot de wet van 1992 maar kan men verwijzen naar internationale rechtsinstrumenten waaraan de wet van 1992 uitvoering geeft. Het is door de nieuwe redenering van het Hof dat, op grond van artikel 22 van de Grondwet (bevoegdheden), men kan verwijzen naar een geheel van internationale normen. De wetgever kan bijgevolg ook andere wetten aannemen

de 1992 soit l'ultime et unique référence en la matière et ce d'autant qu'elle présente différentes lacunes.

Opacité du secteur public

Une des premières lacunes de la LPVP est qu'elle a engendré une certaine opacité quant au traitement des données dans le secteur public. À l'origine, les législations européennes en la matière sont nées de la crainte d'abus liés à l'usage de données par l'État, notamment à l'instar de l'utilisation des nombreux registres au cours de la deuxième guerre mondiale. La crainte était d'avoir un administré « nu » et seul devant une administration omnisciente sachant tout de lui. Les premières lois sont donc nées de cette peur du secteur public et sont très protectrices de l'individu face au secteur public. C'est le cas des lois allemandes et françaises. En Belgique, la LPVP étant plus récente, on s'est rendu compte que le risque d'abus existait également dans le secteur privé (banques, assurances) et finalement on est resté assez lénifiant sur le secteur public.

Ainsi, en cas de collecte de données, un critère de finalité doit être respecté (auto-détermination informationnelle). Toutefois, se pose la question du traitement ultérieur de ces mêmes données. En principe, on peut procéder à un nouveau traitement de données à la condition que ce traitement soit compatible avec la finalité première. Ce critère équivaut à vérifier que ce traitement rentre dans l'attente raisonnable des gens. On peut par exemple s'attendre à ce qu'une banque qui dispose de données sur ses clients leur fasse ensuite des propositions sur des produits bancaires. Par contre, si un club de sport procède à des enregistrements audiovisuels (assimilés par la loi à des données) pour des raisons de sécurité mais les communique ensuite à un tiers, cette communication n'est plus compatible avec la finalité.

Le deuxième critère est l'autorisation prévue par la loi. Ce critère est assez flou puisqu'un arrêté royal suffit pour réutiliser des données récoltées précédemment. Or, aujourd'hui cette pratique est devenue monnaie courante et la dernière en date consiste en une base de données sur les plaques d'immatriculation. Dans ce cas, l'utilisation ultérieure sort manifestement de l'attente raisonnable des citoyens.

En outre, il existe une obligation d'informer les citoyens lorsque l'on collecte des informations personnelles que ce soit de manière directe ou indirecte (acquisition d'une base de données). Ce devoir d'information est lourd puisqu'il oblige le nouveau détenteur d'une base de données à informer en principe chaque individu qu'il a récupéré des données sur lui et

op grond van die internationale normen zonder dat de wet van 1992 de uiterste en enige verwijzing ter zake is, ook al omdat ze verschillende lacunes vertoont.

Ondoorzichtigheid van de overheidssector

Een van de eerste lacunes van de WBPL is dat ze voor minder transparantie heeft gezorgd voor de verwerking van de gegevens in de overheidssector. Oorspronkelijk zijn de Europese wetten ter zake ontstaan vanuit de vrees dat de Staat de gegevens zou misbruiken meer bepaald in navolging van de talrijke registers die in de loop van de Tweede Wereldoorlog werden gebruikt. De vrees was het beeld van een « naakte » en alleenstaande burger tegenover een alwetende overheid die alles van hem weet. De eerste wetten zijn dus ontstaan uit die vrees voor de overheid en zijn dus heel beschermend voor het individu tegenover de overheid. Dat is het geval voor de Duitse en Franse wetten. In België, waar de WBPL van recentere datum is, besefte men dat de kans op misbruik ook vanuit de privésector kon komen (banken, verzekeringen) en uiteindelijk is men vrij soepel gebleven voor de overheidssector.

Zo moet bij het verzamelen van gegevens, een finaliteitscriterium worden nageleefd (zelfbeschikking over informatie). Hierbij rijst echter de vraag naar de verdere verwerking van diezelfde gegevens. In principe mag men de gegevens opnieuw verwerken op voorwaarde dat die verwerking overeenstemt met de oorspronkelijke bedoeling. Dat criterium betekent zoveel als nagaan of die verwerking binnen de redelijke verwachting van de mensen ligt. Men kan bijvoorbeeld verwachten dat een bank aan de hand van de gegevens van zijn klanten, hun voorstellen doet voor bankproducten. Indien een sportclub daarentegen audiovisuele opnames maakt (gelijkgesteld met de wet op de persoonsgegevens) om veiligheidsredenen maar ze vervolgens meedeelt aan derden, dan is die mededeling niet meer in overeenstemming met de doelstelling.

Het tweede criterium is de bij wet bepaalde toelating. Dat criterium is erg vaag omdat een koninklijk besluit volstaat om de vooraf verzamelde gegevens te hergebruiken. Momenteel is dit een gangbare praktijk geworden en de recentste toepassing hiervan is de databank voor nummerplaten. In dit geval valt het verdere gebruik duidelijk buiten de redelijke verwachting van de burger.

Bovendien is men verplicht de burger te informeren wanneer men persoonsgegevens verzamelt op een rechtstreekse of onrechtstreekse manier (opstellen van een databank). Die informatieplicht is zwaar want de nieuwe eigenaar van een databank moet in principe elk individu ervan op de hoogte brengen dat hij diens gegevens heeft en hij moet de doeleinden waarvoor hij

à lui préciser à quelles fins il va les utiliser. Or, il existe une exception pour le secteur public dès lors que « l'enregistrement ou la communication des données est effectué en vue de l'application d'une disposition prévue par ou en vertu de la loi ». Donc, un arrêté royal suffit pour récupérer une base données et à l'utiliser à d'autres fins et sans qu'aucune obligation d'information ne pèse sur l'autorité publique. La Directive prévoit également une exception mais elle est plus exigeante en ce sens que l'obligation d'information est levée si la législation prévoit expressément l'enregistrement des données. En Belgique, le secteur public peut aujourd'hui retraiter des données en toute opacité. Mme de Terwangne plaide donc pour que ces nouveaux traitements de données soient assortis d'une certaine transparence. La norme doit être explicite à cet égard.

Or, les bases de données et les entrepôts de données (« *data warehouses* ») où sont rassemblées plusieurs bases de données en une seule se multiplient au sein de l'administration publique. Par exemple, une base de données du ministère des Finances sera créée pour permettre d'avoir une vue d'ensemble du patrimoine des citoyens et regrouperait les bases de données existantes sur les revenus, les opérations immobilières et les baux. Étant donné ce mouvement en cours, la problématique des traitements ultérieurs mérite un examen tout particulier. A tout le moins, le parlement devrait pouvoir contrôler cette activité car aujourd'hui il n'y a plus aucun contrôle. Il suffirait de prévoir au titre de condition de compatibilité que la loi qui crée ladite base de données précise clairement qu'il y a création d'un nouveau traitement, son contenu et les conditions d'accès.

Activité exclusivement personnelle ou domestique

Une deuxième difficulté provient des activités exclusivement personnelles ou domestiques et donc réalisées par des particuliers. C'est une problématique délicate car il y a une réticence à règlementer la vie privée des gens au nom de la protection de vie privée. Ainsi, si un particulier collecte des informations sur la généalogie de sa famille et crée une base de données, il n'y a pas de problème.

Mais avec l'utilisation du web 2,0 (sites internet qui ont la caractéristique d'être interactifs comme Wikipedia, blogs) et l'ère de « l'Internet des loisirs » (gestion de comptes Facebook ou blogs), on utilise finalement un outil public pour y déposer des informations personnelles. Or, il y a par ce biais des atteintes à la protection des données à caractère personnel. Dès lors, on ne peut pas exclure cette activité du champ d'application de la loi. Une réflexion est menée à ce sujet et une piste serait d'insérer cette activité dans le champ d'application de la loi mais avec

ze gaat gebruiken toelichten. Voor de overheidssector is er een uitzondering wanneer « de registratie of de verstrekking van de persoonsgegevens verricht wordt met het oog op de toepassing van een bepaling voorgeschreven door of krachtens een wet ». Een koninklijk besluit volstaat dus om een databank te hergebruiken voor andere doeleinden, zonder enige informatieplicht voor de overheid. De richtlijn voorziet ook in een uitzondering maar is veeleisender omdat de informatieplicht wordt opgeheven als de wet uitdrukkelijk voorziet in de registratie van de gegevens. In België kan de overheidssector momenteel gegevens opnieuw verwerken zonder enige transparantie. Mevrouw Terwagne pleit er dus voor de nieuwe gegevensverwerkingen gepaard te laten gaan met enige transparantie. De norm moet in dat opzicht expliciet zijn.

De databanken en datapakhuizen (« datawarehouses ») waarin meerdere databaken zijn opgeslagen in één enkele bank worden binnen de overheidsdiensten talrijker. Een databank van de FOD Financiën zal bijvoorbeeld worden opgesteld om een overzicht te krijgen van het patrimonium van de burger en zou de bestaande databanken over het inkomen, de onroerende verrichtingen en de huurcontracten samenvoegen. Aangezien die beweging in gang is gezet, verdient de problematiek van de verdere verwerking bijzondere aandacht. Het parlement moet minstens die activiteit kunnen controleren want momenteel is er geen enkel toezicht meer. Het zou volstaan om op grond van verenigbaarheid te bepalen dat de wet die de voornoemde databank opstelt, duidelijk moet preciseren dat er een nieuwe verwerking plaatsvindt, wat de inhoud ervan is en wat de toegangsvoorwaarden zijn.

Activiteit die uitsluitend privé of huiselijk is

Een tweede moeilijkheid betreft activiteiten die uitsluitend privé of huiselijk zijn en dus door privépersonen worden uitgevoerd. Het is een delicate problematiek want er is enige terughoudendheid om het privéleven van de mensen te regelen om de privacy te beschermen. Wanneer een privépersoon informatie verzamelt over zijn stamboom en een database maakt, dan is er geen probleem.

Maar met Web 2,0 (internetsites die interactief zijn zoals Wikipedia, blogs ...) en het tijdperk van « internet als ontspanning » (Facebook of bloggen) gebruikt men uiteindelijk een publiek middel om persoonlijke informatie te vermelden. Op die manier worden er inbreuken gepleegd op de bescherming van de persoonsgegevens. Bijgevolg mag die activiteit niet uitgesloten worden van het toepassingsgebied van de wet. Er worden hierover besprekingen gevoerd waarbij men eventueel die activiteit in het toepassingsgebied van de wet zou opnemen, maar met minder

des obligations allégées pour les particuliers (pas de déclaration, pas de devoir d'information).

Régime d'exception pour certaines professions

La LPVP soumet actuellement certaines catégories professionnelles aux obligations prévues par la loi alors qu'elles sont soumisses au secret professionnel. Il n'existe aucune exception au bénéfice de certaines catégories professionnelles. Ces catégories professionnelles (avocats, médecins) sont donc en principe obligées d'informer les personnes sur lesquelles portent les données et de leur accorder un droit d'accès. Or, si un avocat est consulté par une épouse pour un divorce, il sera amené à collecter des données sur le mari. La loi est telle que l'avocat doit en théorie informer le mari qu'il est en train de récolter des informations sur lui et en plus lui accorder un droit d'accès. À défaut, une sanction pénale est prévue. La problématique est identique pour les médecins.

Notion de données à caractère personnel (DACP)

La notion de DACP est une notion très vaste puisqu'elle couvre la donnée et sa collecte jusqu'au moment où soit elle devient anonyme ou soit elle est détruite. On entend par donnée à caractère personnel toute information concernant toute personne physique identifiée ou identifiable. Le terme « identifiable » pose ici problème puisque l'on peut toujours, de manière indirecte, lier une information à une personne physique avec la conséquence que toute donnée est une donnée à caractère personnel.

Or, pour M. Van Gyseghem, la notion de DACP doit être liée à la finalité qui est poursuivie dans ce traitement. Si un magasin veut faire une étude de fréquentation de son établissement et photographie en toute légalité (déclaration est faite) les plaques d'immatriculation des véhicules du parking, ces données ne devraient pas être considérées comme des DACP car le magasin n'a pas la possibilité de faire le lien entre le numéro de plaque et le propriétaire du véhicule. Toutefois, au sens de la loi, il existe en théorie des liens indirects pour faire ce lien, ce qui donnerait quand même à ces données le caractère de DACP. Or, si on remet à sa juste place la finalité que ledit magasin recherche et les moyens dont il dispose, il conviendrait de sortir ce traitement de données du champ d'application des DACP. Par contre, un agent verbalisant qui prendrait la même photo poursuit une autre finalité et va effectivement pouvoir identifier le propriétaire du véhicule. Ce critère de finalité devrait être précisé dans la loi pour permettre à certaines personnes de ne pas être confrontée à la lourdeur de la loi car la finalité qu'elles poursuivent et les moyens

zware verplichtingen voor privépersonen (geen verklaring, geen informatieplicht).

Uitzonderingsregeling voor bepaalde beroepen

De WBPL onderwerpt momenteel bepaalde beroepscategorieën aan de bij wet bepaalde verplichtingen, hoewel zij gebonden zijn door het beroepsgeheim. Er bestaat geen enkele uitzondering voor bepaalde beroepscategorieën. Die beroepscategorieën (advocaten, artsen) moeten dus in principe de personen op wie de gegevens betrekking hebben, op de hoogte brengen en hun een inzagerecht verlenen. Als een echtgenote een advocaat om advies vraagt voor een echtscheiding, dan zal de advocaat gegevens over de echtgenoot moeten verzamelen. De wet is zo opgesteld dat de advocaat in theorie de echtgenoot op de hoogte moet brengen van het feit dat hij informatie over hem verzamelt en hem een inzagerecht moet verlenen. Zo niet wordt er in een strafrechtelijke sanctie voorzien. Die problematiek is ook van toepassing op artsen.

Begrip persoonsgegevens

Het begrip persoonsgegevens is een heel uitgebreid begrip, omdat dit betrekking heeft op het gegeven en de inzameling ervan tot het tijdstip waarop het anoniem wordt of vernietigd wordt. Met persoonsgegeven bedoelt men alle informatie over elke geïdentificeerde of identificeerbare natuurlijke persoon. De term « identificeerbaar » doet hier een probleem rijzen, want men kan steeds op indirecte wijze informatie aan een natuurlijke persoon koppelen, met als gevolg dat elk gegeven een persoonsgegeven is.

Volgens de heer Van Gyseghem moet het begrip persoonsgegeven worden gekoppeld aan het doel dat met de verwerking wordt nagestreefd. Wanneer een winkel een studie wil maken van het bezoek aan de vestiging en volstrekt wettelijk (na aankondiging) alle nummerplaten van de voertuigen op de parking fotografeert, dan mogen die gegevens niet worden beschouwd als persoonsgegevens, omdat de winkel niet de mogelijkheid heeft het verband te leggen tussen het nummer op de plaat en de eigenaar van het voertuig. Maar in de zin van de wet bestaan er theoretisch indirecte middelen om dat verband te leggen, waardoor die gegevens toch persoonsgegevens worden. Maar wanneer men het doel dat die winkel nastreeft en de middelen waarover hij beschikt in het juiste perspectief ziet, dan is het raadzaam die gegevensverwerking uit het toepassingsgebied van de persoonsgegevens te halen. Een agent die een procesverbaal opmaakt daarentegen en die dezelfde foto neemt, streeft een ander doel na en zal de eigenaar van het voertuig wel degelijk kunnen identificeren. Dat criterium van doelstelling moet in de wet worden

dont elles disposent ne confèrent pas à ces données le statut de DACP. Il en est de même pour les adresses IP.

Cela permettra aussi de procéder à une classification plus fine des catégories de données « ordinaires » et « sensibles ». En effet, la loi prévoit actuellement deux types d'obligations et deux types de vision. Il y a ce qu'on appelle les données « ordinaires », assorties d'un régime d'autorisation, et les données « sensibles » (données liées à la santé ou à l'ethnie), assorties d'un régime d'interdiction sauf exceptions. Se pose toutefois la question des données qui peuvent être « mixtes ». La photographie d'une personne de couleur par les services du Sénat ne posera aucun souci si la finalité se limite à faire un album photo de toutes les personnes invitées au Sénat. Par contre, si la finalité a pour but de faire un classement par races des personnes venues au Sénat alors la finalité devient « sensible » et le régime d'interdiction sera d'application. La loi devrait être beaucoup plus explicite et précise sur ce point.

La notion de DACP doit également être adaptée à certains domaines car la loi se révèle souvent inapplicable. En cas de recherche médicale, un chercheur ne reçoit des données de la part d'un hôpital qu'après qu'elles ont été codées une ou deux fois. Elles ne sont toutefois pas anonymes car on peut en principe toujours retrouver, par le truchement d'une table de codage, la personne physique liée à l'information. Toutefois, le chercheur lui-même n'a que des données codées et il lui est impossible de faire un lien avec un patient. Il y a donc des domaines précis pour lesquels une réglementation spécifique quant aux obligations est nécessaire.

D'autre part, certaines données doivent faire l'objet d'une protection particulière et qui ne sont pas visées par la loi comme celles relatives à la localisation des individus. Ainsi, les Iphones stockent les données de localisation et ce à l'insu des personnes. La loi devrait s'attacher à règlementer certaines données car elles sont la preuve d'une évolution technologique.

Pour ce qui concerne les données génétiques, celles-ci sont considérées comme sensibles car à priori elles relèvent de la santé. Or, ces données ne sont pas toujours sensibles au sens de la loi. La donnée génétique peut être une donnée non relative à la santé. Ainsi dans une enquête judiciaire, l'analyse de l'ADN ne consiste pas en une information sur la santé mais vise tout simplement à identifier une personne. Mais la donnée génétique reste sensible car elle recèle en soi une information qui ne concerne pas seulement l'individu mais toute la fratrie ou toute une famille.

vermeld, zodat bepaalde personen niet worden geconfronteerd met de logheid van de wet, aangezien hun doelstelling en hun middelen die gegevens niet de status van persoonsgegevens geven. Hetzelfde geldt voor de IP-adressen.

Daardoor wordt ook een fijnere classificatie mogelijk van de « gewone » en « gevoelige » gegevens. Nu voorziet de wet immers in twee soorten verplichtingen en twee soorten visies. Men heeft wat men de « gewone » gegevens noemt met een regeling van toestemming en de « gevoelige » gegevens (gegevens rond gezondheid of etnie) met een verbodsregeling, tenzij er een uitzondering voor bestaat. Er is evenwel het probleem van de gegevens die « gemengd » kunnen zijn. Het fotograferen van een gekleurd iemand door de diensten van de Senaat zal niet verontrusten wanneer het enkel de bedoeling is een fotoalbum te maken van alle personen die door de Senaat werden uitgenodigd. Indien het doel echter is een rangschikking per ras te maken van de personen die naar de Senaat zijn gekomen, dan wordt het doel « gevoelig » en zal de verbodsregeling gelden. Wat dat betreft, moet de wet veel duidelijker en nauwkeuriger zijn.

Het begrip persoonsgegevens moet ook aan bepaalde branches worden aangepast, want vaak blijkt de wet niet toepasbaar. Bij medische research ontvangt een vorser slechts gegevens van een ziekenhuis nadat ze één- of tweemaal werden gecodeerd. Ze zijn echter niet anoniem, want in principe kan men steeds door middel van een coderingstabel de natuurlijke persoon achter de gegevens terugvinden. De vorser zelf heeft echter slechts gecodeerde gegevens en hij kan onmogelijk het verband met een patiënt leggen. Er zijn dus welbepaalde branches waarvoor een specifieke reglementering inzake verplichtingen noodzakelijk is.

Anderzijds moeten bepaalde gegevens die niet binnen de werkingssfeer van de wet vallen, speciaal worden beschermd, zoals de gegevens betreffende de lokalisatie van individuen. I-phones bijvoorbeeld slaan lokalisatiegegevens op zonder dat de betrokkenen dat weten. De wet moet bepaalde gegevens reglementeren, want ze zijn het bewijs van een technologische ontwikkeling.

Genetische gegevens worden *a priori* als gevoelig beschouwd, omdat ze met de gezondheid te maken hebben. Die gegevens zijn echter in de zin van de wet niet altijd gevoelig. Een genetisch gegeven kan een gegeven zijn dat niet met de gezondheid te maken heeft. In een gerechtelijk onderzoek bijvoorbeeld is een DNA-analyse geen gezondheidsgebonden gegeven, maar dient ze gewoon om een persoon te identificeren. Het genetische gegeven blijft echter gevoelig, want het bevat op zich informatie die niet alleen het individu behelst, maar alle broers en zusters

Elle doit être en soi une donnée sensible. Ce n'est actuellement pas prévu par la loi.

Enfin, la notion de données anonymes est prévue par deux législations différentes qui prévoient deux définitions différentes. Au sens de la Directive, on est en présence d'une donnée anonyme lorsque par des moyens raisonnables, on ne peut pas la lier à une personne concernée. Au sens de l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992, une donnée est anonyme lorsque le lien avec une personne est définitivement coupé. Il y a là donc une double définition qui peut être justifiée par la finalité de ces deux législations mais il serait bon de repenser le caractère de données anonymes et ce d'autant plus qu'il est difficile aujourd'hui d'avoir une donnée anonyme sur internet. Par le croisement de multiples bases de données peut-on encore aujourd'hui être anonyme ?

L'intervention d'un tiers de confiance (TT) pour garantir une anonymisation est à prôner afin que les données transitent par cette instance pour les rendre codées ou anonymes. Ce tiers de confiance serait le seul à détenir la clé de hachage de la donnée de sorte que la donnée sortirait du champ d'application de la loi. Cette intervention devrait être assortie d'obligations relatives au secret professionnel et d'un régime de sanctions à prévoir dans la loi.

Notion de personne concernée

La loi prévoit actuellement que seule une personne physique est une personne concernée. Or, certaines législations européennes prévoient qu'une personne morale est aussi une personne concernée. Il convient de se poser la question si, à l'égard des personnes morales, la législation LPVP est la seule qui puisse répondre à certaines attaques comme des actes de diffamation sur internet. Il conviendrait de réaliser une étude de droit comparé et d'examiner la possibilité d'inclure les personnes morales dans la loi LPVP. Il en est de même pour le « *cloudcomputing* » dès lors que de plus en plus de sociétés mettent des données sensibles sur internet et utilisent celui-ci comme zone de « stockage » en lieu et place d'un serveur.

Révision du statut de la Commission de la protection de la vie privée

Il conviendrait selon l'orateur de garantir une meilleure indépendance de la commission de la protection de la vie privée en assurant une nomination des commissaires plus objective et en révisant les règles d'incompatibilités.

of een hele familie. Het moet een gevoelig gegeven op zich zijn. Dat is nu niet in de wet bepaald.

Het begrip anonieme gegevens is ten slotte opgenomen in twee verschillende wetgevingen, met twee verschillende definities. In de zin van de richtlijn heeft men met een anoniem gegeven te maken wanneer men het niet met redelijke middelen aan een betrokkene kan koppelen. In de zin van het koninklijk besluit van 13 februari 2001 ter uitvoering van de wet van du 8 december 1992 is een gegeven anoniem wanneer de band met een persoon definitief doorbroken is. Er is dus sprake van een dubbele definitie, die kan worden verantwoord door de doelstelling van beide wetgevingen. Het zou echter goed zijn om opnieuw na te denken over de definitie van anonieme gegevens, temeer omdat het vandaag moeilijk is een anoniem gegeven op internet te vinden. Kan men door het combineren van de vele databases vandaag nog anoniem zijn ?

Er moet worden gepleit voor het optreden van een derde vertrouwenspersoon om het anoniem maken te waarborgen, opdat de gegevens via die instantie passeren om ze te coderen of anoniem te maken. Die derde vertrouwenspersoon zou dan de enige zijn die de codeersleutel van het gegeven heeft, zodat het gegeven buiten het toepassingsgebied van de wet valt. Dat optreden moet gepaard gaan met verplichtingen inzake het beroepsgeheim en een in de wet op te nemen sanctieregeling.

Het begrip betrokkene

Nu bepaalt de wet dat alleen een natuurlijk persoon een betrokkene is. Een aantal Europese wetgevingen bepalen echter dat een rechtspersoon eveneens een betrokkene is. Het is raadzaam zich af te vragen of de privacywetgeving de enige is die voor rechtspersonen een antwoord kan bieden op bepaalde aanvallen, zoals handelingen van smaad op het internet. Men zou een vergelijkend rechtsonderzoek kunnen doen en de mogelijkheid onderzoeken om de rechtspersonen in de privacywet op te nemen. Hetzelfde geldt voor « cloudcomputing », aangezien steeds meer ondernemingen gevoelige gegevens op het internet brengen en het gebruiken als een « opslagruimte », in plaats van een server te gebruiken.

Herziening van het statuut van de Commissie voor de bescherming van de persoonlijke levenssfeer

Volgens spreker moet de onafhankelijkheid van de commissie voor de bescherming van de persoonlijke levenssfeer beter worden gewaarborgd door een objectievere benoeming van de commissieleden en een herziening van de regels van onverenigbaarheid.

M. Van Gyseghem suggère aussi de prévoir un contrôle régulier de la commission par des auditeurs indépendants. Il s'agirait entre autres de vérifier si la commission remplit correctement sa mission et ce de manière indépendante. Un arrêt de la Cour de justice du 9 mars 2010 confirme d'ailleurs que « la garantie d'indépendance de l'autorité nationale de contrôle vise à assurer la fiabilité et l'efficacité du contrôle du respect des dispositions en matière de protection des personnes physiques à l'égard des données à caractère personnel et doit être interprété à la lumière de cet objectif. Ces autorités doivent être à l'abri de toute influence extérieure y compris celle directe ou indirecte de l'État ».

Il convient aussi de l'instituer comme autorité à l'instar de la CNIL en France et non comme organe parlementaire. Il faut également donner au justiciable la possibilité d'introduire un recours car si la commission ne rend que des avis, ceux-ci peuvent avoir des conséquences importantes pour les individus. Il faut également donner à la commission un pouvoir de sanction (amendes, injonctions). Enfin, les sanctions pénales actuellement prévues par la loi sont souvent insuffisantes et l'on constate de plus en plus que des sociétés préfèrent payer l'amende pénale suite au bénéfice qu'elles ont retiré de la violation de la loi. Il faudrait les assortir de sanctions plus pénalisantes et adaptées au secteur d'affaires pour les contrevenants, comme une publication par exemple.

Capacité d'action des personnes concernées

M. Van Gyseghem constate qu'en pratique l'individu, de par son isolement, n'a aucun poids face à certaines pratiques existantes. De plus, les frais de justice et d'avocats dissuadent l'individu d'entamer une procédure judiciaire dont l'objectif est la réparation d'un dommage qui ne sera souvent que moral. L'orateur suggère dès lors de réactiver les propositions de loi relatives à la procédure de « class action » ou d'éventuellement prévoir cette possibilité dans la LPVP.

*2. Échange de vues*

M. De Padt souligne que les intervenants ont proposé une série d'interventions au niveau législatif. Le groupe de travail pourrait, par-delà les frontières des partis, rédiger un texte en vue de la prise d'une initiative législative.

L'orateur demande s'il existe au sein de la faculté une proposition de texte relatif aux modifications nécessaires. Cela faciliterait grandement le travail des parlementaires tout en permettant aussi d'agir plus vite.

De heer Van Gyseghem suggereert ook te voorzien in regelmatige controle van de commissie door onafhankelijke auditoren. Men moet onder andere nagaan of de commissie haar opdracht correct vervult, en wel op onafhankelijke wijze. Een arrest van het Hof van Justitie van 9 maart 2010 bevestigt overigens : « De waarborg van onafhankelijkheid van de nationale toezichthoudende autoriteiten beoogt de doeltreffendheid en de betrouwbaarheid van het toezicht op de naleving van de bepalingen inzake de bescherming van natuurlijke personen bij de verwerking van persoonsgegevens te verzekeren en moet tegen de achtergrond van deze doelstelling worden uitgelegd. Daartoe moeten zij vrij zijn van beïnvloeding van buitenaf, daaronder begrepen de — rechtstreekse of indirecte — beïnvloeding door de staat ».

Het is ook raadzaam ze als autoriteit in te stellen, zoals de CNIL in Frankrijk, in plaats van als parlementair orgaan. Men moet de rechtzoekende tevens de mogelijkheid bieden om in beroep te gaan, want hoewel de commissie alleen maar adviezen geeft, kunnen die toch belangrijke gevolgen hebben voor de individuen. Men moet de commissie ook sanctiebevoegdheid geven (geldboeten, aanmaningen). De straffen waarin de wet nu voorziet, zijn ten slotte vaak ontoereikend en men ziet steeds vaker dat ondernemingen verkiezen de geldboete te betalen uit de winst die ze hebben gehaald uit de schending van de wet. Men moet de overtreders zwaardere straffen opleggen, die aangepast zijn aan de zakensector, zoals bijvoorbeeld een publicatie.

Actiebereidheid van de betrokkenen

De heer Van Gyseghem stelt vast dat één persoon alleen niet tegen bepaalde praktijken op kan. Vanwege de gerechts- en advocatenkosten zullen individuele personen vaak afzien van een gerechtelijke procedure met als doel het herstel van schade die vaak alleen moreel is. Spreker stelt dan ook voor de wetsvoorstellen betreffende de « class action » nieuw leven in te blazen of eventueel in die mogelijkheid te voorzien in de privacywet.

*2. Gedachtewisseling*

De heer De Padt stipt aan dat sprekers een aantal ingrepen op wetgevend vlak hebben voorgesteld. De werkgroep zou, over de partijgrenzen heen, een wetgevend initiatief kunnen nemen.

Spreker wenst te weten of er binnen de faculteit een voorstel van tekst bestaat met betrekking tot de noodzakelijke wijzigingen. Dit zou het werk van de parlementsleden aanzienlijk vergemakkelijken, zodat sneller kan worden gehandeld.

L'intervenant renvoie par ailleurs à la nécessité qui a été évoquée de rendre applicable aux personnes morales la loi relative à la protection de la vie privée. Il a été souligné à ce sujet qu'un examen plus approfondi s'impose, éventuellement assorti d'un exercice de droit comparé en la matière. Des textes équivalents existent manifestement dans d'autres pays. Cette législation est-elle transposable telle quelle en Belgique ? Y a-t-il lieu d'y consacrer un examen plus approfondi ?

Mme de Terwangne précise qu'aucune étude n'a encore été faite sur le problème de la protection des personnes morales. C'est assez nouveau. Sur les autres questions, le CRIDS n'a pas fait de travail de légistique mais peut si nécessaire transmettre au groupe de travail des articles de doctrine sur les points évoqués.

Mme Piryns remercie les deux orateurs qui, une fois de plus, ont mis le doigt sur les problèmes que pose l'utilisation de l'Internet sur le plan de la protection des données à caractère personnel.

Elle remercie aussi les divers intervenants pour la manière dont ils ont évoqué les initiatives législatives qui doivent être prises en la matière. Plusieurs pistes ont été avancées et le groupe de travail devra décider d'une méthode.

L'intervenante souligne que les groupes sp.a-Groen ! avait en tout cas déjà déposé, sous la précédente législature, une proposition de loi sur la « *class action* ». Cette proposition peut faire l'objet d'un redépôt.

M. Mahoux souhaite formuler quelques réflexions. Tout d'abord, si des initiatives doivent être prises pour modifier des textes existants, il importe de ne pas complexifier ce qui est déjà complexe. Ensuite, si on modifie la loi, il faudrait que l'éventuelle proposition de loi soit soutenue par rapport au contenu.

En termes de méthodologie, on peut se baser sur le texte de la loi du 8 décembre 1992 et procéder par amendements sans avoir le souci absolu de cohérence par rapport à l'ensemble des problèmes qui sont posés. Par exemple, changer un intitulé n'est pas difficile à effectuer. Si, symboliquement, modifier l'intitulé de la loi est important pour réconcilier la doctrine avec la jurisprudence, M. Mahoux estime qu'il convient de le faire.

Sur le secret professionnel, M. Mahoux reste attaché à la valeur première du secret professionnel. Dans la situation actuelle, indiquer que le secret professionnel doit primer sur la réglementation des données à caractère personnel est envisageable également. Ces deux exemples sont des éléments qui permettent d'avancer. Enfin, sur la notion de données sensibles et l'élément de finalité, M. Mahoux pense

Verder verwijst spreker naar de aangehaalde noodzaak om de wetgeving met betrekking tot de bescherming van de privacy ook toepasselijk te maken op rechtspersonen. Er werd hierbij aangestipt dat verder onderzoek, eventueel rechtsvergelijkend, zich opdringt. De gelijke teksten bestaan blijkbaar in andere landen; is deze buitenlandse wetgeving zonder meer te implementeren in België ? Is verder onderzoek nog nodig ?

Mevrouw de Terwangne verklaart dat er nog geen enkel onderzoek werd verricht naar het probleem van de bescherming van de rechtspersonen. Dat is vrij nieuw. Over de andere problemen heeft het CRIDS geen wetgevingstechnisch werk verricht, maar indien nodig kan het centrum de werkgroep artikels uit de rechtsleer over de besproken punten bezorgen.

Mevrouw Piryns dankt beide sprekers die, eens te meer, de vinger leggen op de problemen die, door het gebruik van Internet, rijzen op het vlak van bescherming van de persoonsgegevens.

Spreekster dankt ook voor de wijze waarop werd aangehaald welk wetgevend werk dient te worden verricht. Verschillende pistes voor wetgevende initiatieven worden aangereikt, en de werkgroep zal zich moeten beraden over de werkwijze.

Spreekster wijst erop dat de fractie sp.a-Groen ! in elk geval reeds in vorige zittingsperiode een wetsvoorstel over « *class action* » had ingediend. Dit kan opnieuw worden ingediend.

De heer Mahoux wil enkele bedenkingen formuleren. Ten eerste, indien er initiatieven moeten worden genomen om bestaande teksten te wijzigen, dan is het belangrijk dat men iets wat al complex is, niet nog complexer maakt. Ten tweede, indien men de wet wijzigt, dan moet het eventuele wetsvoorstel inhoudelijk overeind blijven.

Wat de methodologie betreft, kan men zich baseren op de tekst van de wet van 8 december 1992 en met amendementen werken zonder zich veel zorgen te maken over de samenhang met alle problemen die behandeld werden. Een opschrift wijzigen bijvoorbeeld is niet moeilijk. Indien het symbolisch belangrijk is het opschrift van de wet te wijzigen om de rechtsleer in overeenstemming te brengen met de rechtspraak, dan vindt de heer Mahoux dat men dat moet doen.

Wat het beroepsgeheim betreft, blijft de heer Mahoux gehecht aan het primaat van het beroepsgeheim. Bij de huidige stand van zaken is het ook mogelijk te vermelden dat het beroepsgeheim voorrang moet hebben op de reglementering van de persoonsgegevens. Beide voorbeelden zijn mogelijkheden om vooruitgang te boeken. Wat het begrip gevoelige gegevens en het aspect doelstelling betreft,

que cela sera compliqué car cela implique un élément intentionnel qu'il convient d'objectiver.

Sur la question de la protection des personnes morales ainsi que la possibilité d'une « class action », M. Mahoux pense également que la loi pourrait faire l'objet d'une révision. Mais la question est de savoir s'il est raisonnable par rapport à une législation existante de procéder par modifications successives.

Mme de Terwangne réaffirme le fait que l'existence de la LPVP est un atout mais il faut la corriger. Quant à la méthode, il faudra tenir compte de la révision de la Directive 95/46 et la Convention n° 108. Il importe donc de savoir s'il est opportun de modifier la loi belge sans attendre les résultats du processus de révision de la Directive.

denkt de heer Mahoux dat het moeilijk wordt, omdat het een intentioneel aspect behelst dat men moet objectiveren.

Wat de bescherming van de rechtspersonen en de mogelijkheid van een « *class action* » betreft, denkt de heer Mahoux eveneens dat de wet kan worden herzien. Het is echter de vraag of het verstandig is bestaande wetgeving met opeenvolgende wijzigingen aan te pakken.

Mevrouw de Terwangne herhaalt dat het feit dat de privacywet bestaat een troef is, maar dat hij gecorrigeerd moet worden. Wat de methode betreft, zal men rekening moeten houden met de herziening van richtlijn 95/46 en met Verdrag nr. 108. Men dient dus te weten of het opportuun is de Belgische wet te wijzigen zonder de resultaten van de herziening van de richtlijn af te wachten.

## E. Audition du 15 juin 2011.

*1. Exposé de Mme Marie-Hélène Boulanger, chef d'unité « protection de données », DG Justice, Commission européenne*

Le cadre européen de protection de données et le rôle de l'Union européenne

Mme Boulanger rappelle que la directive 95/46 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ainsi que le Traité de Lisbonne constituent les instruments cadre en la matière. La directive 95/46 datant de 1996, la Commission européenne peut déjà tirer plusieurs enseignements de son application en vue de faire face aux nouveaux défis technologiques et à un monde de plus en plus globalisé. Toutefois, les questions liées aux juridictions compétentes et au droit applicable restent des questions fondamentales.

Au niveau de l'Union européenne, on constate depuis l'entrée en vigueur le 1er décembre 2009 du Traité de Lisbonne, un changement d'approche dans la protection des données. À l'origine, la directive 95/46 était basée sur une logique de « marché intérieur ». En effet, la Commission est intervenue pour veiller à ce que les différences entre les différentes législations des États membres ne constituent pas un obstacle à l'échange des données à caractère personnel. Aussi, la directive 95/46 a établi une équivalence des protections pour éviter que des obstacles soient créés aux flux de données. La directive 95/46 précise qu'en tous les cas l'harmonisation recherchée ne peut contribuer à limiter ou à diminuer le niveau de protection qui existait déjà dans les États membres.

## E. Hoorzitting van 15 juni 2011

*1. Uiteenzetting van mevrouw Marie-Hélène Boulanger, hoofd eenheid « Gegevensbescherming », DG Justitie, Europese Commissie*

Het Europees kader van gegevensbescherming en de rol van de Europese Unie

Mevrouw Boulanger herinnert eraan dat richtlijn 95/46 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens,alsook het verdrag van Lissabon de kaderinstrumenten terzake zijn. richtlijn 95/46 dateert van 1996 en dus kan de Europese Commissie al verscheidene lessen trekken uit de toepassing ervan, om het hoofd te bieden aan de nieuwe technologische uitdagingen en aan een steeds meer geglobaliseerde wereld. De vragen omtrent de bevoegde rechtscolleges en het toepasselijk recht blijven echter fundamentele problemen.

Bij de Europese Unie stelt men sinds de inwerkingtreding van het Verdrag van Lissabon op 1 december 2009 een andere aanpak vast van de gegevensbescherming. Oorspronkelijk was richtlijn 95/46 op een « interne marktlogica » gebaseerd. De Commissie is immers opgetreden om ervoor te zorgen dat de verschillen tussen de wetgevingen van de lidstaten geen obstakel waren voor de uitwisseling van persoonsgegevens. Richtlijn 95/46 bracht derhalve een equivalentie in de bescherming tot stand om te voorkomen dat er obstakels voor de datastroom worden opgeworpen. richtlijn 95/46 preciseert dat de nagestreefde harmonisatie in geen geval mag bijdragen tot het beperken of verminderen van het beschermingsniveau dat reeds bestond in de lidstaten. De

L'objectif de la directive est donc un niveau élevé de protection des données à caractère personnel.

Par ailleurs, la Commission avait incité les États membres à ratifier la Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe.

Actuellement, le Traité de Lisbonne dispose que la protection de données constitue un droit fondamental autonome qui peut aussi contribuer à d'autres droits fondamentaux comme la non-discrimination. C'est un élément important parce que ce droit fondamental est distinct de celui de la protection de la vie privée. Par ailleurs, le Traité de Lisbonne considère la protection de données comme une compétence horizontale du Conseil et du Parlement en co-décision et ce pour tous les piliers. Avant l'entrée en vigueur du Traité de Lisbonne, on avait la logique « marché intérieur » pour le premier pilier (« pilier communautaire ») mais la coopération policière et judiciaire en matière pénale relevait du troisième pilier de sorte que les tentatives d'harmonisation effectuées l'ont été sur la base de décisions du Conseil avec une simple opinion du Parlement européen.

La Directive 95/46 protection des données

Mme Boulanger rappelle que la Directive 95/46/CE s'applique dans toute l'Union européenne et vise deux objectifs clés :

— la protection de la vie privée à l'égard des traitements de données et l'harmonisation des critères de base de protection des données en laissant une marge de manœuvre aux États membres;

— garantir la libre circulation des données afin d'éviter que des États membres puissent arguer que d'autres États membres n'ont pas de protection suffisante pour refuser le transfert de données.

Au-delà de la directive, l'harmonisation qui a été réalisée plus récemment mais de manière plus réduite concerne l'harmonisation de la décision-cadre 2008/977/JAI. Cette décision-cadre, devant être mise en œuvre pour cette année, harmonise la protection de données en matière de police et de coopération judiciaire en matière pénale et ne couvre que les données échangées entre États membres.

Au contraire, la directive 95/46, même si elle laisse une marge de manœuvre, est une directive dite d'harmonisation complète car elle impose à chaque État une harmonisation totale sur un certain nombre de points. Dans ce contexte, si l'harmonisation est plus limitée en ne couvrant que les aspects transfrontaliers, elle harmonise réellement la protection dans les différents États membres. Cette interprétation large a

richtlijn beoogt dus een hoog beschermingsniveau voor de persoonsgegevens.

Tevens had de Commissie de lidstaten aangespoord om Verdrag nr. 108 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens van de Raad van Europa goed te keuren.

Momenteel bepaalt het Verdrag van Lissabon dat gegevensbescherming een autonoom grondrecht is dat ook tot andere grondrechten, zoals niet-discriminatie, kan bijdragen. Dat is een belangrijk gegeven, want dat grondrecht staat los van dat van de bescherming van de privacy. Tevens beschouwt het Verdrag van Lissabon gegevensbescherming als een horizontale medebeslissingsbevoegdheid van de Raad en het Parlement en wel voor alle pijlers. Vóór de inwerkingtreding van het Verdrag van Lissabon had men de « interne marktlogica » voor de eerste pijler (« communautaire pijler »), maar de politiële en justitiële samenwerking in strafzaken viel onder de derde pijler, zodat de harmonisatiepogingen plaatsvonden na beslissingen van de Raad, met een eenvoudige opinie van het Europees Parlement.

Richtlijn 95/46 gegevensbescherming

Mevrouw Boulanger herinnert eraan dat richtlijn 95/46/EG in de hele Europese Unie van toepassing is en twee hoofddoelstellingen heeft :

— de bescherming van de persoonlijke levenssfeer in verband met gegevensverwerking en de harmonisatie van de basiscriteria voor de gegevensbescherming met enige manoeuvreerruimte voor de lidstaten;

— het vrij verkeer van gegevens waarborgen om te voorkomen dat lidstaten zouden aanvaren dat andere lidstaten onvoldoende bescherming hebben om de gegevenstransfer te weigeren.

Behalve de richtlijn was de recentste harmonisering, die evenwel beperkter was, die van Kaderbesluit 2008/977/JBZ. Dat kaderbesluit, dat dit jaar ten uitvoer moet worden gelegd, harmoniseert de gegevensbescherming inzake politiële en justitiële samenwerking in strafzaken en heeft alleen betrekking op de gegevens die tussen lidstaten worden uitgewisseld.

Richtlijn 95/46 daarentegen is een richtlijn van zogenaamde volledige harmonisatie — ook al laat ze enige manoeuvreerruimte — omdat ze elke lidstaat een volledige harmonisatie op een aantal punten oplegt. De harmonisatie is weliswaar beperkter doordat ze slechts de grensoverschrijdende aspecten behelst, maar ze harmoniseert de bescherming in de diverse lidstaten werkelijk. Die ruime interpretatie

été confirmée par la Cour de Justice dans un arrêt « *Rechnungshof* ».

Enfin, il existe une directive spécifique au secteur des télécommunications qui a déjà été révisée plusieurs fois et notamment sur la question des *cookies*.

La directive s'applique indifféremment au secteur public et au secteur privé. Les concepts de base de la directive 95/46 pour l'application de la protection des données sont :

— la notion de « données à caractère personnel » qui recouvre « toute information concernant une personne physique identifiée ou identifiable ». C'est un concept large puisque le terme identifiable recouvre aussi une identification par une personne tierce. Aujourd'hui, un manque d'harmonisation sur différentes questions est constaté. Ainsi, des divergences existent quant aux adresses IP (n° généré par l'ordinateur en cas de connexion internet). Doivent-elles être considérées comme une donnée personnelle alors que plusieurs personnes peuvent avoir accès à un seul et même ordinateur ? De même, les données de localisation transmises par un GSM sont-elles des données personnelles ou pas ?;

— la notion de « traitement » est toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel.

Enfin, la directive repose sur les principes atechnologiques de base suivants :

— le traitement doit être légitime et proportionné et les données traitées doivent être proportionnelles par rapport à ce traitement. La légitimité d'un traitement est garantie par différents fondements comme le consentement de la personne, la nécessité contractuelle ou légale, la nécessité par rapport à un intérêt vital ou un intérêt public, ou encore un équilibre d'intérêts et nécessite une évaluation;

— une obligation de transparence impliquant par exemple la communication de l'identité du responsable de traitement de données et la finalité du traitement. Or, sur internet, les mentions existantes sont complexes et juridiques. Par ailleurs, vu la multitude d'opérateurs qui interviennent dans le traitement de données, l'internaute sera vite lassé de répondre à ces innombrables « *privacy notice* »;

— l'instauration d'obligations administratives spécifiques (régime de notification ou d'autorisation préalable). Ainsi, certains transferts de données vers des pays tiers sont soumis à autorisation préalable;

— l'interdiction de traitement des données sensibles (données raciales, ethniques,..) sauf autorisation (consentement ou motifs d'intérêt public).

werd bevestigd door het Hof van Justitie in een « *Rechnungshof* »-arrest.

Er bestaat tot slot een specifieke richtlijn voor de telecomsector, die reeds meermaals werd herzien, onder andere in verband met het cookiesprobleem.

De richtlijn geldt zowel voor de publieke als voor de private sector. De basisconcepten voor richtlijn 95/46 voor de toepassing van de gegevensbescherming zijn :

— het begrip« persoonsgegevens », dat « iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon » behelst. Dat is een ruim concept, want de term identificeerbaar behelst ook identificatie door een derde persoon. Men stelt vandaag een gebrek aan harmonisatie vast voor verscheidene problemen. Er zijn bijvoorbeeld verschillen inzake de IP-adressen (het nummer dat de computer geeft bij verbinding met het internet). Moeten ze als een persoonsgegeven worden beschouwd, terwijl verscheidene personen toegang kunnen hebben tot eenzelfde computer ? Zijn localisatiegegevens die door een GSM worden verzonden persoonsgegevens of niet ?;

— het begrip« verwerking » iselke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procédés.

De richtlijn steunt ten slotte op de volgende atechnologische basisprincipes :

— de verwerking moet rechtmatig en evenredig zijn en de verwerkte gegevens moeten evenredig zijn met die verwerking. Of een verwerking rechtmatig is, wordt op verscheidene gronden gewaarborgd, zoals de toestemming van de betrokkene, de contractuele of wettelijke verplichting, de noodzaak voor een vitaal of algemeen belang, of nog een evenwicht van belangen en vergt een evaluatie;

— de verplichting tot transparantie die bijvoorbeeld impliceert dat de identiteit van de verantwoordelijke voor de verwerking van de gegevens en het doel van de verwerking wordt meegedeeld. Op internet zijn de vermeldingen nu complex en juridisch. Bovendien zal de internaut het door de vele operatoren die bij de gegevensverwerking betrokken zijn snel beu zijn op die talloze « *privacy notices* » te antwoorden;

— het instellen van specifieke administratieve verplichtingen (regeling van voorafgaande kennisgeving of toestemming). Doorgiften van gegevens naar derde landen bijvoorbeeld kan alleen indien daar vooraf toestemming voor is gegeven;

— het verbod op het verwerken van gevoelige gegevens (gegevens van raciale en etnische afkomst,..) tenzij toestemming is gegeven (toestemming of redenen van openbaar belang).

Malgré la réforme de la directive en cours, ces principes restent valides aujourd'hui.

Les droits de la personne

La personne dont les données personnelles ont été traitées disposent d'un droit d'accès qui est explicitement reconnu dans la charte des droits fondamentaux et qui implique :

— une confirmation que des données sont ou ne sont pas traitées,

— un droit de communication des données faisant l'objet des traitements,

— un droit de rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme,

— une notification des modifications aux tiers auxquels les données ont été communiquées.

La personne dispose également d'un droit d'opposition individuel aux traitements de données. La personne concernée a le droit de s'opposer, pour des raisons légitimes, à ce que des données la concernant fassent l'objet d'un traitement. En matière de marketing, il ne faut toutefois pas démontrer d'intérêt.

Les transferts internationaux

Pour éviter que la protection européenne soit mise à mal par un transfert des données à l'étranger, il a fallu assurer une certaine continuité de la protection des données. Pour ce faire, la directive prévoit un double régime.

Pour les pays qui ont une protection adéquate (pas nécessairement équivalente), les données peuvent être transférées et circuler librement car ces États sont assimilés à des États membres.

Le processus d'adéquation est toutefois un processus assez lourd car il aboutit à mettre un pays tiers au même niveau qu'un État membre sans réelle possibilité pour la Commission d'intervenir dans ce pays. Le processus d'adéquation peut être initié soit au niveau des États membres soit par la Commission européenne et nécessite, outre un dialogue avec les pays tiers, une analyse approfondie de leur législation, et au niveau européen l'avis du groupe des autorités de protection de données (« groupe article 29 »), l'avis des États membres dans le cadre de la procédure de comitologie, un droit de regard du Parlement européen, puis une décision formelle du collège des commissaires. À titre d'exemple, la dernière décision d'adéquation a concerné Israël.

Ondanks de hervorming van de richtlijn waarmee men nu bezig is, blijven die principes vandaag gelden.

De rechten van de betrokkene

De persoon wiens persoonsgegevens verwerkt zijn, heeft een recht op toegang dat uitdrukkelijk erkend wordt in het Handvest van de grondrechten. Dit houdt het volgende in :

— uitsluitsel omtrent het al dan niet bestaan van verwerkingen van hem betreffende gegevens,

— recht op verstrekking van de gegevens die zijn verwerkt,

— recht op rectificatie, de uitwissing of de afscherming van de gegevens waarvan de verwerking niet overeenstemt met de bepalingen van deze richtlijn,

— kennisgeving van de wijzigingen aan de derden aan wie de gegevens zijn verstrekt.

De betrokkene beschikt ook over een individueel recht van verzet tegen de verwerking van gegevens. De betrokkene heeft het recht zich te verzetten, om gegronde redenen, tegen de verwerking van zijn gegevens. Inzake marketing, moet men echter geen belang aantonen.

Internationale overdrachten

Om te voorkomen dat de Europese bescherming wordt tenietgedaan bij een overdracht van gegevens naar het buitenland, moest er een zekere continuïteit van de bescherming van de gegevens worden gewaarborgd. Daartoe voorziet de richtlijn in een tweevoudig stelsel.

De gegevens mogen worden overgedragen naar en circuleren vrij in de landen die een passend (niet noodzakelijk equivalent) beschermingsniveau hebben, aangezien die Staten zijn gelijkgesteld met de lidstaten.

De procedure van passend beschermingsniveau is echter een vrij zware procedure want het komt erop neer dat een derde land op hetzelfde niveau wordt geplaatst als een lidstaat zonder dat de Commissie in dat land reëel kan optreden. De procedure van passend beschermingsniveau kan worden opgestart op het niveau van de lidstaten of door de Europese Commissie en vereist, naast overleg met de derde landen, een diepgaande analyse van hun wetgeving en, op Europees niveau, het advies van een groep van de gegevensbeschermingsautoriteiten (« groep artikel 29 »), het advies van de lidstaten in het kader van de comitologieprocedure, het toetsingsrecht van het Europees Parlement en een formeel besluit van het College van commissarissen. Zo betrof de recentste beslissing van passend beschermingsniveau Israël.

Avec les autres pays qui n'ont pas de protection adéquate, il existe une possibilité de régime dérogatoire notamment en cas de consentement de l'individu au transfert, en cas de clauses contractuelles spécifiques ou encore de « *binding corporate rules* ». Celles-ci sont des règles qu'une entreprise multinationale peut adopter, qui doivent être obligatoires pour l'ensemble de ses entités, et qui portent sur les transferts internationaux de données personnelles qui sont réalisés au sein du groupe. Cette approche globale est utile car elle se base sur une solution unique pour l'ensemble de la multinationale et évite ainsi la signature d'une multitude de conventions de transferts de données.

La supervision

La directive prévoit un interlocuteur privilégié proche du citoyen, soit l'autorité de protection des données. Un recours devant les cours et tribunaux est également accordé.

Dans la réalité des faits, des affaires sont portées en justice devant la Cour de Luxembourg mais la majorité des cas sont soumis aux autorités de protection de données notamment en raison de la gratuité de la procédure.

La réforme de la Directive protection des données

Mme Boulanger rappelle que le processus de réforme de la directive a débuté en 2009 et que de nombreuses consultations ont été initiées depuis. À la suite d'une consultation ouverte en ligne fin 2009 et à de nombreuses autres plus spécifiques en 2010, la Commission européenne a abouti en novembre 2010 à une communication qui a, à son tour, été mise en processus de consultation.

Mme Boulanger signale que de nombreuses réponses institutionnelles ont été reçues. Ainsi, le Conseil européen a adopté des conclusions sur cette communication, le Parlement européen est en voie d'adopter un rapport sur cette communication et le Comité économique et social européen prépare également un rapport sur cette communication.

Le contexte de la réforme est surtout influencé par les nouvelles technologies (Internet, compteurs intelligents, puces RFID) et la globalisation. Mme Boulanger souligne également qu'en parallèle, la Commission négocie un accord sur la protection des données en matière de coopération policière et judiciaire en matière pénale. Il s'agit d'aboutir à un accord cadre qui énonce des standards pour la protection des données.

Met de overige landen die geen passend beschermingsniveau hebben, is een afwijkende regeling mogelijk, meer bepaald wanneer de betrokkene akkoord gaat met de overdracht, wanneer er specifieke contractuele clausules zijn of in geval van « *binding corporate rules* ». Dat zijn regels die een multinational kan aannemen, die bindend zijn voor alle eenheden en die de internationale overdrachten van persoonsgegevens betreffen die binnen de groep worden uitgevoerd. Die algemene benadering is nuttig want ze is gebaseerd op één enkele oplossing voor de multinational in zijn geheel waardoor de ondertekening van een groot aantal overeenkomsten betreffende de overdracht van gegevens wordt voorkomen.

Supervisie

De richtlijn voorziet in een bevoorrechte gesprekspartner die dicht bij de burger staat, namelijk de gegevensbeschermingsautoriteit. Een beroep instellen voor de hoven en rechtbanken is ook mogelijk.

In feite worden er zaken voor het Hof van Luxemburg gebracht, maar de meeste zaken worden voorgelegd aan de gegevensbeschermingsautoriteiten, meer bepaald omdat de procedure gratis is.

De hervorming van de richtlijn bescherming van gegevens

Mevrouw Boulanger herinnert eraan dat de hervorming van de richtlijn in 2009 begon en dat er sindsdien heel wat raadplegingen hierover zijn geweest. Na een open onlineraadpleging eind 2009 en na heel wat meer specifieke raadplegingen in 2010, kwam de Europese Commissie in november 2010 tot een mededeling die op haar beurt voor raadpleging werd voorgelegd.

Mevrouw Boulanger wijst erop dat men hierop heel wat institutionele antwoorden kreeg. Zo keurde de Europese Raad conclusies goed over die mededeling, het Europees Parlement zal een verslag over die mededeling goedkeuren en het Europees en Sociaal Comité bereidt ook een verslag over die mededeling voor.

De context van de hervorming is vooral ingegeven door de nieuwe technologieën (internet, intelligente meters, rfid-chips) en de globalisering. Mevrouw Boulanger benadrukt ook dat de Commissie tegelijkertijd over een overeenkomst onderhandelt over de bescherming van gegevens inzake politionele en gerechtelijke samenwerking in strafzaken. Het is de bedoeling een raamovereenkomst te bereiken die standaarden bepaalt voor de bescherming van gegevens.

Les objectifs clés de la réforme visent à renforcer les droits des personnes et la dimension « marché intérieur ». La Commission est consciente que si la Directive contient des droits, les États ont conservé une certaine marge de manœuvre et le degré d'abstraction de certains droits accordés aux citoyens est réel. En conséquence, les citoyens ont aujourd'hui du mal à exercer certains droits de manière efficace et plus particulièrement face aux multinationales. Il convient donc d'alléger les processus pour permettre aux citoyens d'exercer effectivement leurs droits.

Le renforcement de la dimension « marché intérieur » vise à générer moins de formalités préalables pour les entreprises mais à assurer un plus haut degré de responsabilisation et plus de contrôles ex post. La continuité de la protection en cas de transferts internationaux doit également être garantie.

Mme Boulanger rappelle que d'autres organismes ont adopté des réglementations sur la protection des données à caractère personnel. Le Conseil de l'Europe révise ainsi actuellement la Convention n° 108 pour « la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ». Il existe également de nombreuses propositions de loi aux États-Unis, en partie initiées par l'administration américaine, en vue de définir un niveau de protection minimal. À cet égard, Mme Boulanger estime qu'il y a aujourd'hui plus de similarités entre l'approche américaine et européenne qu'il y a quinze ans. Enfin, l'OCDE révise également ses lignes directrices en la matière. Compte tenu de cette multitude d'initiatives, la Commission veille d'abord à ce qu'il y ait une certaine compatibilité des approches.

La réforme vise aussi à réviser les règles de protection des données dans les domaines de la coopération policière et judiciaire en matière pénale et à les intégrer dans un cadre légal européen; le traité de Lisbonne prévoyant actuellement une base légale unique en co-décision entre le Conseil et le Parlement européen.

Enfin, il convient d'assurer une meilleure mise en œuvre des mesures de protection mais également une réponse européenne forte et plus uniforme. En effet, les États membres n'ont pas, malgré le processus de coopération des autorités de protection de données, adopté de position identique par rapport à un même traitement de données.

*2. Échange de vues*

Mme Niessens souhaite être informée quant à la position belge sur la communication de la Commission. Quelles remarques ont été formulées par le gouvernement belge ?

De hoofddoelstellingen van de hervorming zijn de rechten van personen en de dimensie « interne markt » te versterken. De Commissie is zich ervan bewust dat de richtlijn weliswaar rechten bepaalt, maar dat de lidstaten een zekere manoeuvreerruimte behouden en dat de abstractiegraad van bepaalde rechten voor de burgers reëel is. Bijgevolg heeft de burger het momenteel moeilijk om bepaalde rechten op een doeltreffende manier te laten gelden, meer in het bijzonder tegenover multinationals. De procedures moeten dus minder zwaar worden opdat de burger zijn rechten daadwerkelijk kan laten gelden.

De bedoeling van de versterking van de dimensie « interne markt » is minder voorafgaande formaliteiten te genereren voor ondernemingen, maar meer responsabilisering en meer *ex post* toezicht te waarborgen. De continuïteit van de bescherming bij een internationale overdracht moet ook worden gewaarborgd.

Mevrouw Boulanger herinnert eraan dat andere instellingen regelingen over de bescherming van persoonsgegevens hebben aangenomen. Zo werkt de Raad van Europa momenteel Verdrag nr. 108 bij voor « de bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens » Er zijn ook heel wat wetsvoorstellen ingediend in de Verenigde Staten, waartoe de Amerikaanse overheidsdiensten deels het initiatief namen, om een minimum aan bescherming te omschrijven. In dat opzicht meent mevrouw Boulanger dat er momenteel meer gelijkenissen zijn tussen de Amerikaanse en de Europese benadering dan vijftien jaar geleden. Ten slotte, bekijkt de OESO opnieuw haar richtlijnen ter zake. Gelet op dit groot aantal initiatieven, ziet de Commissie er in de eerste plaats op toe dat de benaderingen enigszins verenigbaar zijn.

De hervorming beoogt ook de regeling voor de bescherming van de gegevens inzake politionele en gerechtelijke samenwerking in strafzaken opnieuw te bekijken en ze te integreren in een wettelijke Europees kader; het Verdrag van Lissabon voorziet momenteel ook in één wettelijk kader met medebeslissing van de Raad en het Europees Parlement.

Tot slot, moet er een betere uitvoering van de beschermingsmaatregelen worden gewaarborgd en moet het Europees antwoord sterker en eenvormiger zijn. De lidstaten hebben immers, ondanks de samenwerking van de gegevensbeschermingsautoriteiten, geen identiek standpunt ingenomen over een gelijkvormige gegevensverwerking.

*2. Gedachtewisseling*

Mevrouw Niessens wenst te worden geïnformeerd over het Belgische standpunt met betrekking tot de mededeling van de Commissie. Welke opmerkingen heeft de Belgische regering geformuleerd ?

Mme Boulanger confirme que la Commission de la protection de la vie privée belge a introduit une contribution mais ignore si le gouvernement belge a fait de même. Elle rappelle également qu'en tout état de cause le Conseil a adopté des conclusions de sorte qu'il existe déjà une position commune des États membres sur la communication de la Commission européenne.

Elle renvoie enfin au site Internet de la Commission qui mentionne toutes les observations formulées sur cette communication.

M. Mahoux s'interroge quant au timing du processus de révision de la directive 95/46. D'autre part, il prend acte des dernières évolutions en ce qui concerne la collaboration en matière policière et judiciaire car jusqu'à présent celui qui transmettait des données à des services étrangers tiers n'avait pas d'information sur le degré de protection assuré par ces services.

Enfin, la prochaine directive va-t-elle prévoir la compétence de la Cour de Luxembourg ou la Cour de Strasbourg dès lors qu'il s'agit maintenant d'un droit fondamental ?

En terme de calendrier, Mme Boulanger précise que la Commission est dans le processus d'analyse d'impact. Ce processus est en l'espèce très complexe et ce d'autant plus que la directive s'applique au secteur privé et public. L'objectif est d'aboutir à des propositions législatives présentées par la Commission au mois de novembre 2011.

Sur la question de la coopération policière et judiciaire en matière pénale, la décision-cadre 2008/977/JAI avait été adoptée sur la base de dispositions spécifiques de l'ancien troisième pilier. Elle est toutefois imparfaite. L'objectif est donc de mettre en place un système global et cohérent dans l'UE ce qui passe par une révision des règles actuelles de protection de données dans ce domaine. Il conviendra toutefois d'évaluer dans un premier temps l'impact d'un éventuel nouveau instrument-cadre sur les divers instruments législatifs qui ont déjà été adoptés dans les domaines de la coopération policière et judiciaire en matière pénale.

Sur la compétence de la Cour de Luxembourg et Strasbourg, Mme Boulanger estime qu'il s'agit là plus d'une question de nature politique que juridique. Toutefois, il n'y a pour l'instant pas de contradiction entre les jurisprudences des deux Cours.

## IV. CONCLUSIONS ET RECOMMANDATIONS

Les auditions menées par le groupe de travail ont permis de prendre la mesure des évolutions technolo-

Mevrouw Boulanger bevestigt dat de Belgische Commissie voor de bescherming van de persoonlijke levenssfeer een bijdrage heeft ingediend, maar weet niet of de Belgische regering dat ook heeft gedaan. Ze herinnert er tevens aan dat de Raad in elk geval conclusies heeft goedgekeurd, waardoor er reeds een gemeenschappelijk standpunt van de lidstaten over de mededeling van de Europese Commissie bestaat.

Tot slot verwijst ze naar de website van de Commissie die alle opmerkingen over deze mededeling bevat.

De heer Mahoux heeft vragen over de timing van het herzieningsproces met betrekking tot de richtlijn 95/46. Anderzijds neemt hij akte van de recente evolutie van de samenwerking inzake politie en justitie, want tot op heden had diegene die gegevens naar derde buitenlandse diensten doorstuurde geen informatie over de graad van bescherming die deze diensten waarborgden.

Zal de volgende richtlijn tot slot de bevoegdheid van het Hof van Luxemburg of het Hof van Straatsburg vaststellen, aangezien het nu gaat om een fundamenteel recht ?

Wat het tijdschema betreft, wijst mevrouw Boulanger erop dat de Commissie zich momenteel over de impactanalyse buigt. Dit proces is in dit geval zeer complex, temeer omdat de richtlijn van toepassing is op de privésector en op de openbare sector. Het is de bedoeling te komen tot wetgevingsvoorstellen die door de Commissie in november 2011 worden voorgesteld.

Wat de politiële en justitiële samenwerking in strafzaken betreft, werd het kaderbesluit 2008/977/JBZ aangenomen op grond van specifieke bepalingen van de vroegere derde pijler. Toch is het onvolledig. Het is bijgevolg de bedoeling een allesomvattend en coherent systeem in de EU in te voeren via een herziening van de huidige regels inzake gegevensbescherming op dit gebied. In een eerste fase zal men echter de impact van een eventueel nieuw kaderinstrument moeten evalueren op de diverse wetgevende instrumenten die reeds zijn aangenomen op het gebied van politiële en justitiële samenwerking in strafzaken.

Wat de bevoegdheid van het Hof van Luxemburg en Straatsburg betreft, meent mevrouw Boulanger dat het hier veeleer om een politieke dan om een juridische kwestie gaat. Momenteel is de rechtspraak van beide hoven onderling niet tegenstrijdig.

## IV. CONCLUSIES EN AANBEVELINGEN

De hoorzittingen die door de werkgroep zijn gehouden hebben het mogelijk gemaakt de evolutie op

giques et sociétales à l'œuvre dans le domaine « informatique et libertés ». Ces évolutions posent de nouveaux défis pour la protection de la vie privée en ligne, et la protection des données personnelles de chaque individu.

Les évolutions technologiques d'abord. Elles sont considérables et multiples. Il n'entre pas dans le cadre de ce rapport d'en faire un relevé exhaustif; mais il est évident pour les membres du groupe de travail que les capacités techniques et l'évolution des technologies génèrent des questions nouvelles, ou donnent une nouvelle forme ou une autre ampleur à des questions déjà présentes. Même les législations les plus « a-technologiques », dont les principes fondamentaux sont exprimés de manière générale, indépendante des technologies mises en œuvre, doivent aujourd'hui être adaptées pour rester pertinentes.

À titre illustratif de ces évolutions technologiques tellement importantes qu'elles impliquent une actualisation des normes, le groupe de travail a relevé :

— la croissance exponentielle des capacités de stockage des données, et une nouvelle modalité, le « *cloudcomputing* » (stockage des données « dans le nuage informatique », sur les milliards de machines connectées au réseau mondial);

— la croissance au moins aussi importante des capacités de traitement des informations, permettant par exemple la pratique du profilage à une très grande échelle;

— la croissance des capacités de transmission de données avec, et sans fil (de la fibre optique au réseau de mobilophonie);

— la généralisation des outils de géolocalisation dans des appareils personnels portables;

— la multiplication des puces RFID et des techniques de communication à courtes distances sans fil (*bluetooth*);

— le développement des techniques d'identification biométrique.

Les évolutions comportementales ne sont pas moindres, souvent portées par ces nouvelles possibilités techniques. Les auditions ont mis en avant une évolution essentielle, à savoir l'apparition d'un nouveau modèle économique : l'échange « services contre données personnelles » se substituant à l'échange « services contre argent ». Bien entendu, un échange monétaire subsiste, mais il intervient en seconde ligne : l'opérateur ayant recueilli les données les vend, généralement après traitement, à des fournisseurs de biens ou de services désireux d'adresser de la publicité ciblée. L'utilisateur des services en ligne, lui, ne débourse pas d'argent pour utiliser ces « services

het vlak van de technologie en de samenleving in te schatten wat het domein betreft van « informatica en vrijheden ». Deze evolutie brengt nieuwe uitdagingen met zich mee voor de bescherming van de persoonlijke levenssfeer online en de bescherming van de persoonlijke gegevens van ieder individu.

Eerst iets over de technologische evolutie. Die is groot en bestrijkt verschillende vlakken. In het verslag hoeft daar geen volledige lijst van te komen, maar voor de leden van de werkgroep is het duidelijk : de technische mogelijkheden en de evolutie van de technologie geven aanleiding tot steeds nieuwe vragen, of geven een andere vorm of een andere belangrijkheidsgraad aan reeds bestaande vragen. Zelfs de meest « a-technologische » wetgeving waarvan de fundamentele principes al algemeen zijn uitgelegd, moet tegenwoordig, ongeacht wat voor technologie erin wordt gebruikt, worden aangepast om relevant te blijven.

De werkgroep noemt een paar voorbeelden van de technologische vooruitgang die zo belangrijk is dat ook de normen vervolgens moeten worden aangepast :

— de exponentiële groei van de opslagcapaciteit voor gegevens en een nieuwe manier om dit te doen, « *cloudcomputing* » (opslag van die gegevens in een « informaticawolk », op de miljarden machines die met het wereldwijde net verbonden zijn);

— de zeker even grote groei van de verwerkingscapaciteit met betrekking tot die gegevens, waardoor op een zeer grote schaal aan *profiling* kan worden gedaan bijvoorbeeld;

— de grotere doorgeefcapaciteit, met en zonder kabel (gaande van optische kabels tot het mobiele telefoonnetwerk);

— de veralgemening van de middelen voor positiebepaling (GPS) in de persoonlijke zakinstrumenten;

— de toename van de RFID chips en de technieken voor draadloze korteafstandscommunicatie (*bluetooth*);

— de ontwikkeling van biometrische identificatietechnieken.

Door de nieuwe technische mogelijkheden ziet men ook gedragswijzigingen. Uit de hoorzittingen bleek een essentiële evolutie, namelijk het ontstaan van een nieuw economisch model : de uitwisseling van diensten tegen persoonlijke gegevens, in plaats van wat vroeger de uitwisseling van diensten tegen geld was. Er worden natuurlijk nog diensten geleverd voor geld, maar dit verdwijnt naar de tweede plaats. Eens de operator de gegevens heeft verzameld, verkoopt hij ze aan leveranciers die hun goederen of diensten graag aan een bepaald doelpubliek verkopen. De gebruiker van online diensten betaalt geen geld voor het gebruik van die « gratis diensten » als e-mail, sociale net-

gratuits » que sont les messageries mails, réseaux sociaux, outils de partage de données en lignes (photos, etc.), logiciels de traduction etc., mais met ses données personnelles à disposition.

Ce nouveau type d'échange se nourrit de — ou suscite — la tendance croissante à l'exposition de soi et d'autrui, notamment sur les réseaux sociaux. C'est aujourd'hui l'individu qui fournit de manière volontaire d'innombrables données personnelles sur lui-même et ses relations.

S'il le fait volontairement, le fait-il pleinement conscient de toutes les conséquences de cette exposition publique, particulièrement des différentes formes de l'utilisation ultérieure de ces données ? On ne peut qu'en douter.

Les évolutions technologiques vont plus vite que les adaptations sociétales à ces évolutions; et il n'est pas certain que chacun mesure et maîtrise toutes les conséquences de son comportement au regard de la protection de sa vie privée et du respect de celle d'autrui.

Encore mal approprié, l'espace numérique est aussi le lieu de commission de comportements répréhensibles divers. Deux types de comportements délictueux, liés à l'inflation de trafics en ligne peuvent être identifiés. Tout d'abord, l'utilisation frauduleuse d'informations à des fins de vol, d'arnaque : l'activité criminelle n'est pas nouvelle, mais elle trouve là de nouveaux canaux, utilisant certes de nouvelles technologies, mais profitant surtout d'un manque « d'éducation » des utilisateurs, manifestement moins prudents et plus crédules en ligne que dans la vie « réelle ». Autres types d'usages problématiques : l'usage impropre, et pénalement répréhensible, des possibilités d'expression en ligne : développement de la calomnie publique, de l'usurpation d'identité etc. Ces actes sont souvent commis hors de toute idée criminelle par des individus qui ne mesurent pas que l'expression sur les réseaux est — dans la majorité des cas — publique, ou ne réalisent pas que l'usurpation d'identité en ligne est aussi grave, par exemple, que la réalisation d'un faux en écriture.

La politique en la matière doit être articulée autour des trois axes de la prévention, la détection et la répression.

Face à ces défis techniques et comportementaux, l'implication des individus est le premier des leviers à utiliser pour protéger la vie privée et les données personnelles des individus.

Comme l'ont rappelées les auditions, l'auto-détermination informationnelle est au cœur des législations de protection des données. Cette notion provient d'un arrêt de la Cour constitutionnelle allemande de 1981 qui énonce que chaque individu doit pouvoir faire des choix existentiels et maîtrisés. En l'espèce, un individu

werken, websites om gegevens online te delen (foto's, ...), vertaalprogramma's, enz ..., maar geeft wel toegang tot zijn persoonlijke gegevens.

Die nieuwe vorm van uitwisseling is gebaseerd op een groeiende tendens om zichzelf en anderen zichtbaar te maken, meer bepaald op de sociale netwerksites. Tegenwoordig levert het individu zelf vrijwillig een pak informatie aan over hemzelf en zijn kennissen.

Hij doet dit weliswaar vrijwillig, maar is hij zich daarbij wel bewust van alle gevolgen van deze publieke terbeschikkingstelling en meer bepaald van alle manieren waarop er naderhand van zijn gegevens gebruik wordt gemaakt ? Dat kan betwijfeld worden.

De technologische evolutie gaat sneller dan de maatschappelijke aanpassing aan die veranderingen. Het is dan ook niet zeker dat iedereen, vanuit het oogpunt van de persoonlijke levenssfeer en de inachtneming van die levenssfeer bij anderen, alle gevolgen van zijn gedrag inschat en in de hand houdt.

De digitale wereld is nog niet helemaal geïntegreerd en is dan ook een plek waar allerlei afkeurenswaardig gedrag plaatsvindt. Er zijn twee vormen van misdadig gedrag die gelinkt kunnen worden aan de steeds groeiende online activiteit. Ten eerste kunnen gegevens gebruikt worden voor frauduleuze doeleinden en oplichterij. Deze vorm van misdaad is niet nieuw, maar vindt daar nieuwe kanalen en maakt gebruik van nieuwe technologieën, waarbij ook voordeel wordt gehaald uit het gebrek aan « kennis » van de gebruikers, die online duidelijk minder voorzichtig en lichtgeloviger blijken te zijn dan in het « echte » leven. Een andere problematische toepassing van de technologie is het oneigenlijk en strafbaar gebruik van de online aanwezigheid, wat zich uit in toenemende laster en identiteitsroof bijvoorbeeld. Dit wordt vaak gedaan door mensen die geen misdrijf in gedachten hebben en die niet beseffen dat communicatie via het internet meestal publiek toegankelijk is of dat online identiteitsroof net zo ernstig is als valsheid in geschrifte.

Het beleid moet zich dan ook concentreren rond preventie, detectie en repressie.

Door mensen in de eerste plaats te betrekken bij de nieuwe technologie, kan men deze technische en gedragsgebonden uitdagingen het hoofd bieden, met het oog op de bescherming van de persoonlijke levenssfeer en de persoonlijke gegevens.

Uit de hoorzittingen is eens te meer gebleken dat de wetgeving inzake gegevensbescherming gebaseerd op zelfbepaling. Dit begrip komt uit een arrest van het Duits Grondwettelijk Hof, dat in 1981 besliste dat elk individu zijn existentiële en bewuste keuzes moet kunnen maken. Elkeen moet dus zelf kunnen bepalen

doit pouvoir déterminer lui-même les informations qui circulent sur lui. C'est l'idée du contrôle par chacun de ses informations à caractère personnel (« Qui sait quoi sur moi et qui en fait quoi ? »).

Outre l'éducation, la sensibilisation et la responsabilité de tous les pouvoirs publics compétents comme de la société civile, la norme doit assurer pleinement la primauté de la protection de la vie privée sur toute autre considération, si ce n'est le respect de l'essentiel équilibre avec les autres libertés fondamentales, dont la liberté d'expression. La norme doit prévoir que soit fourni à l'utilisateur un maximum d'informations sur le traitement de ses propres données, et plus de moyens de contrôle sur celles-ci. Elle doit sanctionner les détournements d'usage manifeste.

Les normes démocratiques en cause sont diverses. Les auditions ont montré la variété de niveaux normatifs concernés, depuis les standards établis par la conférence internationale des autorités de protection de données — la résolution de Madrid —, les initiatives des agences de l'ONU, l'actualisation en cours de la Convention du Conseil de l'Europe et de la directive européenne, jusqu'au droit national.

La globalisation étant une caractéristique essentielle du réseau internet, on ne peut qu'espérer l'émergence rapide de règles internationales communes. Le groupe de travail estime que les autorités belges doivent agir à tous les niveaux d'interventions pour favoriser l'émergence de normes internationales protectrices ambitieuses.

Deux normes essentielles au niveau européen sont actuellement soumises à révision :

— la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données est actuellement en cours de modernisation très avancée;

— la Directive 95/46 du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données est également en cours de révision.

Le processus de révision de la directive est en cours depuis plusieurs années. La Commission européenne a présenté, le 25 janvier 2012, un projet de règlement visant à remplacer la directive actuelle. Les consultations vont reprendre sur la base de ce texte. Le Conseil et le Parlement européen devront ensuite l'approuver. Le groupe de travail, formule à titre de recommandations, les principes ad minima qu'il estime souhaitable

welke informatie over hem beschikbaar is. Elkeen moet controle hebben over de persoonlijke gegevens (« wat weet men over mij en wat doet men ermee ? »).

Naast opleiding en sensibilisering, waarvoor alle bevoegde overheidsdiensten en het maatschappelijk middenveld verantwoordelijk zijn, moet de norm ervoor zorgen dat de bescherming van de persoonlijke levenssfeer voorrang krijgt op elke andere overweging, weliswaar met het behoud van een noodzakelijk evenwicht met de andere fundamentele vrijheden, waaronder de vrijheid van meningsuiting. De norm moet bepalen dat de gebruiker zo goed mogelijk wordt geïnformeerd over de behandeling van zijn eigen gegevens, waarop hij meer controle moet kunnen uitoefenen. Hij moet klaarblijkelijke misbruiken strafbaar stellen.

Er zijn verschillende democratische normen in het geding. De hoorzittingen hebben de verscheidenheid aan normatieve niveaus aangetoond, van de standaarden van de internationale conferentie van de diensten bevoegd voor gegevensbescherming — de resolutie van Madrid —, de initiatieven van de VN-agentschappen en de huidige actualisering van de Verdragen van de Raad van Europa en van de Europese richtlijn, tot het nationale recht.

Globalisering is een essentieel kenmerk van het internet, en men kan dan ook maar hopen dat er snel gemeenschappelijke internationale regels komen. De werkgroep meent dat de Belgische overheid op alle niveaus actief moet zijn om de totstandkoming van ambitieuze internationale beschermingsnormen te bevorderen.

Twee essentiële Europese normen worden momenteel herzien :

— verdrag nr. 108 van de Raad van Europa van 28 januari 1981 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, is nu in een ver gevorderd stadium van modernisering;

— richtlijn nr. 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens wordt eveneens herzien.

Het herzieningsproces van de richtlijn is sinds jaren aan de gang. De Europese Commissie heeft op 25 januari een ontwerp van verordening voorgesteld die de huidige richtlijn moet vervangen. Op basis daarvan zouden consultaties worden georganiseerd. De Europese Raad en het Europees Parlement zullen dit later moeten goedkeuren. De werkgroep formuleert aanbevelingen over de minimumprincipes die over-

que toutes les autorités amenées à intervenir dans la discussion sur le texte européen puissent soutenir.

Ces normes supra-nationales se déclinent nécessairement en droit national.

La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard du traitement de données à caractère personnel est le véhicule juridique qui transpose la directive européenne. La révision du texte européen impliquera donc une adaptation importante de la loi de 1992.

De nombreuses suggestions ont été formulées durant les auditions, visant à l'amélioration de l'arsenal législatif national.

Les membres du groupe de travail ont estimé cependant que vu la révision en cours des textes européens, il n'était pas opportun d'entamer un processus de modification fondamentale de la loi de 1992 sans avoir connaissance des grandes évolutions retenues par les futurs textes européens (directive et convention), sous peine de devoir revenir rapidement sur des changements apportés à la loi.

Ils ont donc dégagé quelques thèmes, retenus quelques suggestions parmi celles formulées par les spécialistes auditionnés, qui pourraient faire l'objet de propositions de modifications législatives qui n'interféreraient pas avec le processus de révision de la directive et de la convention du Conseil.

Celles-ci concernent principalement la pénalisation de l'usurpation de l'identité en ligne, l'amélioration des moyens de maîtrise de ses propres données par chaque citoyen, notamment dans l'objectif de faire respecter un « droit à l'oubli » encadré, l'encadrement des pratiques de « profilage » et la meilleure information sur les failles de sécurité pouvant provoquer des atteintes aux données à caractère personnel.

La première thématique concerne donc l'usurpation de l'identité en ligne. Ce phénomène se développe, les chroniques journalistiques comme la jurisprudence en attestent : qu'il s'agisse de recueillir les identifiants personnels d'une personne pour commettre en son nom des infractions, ou créer une page en son nom sur un réseau social, cette criminalité est en développement important; la FCCU en a témoigné.

La justice n'est pas sans outils face à ce phénomène : plusieurs condamnations récentes se sont basées sur des infractions existantes pour condamner les auteurs de faux profils sur le réseau social « facebook » par exemple (notamment faux en informatique — article 210*bis* du Code pénal, usurpation de nom — article 231 du Code pénal).

Mais les responsables de la *Federal Computer Crime Unit* (FCCU) ont estimé, au cours de leur audition, qu'il serait opportun de clarifier les choses en

heden die betrokken zijn bij de bespreking van de Europese tekst volgens hem zouden moeten verdedigen.

Deze supranationale normen hebben hun weerslag op het nationaal recht.

De wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens houdt de omzetting in van de Europese richtlijn. Na de herziening van de richtlijn zal dus ook de wet van 1992 grondig moeten worden herzien.

Tijdens de hoorzittingen werden vele suggesties gedaan om de nationale wetgeving te verbeteren.

De leden van de werkgroep menen echter dat gelet op de aan de gang zijnde herzieningen van de Europese teksten, het nu niet het geschikte ogenblik is om de wet van 1992 grondig te herzien zonder te weten welke de grote lijnen van de toekomstige Europese teksten zullen zijn (richtlijn en verdrag). Anders dreigt men de aangebrachte wetswijzigingen snel weer ongedaan te moeten maken.

Zij hebben dan ook een aantal thema's vastgesteld, en enkele suggesties overgenomen van de gehoorde deskundigen die zouden kunnen uitmonden in voorstellen tot wetswijzigingen die het herzieningsproces van de richtlijn en het verdrag van de Raad niet doorkruisen.

Het gaat vooral om het strafbaar stellen van online identiteitsroof, het verbeteren van de middelen van de burgers om greep te hebben op hun eigen gegevens, met name door middel van een « recht op vergetelheid », een regeling voor « *profiling* »-praktijken, en betere informatie over tekortkomingen in de beveiliging die tot misbruik van persoonlijke gegevens kunnen leiden.

Het eerste thema is dus de online identiteitsroof. Dit verschijnsel is in opmars. Zowel de media als de rechtspraak wijzen erop dat deze vorm van criminaliteit toeneemt, of het nu gaat om het stelen van persoonsgegevens om in naam van die persoon strafbare feiten te plegen, of om een profiel op een sociaal netwerk aan te maken. Ook de FCCU heeft hierop gewezen.

Het gerecht staat niet machteloos tegenover deze praktijken : verschillende recente vonnissen passen de bestaande wetgeving toe om bijvoorbeeld auteurs van valse profielen op het sociale netwerk *Facebook* te veroordelen (met name valsheid in informatica — artikel 210*bis* van het Strafwetboek, aannemen van een naam — artikel 231 van het Strafwetboek).

Verantwoordelijken van de *Federal Computer Crime Unit* (FCCU) hebben er tijdens de hoorzitting echter op gewezen dat het goed zou zijn om de zaken

incriminant directement l'usurpation d'identité sur Internet.

Deuxième thématique retenue, la maîtrise de ses données par l'utilisateur et le « droit à l'oubli ».

Parmi toutes les mesures imaginables pour encadrer le développement des techniques et l'évolution des comportements, l'implication des individus est le premier des leviers : la loi peut donner à l'individu plus d'information, et plus de moyen de contrôle sur ses propres données.

C'est l'objet de ce point des recommandations, visant à actualiser la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel sur certaines questions précises.

Les mesures proposées sont les suivantes :

— la communication de la durée de conservation des données dans le cadre de l'information préalable de la personne concernée;

— un meilleur encadrement des possibilités de réutilisation des données autorisées par la loi : l'habilitation devra être expressément prévue par le texte de loi;

— la communication obligatoire de l'origine des données dans le cadre de l'information de la personne concernée en cas d'utilisation de données obtenues indirectement; cela aux fins de permettre à la personne concernée de demander le cas échéant des corrections ou suppressions au responsable du traitement du fichier originel;

— la possibilité de se voir communiquer ses données par voie électronique;

— plus de possibilité de demander l'effacement ou l'interdiction d'utilisation de certaines données;

— l'obligation d'effacement des données des fichiers quand la détention de ces données est liée à un contrat, qui vient à terme ou est dénoncé; et l'obligation d'effacement des données des fichiers quand elles ont été mises en ligne par l'internaute lui-même, et que celui-ci les en retire;

— l'obligation d'effacement des données, en cas d'utilisation des données pour du « direct marketing », et obligation, pour le responsable du traitement de redemander régulièrement le consentement de la personne concernée, en lui communiquant toutes les données qu'il détient.

te verduidelijken en identiteitsroof op het internet rechtstreeks strafbaar te stellen.

Het tweede thema betreft de beheersing van de eigen gegevens door de gebruiker en het « recht om vergeten te worden ».

Van alle mogelijke maatregelen om de ontwikkeling van technieken en de evolutie van gedrag te sturen, is de betrokkenheid van het individu de belangrijkste hefboom : de wet kan het individu meer informatie geven en meer mogelijkheden om zijn eigen gegevens te controleren.

Dat is de bedoeling in deze aanbevelingen, namelijk de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, bijwerken voor bepaalde specifieke kwesties.

De voorgestelde maatregelen zijn de volgende :

— het meedelen van de bewaartermijn van de gegevens in het kader van het voorafgaandelijk informeren van de betrokken persoon;

— een betere begeleiding van de mogelijkheden om de bij wet toegelaten gegevens opnieuw te gebruiken : de bevoegdheid moet uitdrukkelijk worden bepaald in de wettekst;

— de verplichte vermelding van de oorsprong van de gegevens wanneer de betrokken persoon wordt meegedeeld dat zijn gegevens worden gebruikt en onrechtstreeks werden verkregen; de bedoeling is de betrokken persoon in staat te stellen om, indien nodig, verbeteringen of wijzigingen te vragen aan de beheerder van de oorspronkelijke gegevens;

— de mogelijkheid om zijn gegevens elektronisch te ontvangen;

— meer mogelijkheid om bepaalde gegevens te verwijderen of te verbieden;

— verplichte verwijdering van de gegevens in de bestanden wanneer de bewaring van die gegevens te maken heeft met een contract dat afloopt of wordt verbroken; en de verplichte verwijdering van de gegevens in de bestanden wanneer ze online zijn geplaatst door de internetgebruiker zelf en laatstgenoemde ze zelf verwijdert;

— verplichte verwijdering van de gegevens wanneer de gegevens worden gebruikt voor « *direct marketing* » en verplichting voor de databeheerder om geregeld de toestemming van de betrokken persoon te vragen waarbij hij alle gegevens waarover hij beschikt, meedeelt.

**Troisième thématique abordée : le profilage**

Le profilage est une technique de traitement automatisé des données qui consiste à appliquer un profil à une personne physique afin de prendre des décisions à son sujet ou d'analyser ou de prévoir ses préférences, comportements et attitudes personnel. Parmi toutes les utilisations imaginables, c'est évidemment un outil essentiel du marketing direct, qui permet d'adresser des publicités ciblées à un public pré-sélectionné.

Les auditions ont montré que cette pratique est au cœur des activités des fournisseurs de services sur Internet. Elle fonde le modèle économique des services dit « gratuits ». L'échange « données personnelles contre service » se substitue de plus en plus à la vente de service.

Or la pratique du profilage a des implications fondamentales sur les droits et libertés des individus.

Le Conseil de l'Europe à émis une recommandation sur la protection des personnes dans le cadre du profilage (1), dans laquelle il indique notamment que « l'utilisation des profils, même de manière légitime, sans précautions ni garanties particulières, est susceptible de porter gravement atteinte à la dignité de la personne de même qu'à d'autres libertés et droits fondamentaux, y compris aux droits économiques et sociaux ». Et le Conseil poursuit « persuadé qu'il est donc nécessaire de réglementer le profilage en termes de protection des données à caractère personnel, afin de sauvegarder les libertés et droits fondamentaux des individus, notamment le droit à la vie privée, et de prévenir la discrimination fondée sur le sexe, la race ou l'origine ethnique, la religion ou les convictions, le handicap, l'âge ou l'orientation sexuelle ».

Le Conseil recommande que la collecte et le traitement de données dans le cadre du profilage soit toujours « loyaux, licites et proportionnés » et poursuive des finalités déterminées et légitimes. Il estime que la collecte et le traitement de données dans le cadre du profilage ne peuvent être effectués que si la loi le prévoit ou l'autorise sous certaines conditions, dont le consentement libre, spécifique et éclairé de la personne concernée.

Les membres du groupe de travail suggèrent de donner corps à ces recommandations dans notre droit national.

(1) Recommandation CM/Rec 2010)13 du Comité des ministres aux États membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, adoptée le 23 novembre 2010.

**Derde thema : *profiling***

*Profiling* is een geautomatiseerde verwerkingstechniek van gegevens waarbij een profiel wordt toegepast op een natuurlijke persoon om beslissingen over hem te nemen of zijn voorkeuren, gedrag en persoonlijke houding te analyseren of te bepalen. Van alle denkbare toepassingen, is dit uiteraard een essentieel instrument voor direct marketing, waarmee doelgerichte reclame kan worden gestuurd naar een voorgeselecteerd publiek.

De hoorzittingen hebben aangetoond dat die praktijk centraal staat in de activiteiten van dienstenleveranciers op internet. Ze vormt het economisch model van zogenoemde « gratis » diensten. De uitwisseling van « persoonsgegevens tegen diensten » neemt steeds meer de plaats in van de verkoop van diensten.

*Profiling* heeft fundamentele gevolgen voor de rechten en vrijheden van het individu.

De Raad van Europa heeft een aanbeveling uitgevaardigd over de bescherming van personen in het kader van profiling, waarin meer bepaald staat dat (1), « *l'utilisation des profils, même de manière légitime, sans précautions ni garanties particulières, est susceptible de porter gravement atteinte à la dignité de la personne de même qu'à d'autres libertés et droits fondamentaux, y compris aux droits économiques et sociaux* ». De Raad vermeldt voorts dat « *persuadé qu'il est donc nécessaire de réglementer le profilage en termes de protection des données à caractère personnel, afin de sauvegarder les libertés et droits fondamentaux des individus, notamment le droit à la vie privée, et de prévenir la discrimination fondée sur le sexe, la race ou l'origine ethnique, la religion ou les convictions, le handicap, l'âge ou l'orientation sexuelle* ».

De Raad beveelt aan om gegevens in het kader van *profiling* altijd loyaal, legaal en evenredig te verzamelen en te verwerken en de vastgestelde en wettige doelstellingen na te leven. Hij meent dat het verzamelen en verwerken van gegevens in het kader van profiling slechts mag worden uitgevoerd als de wet dit bepaalt of toestaat onder bepaalde voorwaarden, waaronder de vrije, specifieke en weloverwogen instemming van de betrokkene.

De leden van de werkgroep stellen voor om die aanbevelingen vorm te geven in ons nationaal recht.

(1) Aanbeveling CM/Rec 2010)13 van de Ministerraad aan de lidstaten tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens in het kader van de *profiling*, aangenomen op 23 november 2010.

**Quatrième thématique : la meilleure information sur la survenance de faille de sécurité pouvant compromettre l'intégrité de données à caractère personnel**

Parmi les informations cruciales pour contrôler la transmission des données à caractère personnel figurent bien sûr les failles de sécurité qui rendent possible l'atteinte à ces données par des personnes non accréditées.

Actuellement, l'obligation d'information n'est pas généralisée.

Les membres du groupe de travail recommandent que toute atteinte grave au traitement de données à caractère personnel soit obligatoirement communiquée à la Commission pour la Protection de la Vie privée, et dans certains cas, aux personnes concernées.

Enfin, si la loi est adaptée, les moyens de la faire appliquer doivent être renforcés. En particulier, le groupe de travail estime qu'il conviendrait de définir une politique criminelle consacrée à cette question.

Il convient également d'entamer une réflexion sur les pouvoirs et les moyens de la CPVP, à la lumière des obligations imposées par le futur texte européen.

*
* *

En conclusion, le groupe de travail formule quatre niveaux de recommandations :

— recommandations globales;

— recommandations relatives à la révision des textes européens;

— recommandations relatives aux autorités de contrôle et à l'appareil judiciaire;

— recommandations de réformes législatives immédiates;

**Recommandations**

*Recommandations globales*

1. Favoriser la sensibilisation des citoyens à leurs droits en matière de protection de leur vie privée et de leurs données personnelles, et en particulier auprès des publics maîtrisant mal l'outil numérique. Cet aspect devrait être pris en compte, notamment, dans le plan national de lutte contre la fracture numérique.

**Vierde thema : betere informatie wanneer de veiligheid niet waterdicht is en de integriteit van persoonsgegevens in het gedrang kan komen**

Cruciale informatie om de overdracht van persoonsgegevens te controleren, wordt uiteraard verkregen zodra de veiligheid doorbroken wordt en die gegevens door onbevoegden kunnen worden misbruikt.

Momenteel is de informatieplicht niet algemeen.

De leden van de werkgroep bevelen aan om elke ernstige inbreuk op de verwerking van persoonsgegevens verplicht mee te delen aan de Commissie voor de Bescherming van de Persoonlijke Levenssfeer, en in bepaalde gevallen, aan de betrokken personen.

Wanneer ten slotte de wet wordt aangepast, moeten de middelen om hem te doen toepassen worden versterkt. De werkgroep acht het vooral raadzaam een strafbeleid uit te tekenen voor dat probleem.

Het is ook raadzaam een reflectie aan te vatten over de bevoegdheden en de middelen van de CBPL in het licht van de verplichtingen die de toekomstige Europese tekst zal opleggen.

*
* *

Tot besluit formuleert de werkgroep aanbevelingen op vier niveaus :

— algemene aanbevelingen;

— aanbevelingen over de herziening van de Europese teksten;

— aanbevelingen over de toezichthoudende overheden en het gerechtelijk apparaat;

— aanbevelingen over onmiddellijke wetsherzieningen.

**Aanbevelingen**

*Algemene aanbevelingen*

1. De bewustwording van de burgers stimuleren over hun rechten inzake bescherming van hun privéleven en hun persoonlijke gegevens, in het bijzonder van de groepen die de digitale media niet goed beheersen. Dat aspect moet met name worden meegenomen in het nationaal actieplan ter bestrijding van de digitale kloof.

2. Favoriser l'application de standards internationaux dans le domaine de la protection de données personnelles et leurs déclinaisons dans des normes *supra*-nationales contraignantes ambitieuses.

*Recommandations relatives à la révision de la directive 94/46*

3. Assurer un suivi attentif du processus de révision de la directive européenne, en favorisant l'adoption d'un texte qui contienne les éléments suivants :

— renforcement des droits des citoyens au respect de leur vie privée et de leurs données personnelles;

— primauté du consentement libre, spécifique et éclairé de la personne concernée préalablement de tout traitement de données, sauf les exceptions explicitement prévues par la loi;

— interdiction du profilage, sauf si la loi le prévoit ou si la loi l'autorise et qu'il est précédé du consentement libre, spécifique et éclairé de la personne concernée;

— renforcement de l'obligation d'information de la personne concernée et généralisation du principe de portabilité des données;

— les données de géolocalisation et les données génétiques sont considérées comme des données sensibles;

— encadrement d'une forme de droit à l'oubli par l'obligation d'effacement, sur demande de la personne concernée, de toute donnée qui n'est plus nécessaire aux buts poursuivis par le traitement ou de toute donnée connue grâce au consentement de la personne concernée, qui retire son consentement. Quand c'est la personne elle-même qui a rendu des données publiques, grâce à des services dont c'est l'objet commercial, les données doivent être effacées systématiquement quand la personne les supprime;

— renforcement du rôle des autorités nationales de contrôle.

*Recommandations relatives aux autorités de contrôle*

4. Politique criminelle

La poursuite des infractions à la loi du 8 décembre 1992 doit être prioritisée, et faire l'objet d'une politique criminelle stratégique.

2. De toepassing stimuleren van internationale standaarden op het gebied van de bescherming van persoonlijke gegevens en de omzetting ervan in ambitieuze, bindende supranationale normen.

*Aanbevelingen over de herziening van richtlijn 94/46*

3. Voor een aandachtige voortgangsbewaking zorgen van de herziening van de Europese richtlijn, waarbij de goedkeuring wordt bevorderd van een tekst die de volgende elementen bevat :

— versterking van de rechten van de burgers inzake de eerbiediging van hun privéleven en hun persoonlijke gegevens;

— het primaat van de vrije, specifieke en weloverwogen instemming van de betrokkene voor elke dataverwerking, behalve voor de uitzonderingen die uitdrukkelijk door de wet zijn bepaald;

— verbod van profiling, tenzij de wet daarin voorziet of indien de wet het toestaat en het wordt voorafgegaan door de vrije, specifieke en weloverwogen instemming van de betrokkene;

— verstrenging van de verplichting om de betrokkene te informeren en veralgemening van het beginsel van de overdraagbaarheid van de data;

— data van geolokalisatie en genetische data worden als gevoelige gegevens beschouwd;

— flankerende maatregelen voor een vorm van recht op vergetelheid door de verplichting tot het wissen op verzoek van de betrokkene van elk gegeven dat niet langer noodzakelijk is voor het door de verwerking nagestreefde doel, of van elk gegeven dat gekend is dankzij de toestemming van de betrokkene, die zijn toestemming intrekt. Wanneer de persoon zelf gegevens publiek heeft gemaakt, door middel van diensten waarvan dat het commercieel doel is, moeten de data systematisch worden gewist wanneer de persoon ze verwijdert;

— grotere rol van de nationale toezichthoudende overheden.

*Aanbevelingen over de toezichthoudende overheden*

4. Strafbeleid

Er moet prioriteit worden verleend aan de vervolging van de overtreding van op de wet van 8 december 1992 en er moet een strategisch strafbeleid voor worden ontwikkeld.

5. Réflexion sur les pouvoirs de CPVP

Une réflexion doit être engagée, visant à donner plus de pouvoir d'action et de sanctions à la CPVP et à préserver son indépendance.

*Recommandations relatives à des propositions législatives immédiates*

6. Modifications législatives immédiates

Pénaliser l'usurpation de l'identité en ligne, tant du nom patronymique que d'autres identifiants, et pénaliser la collecte illégitime d'identifiant en ligne.

Modifier la loi du 8 décembre 1992 pour y insérer :

— l'obligation de communication de la durée de conservation des données dans le cadre de l'information préalable de la personne concernée;

— un meilleur encadrement des possibilités de réutilisation des données autorisées par la loi : l'habilitation devra être expressément prévue par le texte de loi;

— la communication obligatoire de l'origine des données dans le cadre de l'information de la personne concernée en cas d'utilisation de données obtenues indirectement;

— la possibilité de se voir communiquer ses données par voie électronique;

— plus de possibilités de demander l'effacement ou l'interdiction d'utilisation de certaines données;

— l'obligation d'effacement des données des fichiers quand la détention de ces données est liée à un contrat, qui vient à terme ou est dénoncé; et l'obligation d'effacement des données des fichiers quand elles ont été mises en ligne par l'internaute lui-même, et que celui-ci les en retire;

— l'obligation d'effacement des données, en cas d'utilisation des données pour du « direct marketing », et obligation, pour le responsable du traitement de redemander régulièrement le consentement de personne concernée, en lui communiquant toutes les données qu'il détient.

Profilage : édicter un principe d'interdiction, sauf quand la loi le prévoit ou l'autorise sous certaines conditions, dont le consentement libre, spécifique et éclairé de la personne concernée.

5. Reflectie over de bevoegdheden van de CBPL

Er moet een reflectie worden aangevat met het oog op het geven van meer actie- en sanctiebevoegdheden van de CBPL en op het beschermen van haar onafhankelijkheid.

*Aanbevelingen over onmiddellijke wetsherzieningen*

6. Onmiddellijke wetsherzieningen

Online identiteitsroof, zowel van het patroniem als van andere identificatiemiddelen strafbaar stellen, en het onrechtmatig inzamelen van online identificatiemiddelen strafbaar stellen.

De wet van 8 december 1992 wijzigen om er het volgende in te voegen :

— de verplichting om in het raam van de voorafgaande informatie aan de betrokkene mee te delen hoe lang de data bewaard worden;

— een betere flankering van de mogelijkheden tot hergebruik van de door de wet toegestane data : de wettekst zal uitdrukkelijk in de machtiging moeten voorzien;

— de verplichte mededeling van de herkomst van de data in het raam van het informeren van de betrokkene bij het gebruik van onrechtstreeks verkregen data;

— de mogelijkheid om zijn data langs elektronische weg toegezonden te krijgen;

— meer mogelijkheden om het wissen van gegevens of het verbod om bepaalde gegevens te gebruiken te vragen;

— de verplichting om de data uit de bestanden te wissen wanneer het houden van die data aan een contract gekoppeld is dat verstrijkt of opgezegd wordt; en de verplichting de data uit de bestanden te wissen wanneer ze door de internaut zelf *on line* werden gezet en hij ze ervan verwijdert;

— de verplichting de data te wissen bij gebruik van die data voor « *direct marketing* », en de verplichting voor de verantwoordelijke voor de verwerking om regelmatig opnieuw de toestemming te vragen van de betrokkene en daarbij alle data waarover hij beschikt mee te delen.

*Profiling* : een principieel verbod invoeren, tenzij de wet erin voorziet of het toestaat onder bepaalde voorwaarden, waaronder de vrije, specifieke en weloverwogen instemming van de betrokkene.

Améliorer l'information sur la survenance de faille de sécurité pouvant compromettre l'intégrité de données à caractère personnel.

## V. DISCUSSION

M. Courtois relève que le groupe de travail a procédé à l'audition Directeur de la *Federal Computer Crime Unit* (FCCU). Cette cellule se plaint du manque de moyens, y compris en personnel. Est-il exact que la FCCU n'est pas en mesure de suivre les évolutions technologiques dans une série de domaines ? La FCCU ne serait dès lors pas en mesure d'apporter des réponses à certains phénomènes en matière de criminalité informatique. Le groupe de travail a-t-il examiné la question des moyens dont dispose les services de police pour lutter contre ces formes de criminalité organisée ?

L'intervenant demande ensuite s'il n'est pas nécessaire de légiférer en matière d'effacement des données personnelles. En droit pénal belge, il existe deux mécanismes permettant une cessation des effets d'une condamnation après exécution de la peine. Ces mécanismes sont l'effacement et la réhabilitation pénale. Ne devrait-on pas introduire une législation comparable pour l'effacement des données personnelles ?

À la question relative à l'aspect judiciaire et la lutte contre la criminalité organisée, M. Mahoux renvoie à la visite au parquet fédéral effectuée par la commission au mois de novembre 2011. La criminalité informatique est une matière transversale. Le parquet fédéral dispose d'une cellule de lutte contre la criminalité organisée et les délits informatiques liés à la criminalité organisée. Il serait intéressant d'interroger la ministre de la justice sur cet aspect de la politique criminelle.

Sur l'effacement des données, M. Mahoux rappelle que le droit à l'oubli était le point de départ de la réflexion du groupe de travail. De nombreux experts sont favorables à un système d'effacement des données. Le monde de la presse est beaucoup plus réservé sur ce point. L'intervenant cite l'hypothèse d'une personne qui serait condamnée en justice. Après un certain délai, cette condamnation sera effacée sur le plan pénal. Les journalistes ne sont cependant pas prêts à supprimer les documents de presse qui ont été publiés et dans lesquels il a été fait état de la condamnation.

M. Mahoux pense que le droit à l'oubli devrait être une réalité, surtout lorsque l'information a été mise à disposition sur une base volontaire. Il faudrait que la personne puisse obtenir l'effacement des données qui la concernent. La question est plus délicate pour les informations qui ont été mises dans le domaine public

Beter informeren over gebreken in de beveiliging die de integriteit van de persoonsgegevens in het gedrang kunnen brengen.

## V. DEBAT

De heer Courtois wijst erop dat de werkgroep een hoorzitting heeft gehouden met de Directeur van de *Federal Computer Crime Unit* (FCCU). Die cel klaagt over het gebrek aan middelen en ook aan personeel. Klopt het dat de FCCU op een aantal gebieden niet in staat is de technologische ontwikkelingen te volgen ? De FCCU zou dan niet in staat zijn antwoorden te bieden op bepaalde verschijnselen van computercriminaliteit. Heeft de werkgroep het vraagstuk onderzocht van de middelen die de politiediensten hebben om die vormen van georganiseerde misdaad te bestrijden ?

Vervolgens vraagt spreker of het niet nodig is een wetgevend initiatief te nemen inzake uitwissing van persoonsgegevens. In het Belgisch strafrecht zijn er twee mechanismen waardoor een veroordeling na uitvoering van de straf ophoudt uitwerking te hebben. Die mechanismen zijn de uitwissing en het herstel in eer en rechten. Moet men geen vergelijkbare wetgeving invoeren voor de uitwissing van persoonsgegevens ?

Op de vraag over het gerechtelijk aspect en de bestrijding van de georganiseerde misdaad, verwijst de heer Mahoux naar het bezoek van de commissie aan het federaal parket in november 2011. De computercriminaliteit is een transversale materie. Het federaal parket heeft een cel ter bestrijding van de georganiseerde misdaad en de computermisdrijven die een band hebben met de georganiseerde misdaad. Het kan interessant zijn de minister van justitie over dat aspect van het strafbeleid te ondervragen.

Wat de uitwissing van gegevens betreft, herinnert de heer Mahoux eraan dat het recht om vergeten te worden het uitgangspunt was van de reflectie van de werkgroep. Talrijke deskundigen zijn voorstander van een systeem van uitwissing van de gegevens. Wat dat betreft, is de perswereld veel terughoudender. Spreker geeft het voorbeeld van iemand die veroordeeld is. Na enige tijd zal die veroordeling op strafrechtelijk gebied worden uitgewist. De journalisten zijn echter niet bereid om gepubliceerde persdocumenten waarin melding werd gemaakt van de veroordeling, te doen verdwijnen.

De heer Mahoux denkt dat het recht om vergeten te worden een werkelijkheid zou moeten zijn, vooral wanneer de informatie vrijwillig ter beschikking werd gesteld. De persoon moet de uitwissing van de gegevens over hem kunnen verkrijgen. De vraag is delicater voor de gegevens die in het publiek domein

et qui continuent d'exister. Des oppositions se sont manifestées sur ce plan, surtout du monde de la presse.

M. Van Rompuy se réjouit du travail accompli par le groupe de travail sur un thème aussi important.

L'intervenant se bornera à une seule observation.

Le groupe de travail a entamé ses travaux dans l'idée que la législation européenne mettrait encore plusieurs années à voir le jour. Mais à la fin des travaux du groupe de travail, les choses se sont subitement accélérées.

Il faut donc veiller à ce que les initiatives éventuelles, qui seraient prises ultérieurement sur la base du présent rapport, soient conformes aux directives dont l'Europe est en train de tracer les contours.

Pour le surplus, l'intervenant peut pleinement souscrire à l'esprit et à la philosophie du rapport.

## VI. VOTE

Le présent rapport a été approuvé à l'unanimité des 9 membres présents.

*Le rapporteur,* *Le président,*

Philippe MAHOUX. Alain COURTOIS.

zijn beland en die blijven bestaan. Er is verzet gerezen tegen dat plan, vooral bij de pers.

De heer Van Rompuy is verheugd over het werk dat door de werkgroep werd geleverd over zulk belangrijk thema.

Spreker wil wel één bedenking uiten.

De werkgroep heeft zijn werkzaamheden aangevat in de veronderstelling dat de Europese wetgeving nog enkele jaren zou uitblijven. Aan het einde van de werkzaamheden van de werkgroep kwam men echter plots in een stroomversnelling terecht.

Aldus moet men ervoor waken dat eventuele handelingen, bij de latere *output* van dit verslag, in overeenstemming zijn met de richtlijnen die thans door Europa worden uitgetekend.

Voor het overige kan spreker de geest en de filosofie van het verslag volledig onderschrijven.

## VI. STEMMING

Dit verslag werd eenparig goedgekeurd door de 9 aanwezige leden.

*De rapporteur,* *De voorzitter,*

Philippe MAHOUX. Alain COURTOIS.

120268 - I.P.M.